cloud security alliance®

Top Threats Working Group

Publication

Top Threats to Cloud Computing

Deep Dive 2025

The permanent and official location for Cloud Security Alliance Top Threats research:
https://cloudsecurityalliance.org/research/working-groups/top-threats/

Foreword

About the *Top Threats* Working Group

Cloud computing transformed businesses and governments, creating new security challenges at an unprecedented pace. The development of the cloud service model delivers business-supporting technology more efficiently than ever. The shift from traditional client/server to cloud service models transforms how technology departments think about, design, and deliver computing technology and applications.

The security impacts associated with the cloud shift are still emerging. The Cloud Security Alliance (CSA) *Top Threats* Working Group aims to inform organizations with an up-to-date, expert-informed understanding of cloud security risks, threats, and vulnerabilities to make educated risk management and technology decisions regarding cloud computing, services, and software.

Case Study Project Genesis

Since 2010, the CSA *Top Threats to Cloud Computing* survey-driven report has filled a significant gap, providing valuable industry insight into the latest cloud threats, risks, and vulnerabilities. However, security professionals recognize that the top cloud concerns in the report only paint a part of the bigger picture. The collective concerns and reflections of cloud experts, survey respondents, and industry participants miss the real-world impacts and losses. Announced at the Black Hat USA conference in 2019, the *Top Threats* Working Group launched the bi-annual cloud breach case studies document called the "Deep Dive" as a companion to the cloud risks survey.

The Deep Dives attempt to articulate cloud computing's most significant and pressing issues. This work complements the continuous research about top threats by reflecting on real-world attacks and breaches. The *Top Threats* Working Group describes more technical details dealing with architecture, compliance, risk, etc. We hope this data and analysis of recent cloud security incidents will help cloud defenders, vendors, authorities, and users take meaningful action against the top cloud risks. The Deep Dive should direct greater confidence and appreciation of key considerations in making cloud systems and services safer in real-world scenarios.

Target Audience

Cloud and security practitioners or enthusiasts will benefit from this publication, gaining up-to-date insight into the practical state. The case studies' recency keeps the cloud security threats and challenges relevant, with specific industry participants' impacts and improvements. The in-depth breach analysis will equip compliance, risk, and technology staff with security-oriented business considerations. Finally, strategic insights, such as key takeaways, trend observations, and business impacts, will help executive management with cloud resilience planning and adjusting cloud investments.

What You Will Find

This document uses the CSA *Top Threats to Cloud Computing 2024 survey analysis* to reflect real-world cloud breach cases. The paper uses the survey analysis to identify the top threats, guiding the identification of **eight** recent and high-profile real-world cloud attacks and breaches. Each breach case is presented as (1) a threat model and (2) a detailed narrative in a concise and easy-to-reference fashion. The threat model format provides an attack-style synopsis of the malicious actor, spanning the range from threats and vulnerabilities to controls and mitigations.

We encourage security practitioners and technology leaders to use the breach case studies and insights to start their own internal analyses, comparisons, and discussions. Readers should draw on similarities in the threats, controls, and considerations to improve preparation and yield faster responses. The longer-form narratives provide additional context, such as how an incident came to pass and how it should be mitigated. References provide opportunities for additional research. We elaborate on expected outcomes and possibilities where details, such as impacts or mitigations, were not discussed publicly.

We hope you find this work helpful and welcome any feedback and/or participation in upcoming publications.

To your future success,
The CSA *Top Threats* Working Group

Executive Summary

Summary

This *Top Threats to Cloud Computing Deep Dive* analyzes **eight** recent industry cloud breach cases. We derive actionable insights to benefit cloud users, builders, and defenders. In this next installment, we share applicable Cloud Controls Matrix (CCM version 4.1) controls and key takeaway insights to equip the reader with a threat model for each case. The mappings to each applicable *Top Threats to Cloud Computing 2024* tie back each case to the annual *Top Threats* industry survey.

In this publication, we have analyzed and threat-modeled the breach cases of *Snowflake Customers' Data Breaches* (2024), *Football Australia* (2024), *CrowdStrike* (2024), *Toyota* (2023), Darkbeam (2023), *Retool & Fortress* (2023), *FTX* (2022), and *Microsoft* (2024).

Our analysis produced observations on the prevalence of gaps that are currently observed frequently, the growing impact of identity and access management and supply chain risks on cloud security, the changing profile of threat actors targeting cloud services, and, most importantly, key takeaways that cloud users, builders, and defenders can implement to further resilience.

Top Cloud Threats Coverage

In the *Top Threats to Cloud Computing 2024* survey, we surveyed over 500 industry experts on security issues in the cloud industry. Our respondents identified eleven important security issues to their cloud environment (ranked in order of concern indicated by the survey):

TT1. Misconfiguration and Inadequate Change Control	**TT7.** Accidental Cloud Disclosure
TT2. Identity and Access Management (IAM)	**TT8.** System Vulnerabilities
TT3. Insecure Interfaces and APIs	**TT9.** Limited Cloud Visibility/Observability
TT4. Inadequate Selection/Implementation of Cloud Security Strategy	**TT10.** Unauthenticated Resource Sharing
TT5. Insecure Third-Party Resources	**TT11.** Advanced Persistent Threats (APT)
TT6. Insecure Software Development	

The top cloud concerns manifested in the breach cases covered this year are:

	Snowflake	Football Australia	CrowdStrike	Toyota	Darkbeam	Retool & Fortress	FTX	Microsoft
TT1		✓	✓	✓	✓	✓		
TT2	✓	✓		✓	✓	✓	✓	✓
TT3			✓		✓			✓
TT4			✓	✓				✓
TT5			✓			✓		
TT6		✓	✓				✓	✓
TT7		✓		✓	✓			
TT8			✓	✓	✓			
TT9				✓				✓
TT10		✓		✓				
TT11	✓							

Observations

The table above reflects our analysis of real-world cloud breaches and categorizes security threats based solely on how frequently they appeared in our case studies. These threats are grouped into three tiers based on their observed occurrence. The following section presents these findings in a structured format, helping to illustrate which threats have been most commonly observed in the examined breach cases.

Tier 1 - Most Frequent (4 to 7 appearances) – The most commonly observed security threats across breach cases.
- IAM – Weak access controls, lack of multifactor authentication (MFA), and privilege escalation enabled unauthorized access.
- Misconfiguration and Inadequate Change Control – Improperly secured cloud environments led to prolonged data exposure.
- Insecure Software Development – Weak software development, delivery, and deployment practices introduced security flaws that attackers exploited.

Tier 2 - Notable (3 appearances) – These threats appeared in multiple cases and represent significant security concerns.
- Insecure Interfaces and APIs – Publicly exposed or weakly secured APIs served as attack vectors in multiple incidents.
- Inadequate Selection/Implementation of Cloud Security Strategy – Organizations without well-defined cloud security strategies faced governance and risk management challenges.
- System Vulnerabilities – Unpatched software and outdated configurations contributed to security breaches.

Tier 3 - Less Frequent (1 or 2 appearances) – Less frequently observed threats but still relevant.
- Limited Cloud Visibility/Observability – Unintentional exposure of sensitive data due to human error in cloud configurations.
- Unauthenticated Resource Sharing – Publicly accessible cloud resources (e.g., confidential or sensitive data) increase the risk of unauthorized access.
- Insecure Third-Party Resources – Supply chain risks reinforced the need for proactive vendor security assessments and continuous monitoring.
- APT – Threat actors leveraged credential theft, privilege escalation, and lateral movement.

The table below compares the results of the *Top Threats to Cloud Computing 2024* survey with findings from this Deep Dive 2024-2025 report. The survey column ranks cloud security issues based on the number of respondents who identified each issue as a top concern. This survey served as the input for selecting which issues to explore in the Deep Dive.

The Deep Dive column, in contrast to the survey column, presents the frequency with which each issue appeared during the analysis of selected security incidents. While the survey reflects perceived importance, the Deep Dive reflects how often each issue was observed across incidents. Because many incidents involved multiple contributing issues, the order in the Deep Dive differs from the original survey ranking.

Deep Dive and Top Threat Survey Security Issue Comparison

Threat ID	Freq	Deep Dive 2024-2025 Report/ Security Issues	Thread ID	Top Threats 2024 Survey/ Security Issues
Tier 1				
TT2	7	Identity and Access Management (IAM)	TT1	Misconfiguration and Inadequate Change Control
TT1	5	Misconfiguration and Inadequate Change Control	TT2	Identity and Access Management (IAM)
TT6	4	Insecure Software Development	TT3	Insecure Interfaces and APIs
Tier 2				
TT3	3	Insecure Interfaces and APIs	TT4	Inadequate Selection/Implementation of Cloud Security Strategy
TT4	3	Inadequate Selection/Implementation of Cloud Security Strategy	TT5	Insecure Third-Party Resources
TT7	3	Accidental Cloud Disclosure	TT6	Insecure Software Development
TT8	3	System Vulnerabilities	TT7	Accidental Cloud Disclosure
Tier 3				
TT9	2	Limited Cloud Visibility/Observability	TT8	System Vulnerabilities
TT10	2	Unauthenticated Resource Sharing	TT9	Limited Cloud Visibility/Observability
TT5	2	Insecure Third-Party Resources	TT10	Unauthenticated Resource Sharing
TT11	1	Advanced Persistent Threats (APT)	TT11	Advanced Persistent Threats (APT)

Key Takeaways

The vulnerabilities, threats, and security weaknesses outlined in *Top Threats to Cloud Computing 2024* have materialized in real-world breaches, exposing recurring failure patterns and misconfigurations that attackers continue to exploit. By analyzing these incidents, we have identified actionable lessons organizations can adopt today to enhance cloud security and mitigate breach risks.

Cloud Security Must Account for Human Error and Persistent Threats

- Cloud architectures and security strategies must assume misconfigurations and human mistakes will occur as threat actors seek to exploit them.
- Continuous improvement requires continuous auditing, security automation, security awareness initiatives, and integrating lessons learned from past incidents.

Identity and Access Security Controls Are Essential

- Strong IAM practices, including MFA, least privilege access control, and privileged access management (PAM) must be rigorously enforced.
- Excessive privileges, weak authentication, and poor access control policies frequently enable lateral movement and privilege escalation in breaches.

Shared Responsibility in Cloud Security Must Be Enforced

- Cloud providers and users must work together to secure their environments by implementing configuration management, access controls, and security monitoring.
- Vendors should promote secure defaults, enforce strong configurations, and proactively detect abuse within cloud services.

Continuous Monitoring and Real-Time Detection Are Critical

- Automated monitoring, anomaly detection, and centralized logging are necessary to identify misconfigurations, unauthorized access, and malicious activities quickly.
- Many cloud breaches remain undetected for extended periods due to insufficient visibility and alarms/notifications.

Supply Chain Security Must Be Strengthened

- Threat actors target weaknesses in supply chains, open-source components, and third-party integrations to infiltrate cloud environments.
- Organizations must assess vendor security, enforce strict security requirements, and continuously monitor dependencies for potential threats.

Proactive Cloud Governance Reduces Long-Term Risk

- Weak governance, a lack of consistent misconfiguration review, and compliance monitoring allow security gaps to persist for years.
- Organizations must enforce cloud security policies, maintain secure configuration baselines, and conduct regular governance reviews to ensure timely remediation of security risks in compliance with regulations such as GDPR and HIPAA.

Incident Response and Recovery Must Be Cloud Specific

- Traditional incident response plans fail to account for cloud complexity, leading to delayed detection and mitigation.
- Organizations must enforce cloud security policies, maintain secure configuration baselines, and conduct regular governance reviews to ensure timely remediation of security risks in compliance with data protection and industry-specific regulations such as GDPR and HIPAA.

Security Testing and Validation Must Extend Beyond Production

- Many breaches originate from vulnerabilities in development and testing environments, where security controls are often weaker than in production.
- Least privilege, access controls, and security monitoring must be enforced across all cloud environments to prevent attackers from exploiting non-production systems.

This research working group and our valued contributors hope cloud providers, security teams, and users will use the working group's findings to enhance their security programs, inform strategic cloud initiatives, and reduce risks from the evolving threat landscape. Readers are encouraged to review the threat analysis for each breach case, evaluate their security postures, and implement the necessary controls to mitigate emerging threats effectively.

Acknowledgments

Top Threats Working Group Co-chairs

Jon-Michael C. Brook
Alexander Stone Getsin
Vic Hargrave
Michael Roza

Lead Authors

Jon Michael Brook
Randall Brooks
Alexander Stone Getsin
Laura Kenner
Michael Morgenstern
Michael Roza
Sherre Stine
Mark Szalkiewicz

Contributors

Singa Ambikapathi
Sara Farnsworth
Udith Wickramasuriya
Vatsal Gupta
Sathish Holl
Akanksha Chaturvedi
Sakshi Mittal
Pankaj Kumar
Patrick Saint Tulias
Sahil Dhir

Reviewers

Sai Vishnu Vardhan Machapatri
Lakshmi Ramya Gudimella Ananta Venkata
Rangel Rodrigues
Bhavya Jain
Sahil Parmar
Harry Wan
Shiva Pati
Dharnisha Narasappa
Vishnu Machapatri
Morgan King
Rajiv Dewan

CSA Staff

Alex Kaluza
Claire Lehnert
Stephen Lumpe
Stephen Smith

Special Thanks

The *Top Threats* Working Group would like to thank **Sean Heide** for six years of support through this and multiple previous publications.

Table of Contents

MEET THE TOP THREATS

Security Issue 1

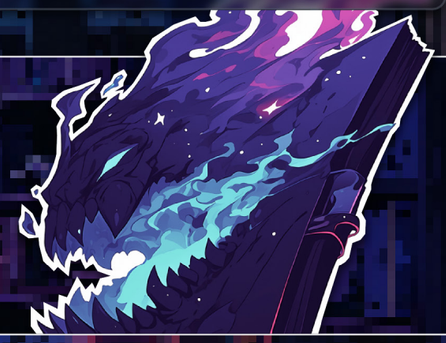
MISCONFIGURATION & INADEQUATE CHANGE CONTROL

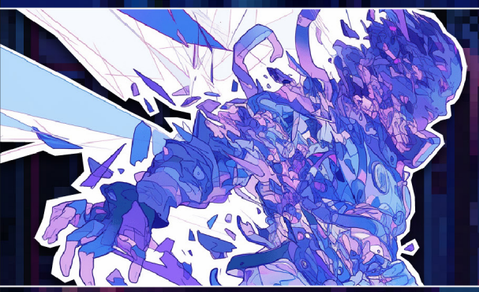
The impact of misconfigurations or inadequate change controls in cloud systems can be severe, depending on their nature and how quickly they're detected and mitigated.

Security Issue 2

IDENTITY & ACCESS MANAGEMENT

Inadequate IAM can cause unauthorized access, data breaches, and non-compliance, leading to major financial and reputational harm. Effective IAM strategies are key to protecting sensitive data.





Security Issue 3

INSECURE INTERFACES & APIS

Cloud providers and vendors often face API and UI challenges from shifting leadership, strategies, or third-party access, leading to weak authentication, lack of encryption, and poor session management.

Security Issue 4

INADEQUATE CLOUD SECURITY STRATEGY

Inadequate Cloud Security Strategy risks misalignment of architecture, service models, and vendors with business goals, stressing the need for a plan to ensure secure operations and mitigate risks.

Security Issue 5

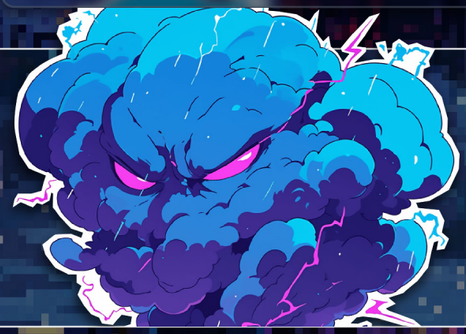
INSECURE THIRD-PARTY RESOURCES

Cloud adoption increases supply chain vulnerabilities via third-party resources, known as Cybersecurity Supply Chain Risk Management (C-CSRM). Two-thirds of breaches result from these supply chain risks.

Security Issue 6

INSECURE SOFTWARE DEVELOPMENT

Developers may unintentionally create insecure software due to cloud complexity, leading to exploitable vulnerabilities. A cloud-first approach, secure practices, and SDLC help mitigate risks and ensure secure applications.



Security Issue 7

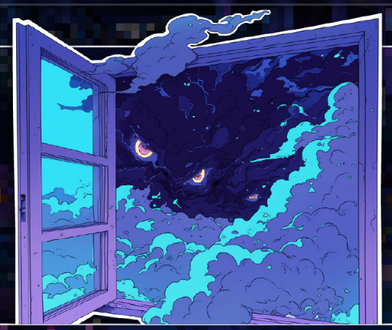
ACCIDENTAL DATA DISCLOSURE

Accidental data disclosures from misconfigurations in cloud platforms like AWS, Azure, and GCP remain a risk, with 21.1% of public buckets holding sensitive data. Breaches result from prioritizing convenience over security.

Security Issue 8

SYSTEM VULNERABILITIES

System vulnerabilities in cloud services can compromise data and disrupt operations. Key vulnerabilities include misconfigurations, zero-day flaws, unpatched software, and weak credentials. Regular monitoring, patch management, and Zero Trust architecture are essential defenses.



Security Issue 9

LIMITED CLOUD VISIBILITY/OBSERVABILITY

Limited cloud visibility poses significant risks, including unsanctioned app use (Shadow IT) and sanctioned app misuse, which can lead to undetected security breaches and costly data breaches.

Security Issue 10

UNAUTHENTICATED RESOURCE SHARING

Unauthenticated cloud sharing is a major security risk. To protect sensitive data in cloud resources, enforce password protection, MFA, third-party authentication, and manage access while monitoring for suspicious activity.

Security Issue 11

ADVANCED PERSISTENT THREATS

Advanced persistent threats (APTs) are a major risk to cloud security, with attackers like nation-states and criminal gangs using tactics such as ransomware, zero-day exploits, and phishing to compromise environments.

SNOWFLAKE | 2024

Threat actor	Threat	Vulnerabilities	Technical impacts	Business Impacts	Controls
TT11- External Organized Crime Hackers, APT An identified attacker associated with hacking forums and partners in data extortion.	**Data Theft** Use of infostealer malware. **Account hijacking** of Snowflake accounts. **Extortion** of victim organizations.	*TT2- Insufficient Identity, Credentials, Access, Key Management* Lack of two-factor authentication.	**Data Breach** Unauthorized access, theft of data, inclusive of personal data, and published some of it. **Threat Operation** Advertising victim data for sale on cybercrime forums, exposing victims further to extortion attempts and attacks. **Compliance** Breach disclosure on behalf of breached companies.	**Financial** Millions of USD in extorted funds (likely more). Non-material financial losses. **Operational** Mandiant and other incident response resources and investment. **Reputational** Association of Snowflake's brand with high-profile data breaches diminishes customer trust, market confidence, and negatively affects future business.	**Preventive** -IAM-14 -IVS-03 -DSP-07 -UEM-09 -UEM-11 **Preventive** -LOG-03 -CCC-07 -LOG-05 -SEF-02 **Preventive** -SEF-07 -STA-14 -TVM-02

Attack Detail

Threat Actor: Mandiant tracks UNC5537, a financially motivated threat actor suspected to have stolen a significant volume of records from Snowflake customer environments and undertaking extortion against breached organizations. The hacker is alleged to act primarily under the name "Judische" or "Waifu" and may be a 26-year-old software engineer living in Ontario, Canada, as per the reporting of Krebs on security. The hacker seemed to operate with close associates and other individuals on hacker forums to exploit his access and exfiltrated data.

Threat: The threat actor used Snowflake account credentials previously stolen via infostealer malware to access the customer's Snowflake instance. Breach and exfiltration of valuable data and consequent extortion of affected companies led to direct financial losses and illicit gain upwards of $2 million USD. Hundreds of Snowflake customers appear to have been breached, and known victims include AT&T, Ticketmaster, and Santander.

Vulnerabilities: Insufficient identity, credentials, access, and key management, specifically lacking two-factor authentication for targeted Snowflake instances, enabled the attackers to gain access to scores of Snowflake accounts. This exploitation was also made possible due to lacking baseline authentication security measures, such as conditional access, and neglect to ensure that access credentials are rotated. Datastore segregation from unsecured networks (the internet) via network allow-lists to limit access to the sensitive datasets was disregarded.

Technical Impacts

Confidentiality: Breached organizations' confidential information was exfiltrated and, in some cases, leaked to the public or hacker communities. Some of the breach victims were identified.

Compliance: Snowflake acted to meet regulatory obligations to disclose the breaches in financial reporting (SEC filing), as well as choosing to inform affected customers. Breached organizations similarly acted on disclosure obligations. In at least two cases, 8-K forms filed with the SEC detailed accounts of the breaches and their impacts.

Data Breach: Unauthorized access to data, theft of data, inclusive of personal data at the care of affected companies took place. These data breaches continue to manifest and surface in business strategies, reporting, performance and brand association of the companies, even if in evidently limited ways.

Threat Operation: Breached organizations' data was advertised for sale on cybercrime forums, exposing victims further to extortion attempts and attacks and contributing to loss of trust and complexity of the organizations' response.

Business Impacts

Financial: Non-material financial losses and financial consequences of up to $3 million USD were reported by companies, as attested by the companies in SEC filings. Material impacts on equity and stock prices of affected companies were not evident. Some of the affected companies were subject to data extortion and elected to pay, resulting in further financial losses and related compliance complications.

Operational: Breached organizations engaged specialized incident response teams, such as Mandiant, and significantly increased investments in advanced threat containment, forensic investigations, and proactive recovery strategies. They also strengthened security infrastructures to mitigate ongoing risks and prevent recurrence. Snowflake conducted a joint investigation with Mandiant and invested in new product strategies, controls, and efforts to strengthen customer database accounts' security posture.

Reputational: The repeated association of Snowflake's brand with high-profile data breaches is likely to detrimentally impact customer trust, diminish market confidence, and influence future procurement decisions and investor perceptions, potentially affecting long-term competitive positioning.

Controls - Preventive Mitigation

IAM-14: Strong Authentication – Implement and evaluate appropriate measures for authenticating access to systems, applications, and data assets, including multifactor authentication for privileged user and sensitive data access.

IVS-03: Network Security – Restrict communications between environments and sensitive data systems to only authenticated and authorized connections and networks, as justified by the business. Consider restricting internet access to internal data stores using allow lists and other means.

DSP-07: Data Protection by Design and Default – Develop systems, products, and business practices based upon a principle of security by design and industry best practices. For example, when designing authentication for a data store or adoption of a data store, integrate controls against the likely failure of users neglecting to implement their two-factor authentication, or against its capability to lead to a sensitive data breach.

UEM-09: Anti-Malware Detection and Prevention – Apply and maintain measures to protect against malware on managed assets.

UEM-11: Data Loss Prevention – Employ Data Loss Prevention (DLP) technologies and rules in accordance with a risk assessment.

IAM-05: Least Privilege – Employ the least privilege principle when implementing information and data systems access.

Controls - Detective Mitigation

LOG-03: Security Monitoring and Alerting – Continuously identify, monitor, and correlate security-related events across applications, networks, and underlying infrastructure, leveraging automated analytics and real-time threat intelligence integrations to enhance anomaly detection capabilities and expedite incident response.

CCC-07: Detection of Baseline Deviation – Implement detection measures with proactive notification in case of changes deviating from the established baseline, such as two-factor authentication for critical systems and data access.

LOG-05: Audit Logs Monitoring and Response – Detect activity outside of typical or expected patterns and take timely actions on detected anomalies, particularly as they relate to identity, access, databases, and data.

SEF-02: Incident Management – Establish and maintain an incident response plan to promptly identify, respond to, limit, analyze, and report incidents.

Controls - Corrective Mitigation

SEF-07: Security Breach Notification – Define and implement processes, procedures, and technical measures for security breach notifications. Report security breaches and assumed security breaches including any relevant supply chain breaches, as per applicable SLAs, laws,and regulations.

STA-14: Supply Chain Data Security Assessment – Define and implement a process for conducting security assessments periodically for all organizations within the supply chain.

TVM-02: Vulnerability/Patch Management – Implement and maintain a documented vulnerability management process to address the discovery, reporting, and remediation of vulnerabilities.

Metrics

Key Performance Indicators

- Mean-Time-to-Detect (MTTD) unsanctioned or anomalous use of human and programmatic credentials
- Mean-Time-to-Detect (MTTD) a breach, a leak, and indicators of compromise in the wild (e.g., using threat intelligence)
- Human access to data, total users able to access sensitive data (the fewer the better)

Control Effectiveness Measurements

- Deviations from baseline security controls in systems, identities, and data stores
- Coverage of multifactor authentication, single sign-on, and least privilege implementation for users

Key Takeaways

- Baseline configuration and identity security controls (TT1, TT2) continue to dominate as effective controls in common and advanced breach cases.
- Review and implement the shared responsibility model. Cloud users ought to understand and practice their responsibility over the security measures in their control, securing the data and workloads they put in cloud services.
- Vendors have a responsibility to create and promote the use of safe configurations and security controls in their offered cloud service. Secure defaults and the path of least resistance for sensitive cloud services, such as data stores, should be safe and secure, while exceptions and abuse should be flagged and contained within functional and business areas.

References

1. Hacker in Snowflake Extortions May Be a U.S. Soldier
   https://krebsonsecurity.com/2024/11/hacker-in-snowflake-extortions-may-be-a-u-s-soldier/

2. Detecting and Preventing Unauthorized User Access, by Snowflake
   Snowflake's own post on the breach, their response, and following developments

3. UNC5537 Targets Snowflake Customer Instances for Data Theft and Extortion, by Google's Mandiant
   Mandiant's publication on identifying the breaches and working with the different actors to uncover and contain them

4. Hacker behind Snowflake customer data breaches remains active, by Cyberscoop
   Follow-up media coverage of fallouts and continued threat actor activity in the wake of the Snowflake customer breaches

5. Lawsuit accusing LendingTree, a Snowflake customer, of failure to implement adequate security measures to protect against the data breach
   https://www.mpamag.com/us/news/general/lendingtree-facing-snowflake-class-action-claim/523469

FOOTBALL AUSTRALIA | 2024

Threat actor	Threat	Vulnerabilities	Technical impacts	Business Impacts	Controls
Internal Developer design flaw or misconfiguration. **External** This issue was identified by cybersecurity researchers.	**Data Theft** Potential data theft of Personal Identifiable Information (PII) of players, ticket purchase information, internal infrastructure details, source code of the digital infrastructure, and infrastructure as code.	*TT1- Misconfiguration and Inadequate Change Control* AWS S3 bucket with no protected access keys, access keys were not updated in over 2 years. An S3 bucket was publicly listable. *TT2- Identity Access and Mgmt (IAM)* AWS access keys are used for AWS Cognito, an identity platform for web and mobile apps. *TT6- Insecure Software Development* The website was developed with hard-coded credentials. *TT10- Unauthenticated Resource Sharing* AWS S3 bucket set to open.	**Confidentiality:** *TT7- Accidental Cloud Disclosure* Sensitive user data, including PII, ticket purchases, passport data, contracts, etc., is publicly exposed. **Integrity** Although the sensitive data was publicly accessible for over 700 days, there was no indication that the data was modified. **Availability** There was a minor service disruption in the centralized registration platform.	**Financial** Notification costs for any PII data lost. **Operational** The system had to be reconfigured and coded to properly utilize AWS access keys. These keys now need to be rotated. **Compliance** Potential issues with the Australian Privacy Act 1988. **Reputational** Media exposure of the data breach.	**Preventive** -AIS-02 -AIS-05 -CCC-03 -CEK-03 -DSP-07 -STA-13 **Detective** -CCC-07 -IAM-08 -TVM-06 -LOG-03 **Corrective** -AA-06 -CEK-05 -DSP-08

Attack Detail

Threat Actor: The actual threat actor was not identified, but it was determined that the vulnerability directly resulted from human error. The vulnerability was discovered by Cybernews cybersecurity researchers and disclosed to the service provider.

Threat: Plaintext keys were encoded in the source of Football Australia's website. These keys provided access to Football Australia's 127 digital storage containers. One of the accessible buckets contained personal details of the football players. Additionally, data was externally disclosed, including attendee purchase information, computing infrastructure and design, and source code.

Vulnerabilities: The AWS S3 buckets were misconfigured, with one publicly accessible to anyone on the internet without any authentication. As a result, any potential threat actor could access the plaintext keys. The website was designed and developed with a critical architectural flaw: an AWS long-term access key was embedded directly into the source code of the Football Australia website. These hard-coded credentials were used to access the fully open AWS S3 buckets.

Technical Impacts

Confidentiality: The breach resulted in the unauthorized disclosure of PII and sensitive organizational data, compromising data privacy and security. Sensitive user data, including PII, ticket purchases, passport data, contracts, etc., were publicly exposed. This issue aligns with TT7 Accidental Cloud Disclosure. (2) (5) (6)

Integrity: There is no evidence indicating that the exposed data was altered, suggesting its original state remained intact despite the exposure for over 700 days. (5) (6)

Availability: There was a minor service disruption in the centralised registration platform. Beyond this, the incident did not cause any major system downtime or service disruptions, indicating that availability was only slightly limited. (6)

Business Impacts

Financial: The average cost of data breach notifications, estimated at $370k USD in 2023, could escalate based on the volume of compromised data and potential legal liabilities. (4)

Operational: The system had to be reconfigured and coded to utilize AWS access keys properly. These keys now need to be rotated regularly. (1)

Compliance: Potential issues with the Australian Privacy Act 1988 are due to the failure to produce private data for Australian citizens. (3)

Reputational: Media coverage of the data breach could damage public trust, tarnish brand reputation, and potentially reduce ticket sales, sponsorships, and partnerships.

Controls - Preventive Mitigation

AIS-02: Application Security Baseline Requirements – Establish, document, and maintain baseline requirements for securing different applications.

AIS-05: Automated Application Security Testing – Implement a testing strategy, including criteria for acceptance of new information systems, upgrades, and new versions, that provides application security assurance and maintains compliance while enabling organizational speed of delivery goals. Automate when applicable and possible.

CCC-03: Change Management Technology – Manage the risks associated with applying changes to organization assets, including application, systems, infrastructure, configuration, etc., regardless of whether the assets are managed internally or externally (i.e., outsourced).

CEK-03: Data Encryption – Provide cryptographic protection to data at-rest and in-transit, using cryptographic libraries certified to approved standards.

DSP-07: Data Protection by Design and Default – Develop systems, products, and business practices based upon a principle of security by design and industry best practices.

STA-13: Infrastructure as Code (IaC) – Use Infrastructure as Code to automate the provisioning and configuration of cloud resources. This helps enforce consistent security configurations and reduces the risk of manual errors. This ensures S3 buckets are correctly configured from the start.

Controls - Detective Mitigation

CCC-07: Detection of Baseline Deviation – Implement detection measures with proactive notification in case changes deviate from the established baseline, such as network shares, misconfiguration, and accessibility.

IAM-08: User Access Review – Review and revalidate user access for least privilege and separation of duties with a frequency commensurate with organizational risk tolerance. Programmatic access to provisioned scripts and privileged access systems can help detect gaps and exploits similar to what happened here.

TVM-06: Penetration Testing – Define, implement, and evaluate processes, procedures, and technical measures for the periodic performance of penetration testing by independent third parties.

LOG-03: Security Monitoring and Alerting – Identify and monitor security-related events within applications and the underlying infrastructure. Define and implement a system to generate alerts to responsible stakeholders based on such events and corresponding metrics.

Controls - Corrective Mitigation

AA-06: Remediation – Establish, document, approve, communicate, apply, evaluate, and maintain a risk-based corrective action plan to remediate incident and breach case findings, lessons learned, and improvement plans findings; review and report remediation status to relevant stakeholders. This is particularly critical in cases where recurring breaches have occurred.

CEK-05: Encryption Change Management – Establish a standard change management procedure to accommodate changes from internal and external sources for review, approval, implementation, and communication of cryptographic, encryption, and key management technology changes.

DSP-08: Data Breach Response Plan – Develop and maintain a data breach response plan that outlines the steps to take in the event of a data breach, including notification procedures, containment measures, and recovery strategies. This ensures a structured approach to handle breaches.

Metrics

Key Performance Indicators

- Mean-Time-to-Detect (MTTD): Average time taken to detect misconfigurations, unauthorized access attempts, or cloud security incidents in Football Australia's cloud environment.
- Access Violation Rate: Percentage of unauthorized access attempts or resource misuse incidents detected over a specific period in Football Australia's cloud environment.
- Detection of Baseline Deviation: Percentage of Football Australia's cloud environment where security settings deviated from approved baselines, detected by audits or automated tools.
- Logging and Monitoring Coverage: Percentage of Football Australia's cloud environment enabled by real-time logging, monitoring, and anomaly detection.
- Policy Compliance Rate: Percentage of cloud services and configurations meeting internal or regulatory security policies.
- Number of Cloud Resources Accessible through the Internet: The total number of resources that can be directly connected to by any system.

Control Effectiveness Measurements

- Mean-Time-to-Remediate (MTTR): Average time to correct security misconfigurations in Football Australia's cloud environments from detection to resolution.
- Cloud Configuration Compliance Rate: Percentage of Football Australia's cloud assets (storage, networks, applications) that adhere to security configuration baselines.
- Audit and Access Review Coverage: The percentage of Football Australia's cloud accounts and access controls reviewed and adjusted to the least privilege during security audits.
- Unauthorized Access Attempt Rate: Percentage of unauthorized access attempts to Football Australia's cloud environments successfully blocked by authentication and access controls.
- Anomaly Detection Efficacy: Percentage of detected baseline deviations in the Football Australia's cloud environment that result in actionable alerts.

Key Takeaways

- Embedding long-term AWS access keys directly within website source code presents a severe security vulnerability, as it enables unauthorized access to critical cloud services. Instead, organizations should adopt dynamic credential management systems, such as AWS Secrets Manager or IAM roles, to securely generate and manage keys at runtime.
- Regularly rotating AWS access keys is essential to limit their exposure and reduce the risk of credential misuse in the event of unauthorized access. Organizations should enforce automated key rotation policies with short-lived credentials to further minimize exposure.
- Protecting sensitive data, such as PII, requires robust encryption mechanisms at rest and in transit. Organizations should ensure that data stored in AWS S3 buckets or other cloud services is encrypted using AWS Key Management Service (KMS) or equivalent solutions.
- Misconfigured AWS S3 buckets are a leading cause of cloud data leaks. Organizations should implement policies to block public access across all S3 buckets and enable access logging to monitor for unauthorized or unintended access.

References

1. Football Australia - Public Cloud Security Breaches
   https://www.breaches.cloud/incidents/footballaustralia/
2. Football Australia leak exposes players' details
   https://cybernews.com/security/football-australia-leak-expose-players/
3. Understanding Data Protection and Privacy Laws Australia
   https://generisonline.com/understanding-data-protection-and-privacy-laws-in-australia/
4. 110 of the Latest Data Breach Statistics [Updated 2024]
   https://secureframe.com/blog/data-breach-statistics
5. Players' Passports, Contracts Exposed in Football Australia Data Leak
   Football Australia data breach exposes players' passports, contracts
6. Football Australia data breach reportedly exposes contracts, passports, and ticket information
   Football Australia data breach reportedly exposes contracts, passports, and ticket information - ABC News

CROWDSTRIKE | 2024

Threat actor	Threat	Vulnerabilities	Technical impacts	Business Impacts	Controls
Internal A failed CrowdStrike quality assurance process. **External** *TT5- Insecure Third-Party Resources* - Trusting, quality expectant CrowdStrike customers. *Organized Crime Hackers, APT* Opportunistic threat actors launching email, malware, and misinformation attacks, exploiting confusion and panic.	*TT6- Insecure Software Development* Directly resulted in an outage in Microsoft systems, servers, infrastructure, and many reliant services and organizations in the industry.	*TT1- Misconfiguration and Inadequate Change Control* Lacking change control on software deployment and implementation permitted a faulty update to affect systems globally. *TT3- Insecure Interfaces and APIs* Reports of tools using the same ring 0 Windows vulnerability. *TT4- Inadequate Selection/ Implementation of Cloud Security Strategy* A strategic direction for a homogeneous environment oftentimes manifests as a single point of failure vs. multiple vendor selections. *TT6 - Insecure Software Development* An out-of-bounds read issue in a Crowdstrike update caused a failure of the product and the host system. TT6- Insecure Software Development CrowdStrike's deployment processes on Microsoft Windows utilize over-provisioned access that did not impact Linux implementations of CrowdStrike.	**Confidentiality** None publicly disclosed. **Integrity** Failed recoveries and corrupted backups. **Availability** Even with CrowdStrike's one-day patch and recovery procedures, physical access to machines for safe mode boot identified poor internal processes within customers' environments.	**Financial** -45% CrowdStrike stock price drop and 3rd quarter losses of $16.82 million USD -$5.4 billion USD in Fortune 500 direct losses -Delta claimed $500 billion USD in revenue/ expenses. **Operational** With an 18% endpoint protection market share, CrowdStrike customers worldwide scrambled directly or due to third party suppliers. **Compliance** No reports. **Reputational** CrowdStrike's 24-hour patch and transparency helped the company rebound quickly.	**Preventive** -CCC-02 -CCC-03 -STA-02 -AIS-05 -BCR-11 **Detective** -CCC-07 -LOG-03 -SEF-05 -TVM-08 **Corrective** -A&A-06 -SEF-03 -STA-12 -TVM-03 -BCR-10

Attack Detail

Threat Actor: Unlike many of this year's case studies, most of the companies affected by the CrowdStrike outage see the threat actor as CrowdStrike, their trusted third-party (or fourth-party) supplier. Not covered are opportunistic cybercriminals who exploited the ensuing confusion by launching phishing attacks and distributing malware disguised as legitimate CrowdStrike updates.

Threat: The CrowdStrike outage in July 2024 exposed the critical dependency on centralized security solutions, highlighting the risk of single points of failure in endpoint protection. With an 18% global market share, numerous companies found themselves impacted directly or through their supply chain.

Vulnerabilities: The CrowdStrike outage revealed vulnerabilities in process management, testing, third-party security assessments, risk evaluations, and incident response planning. Both CrowdStrike and its customers failed to conduct adequate testing in their change management processes, underscoring the importance of robust software testing and safeguard development. Even customers following best practices, such as keeping the latest revision in QA testing and rolling out production versions one revision behind, overlooked critical system components, leaving the core functionality untested. The immediate deployment of faulty definition files across all Falcon endpoint agents compounded the issue. Additionally, the outage exposed gaps in third-party security assessments, as companies often relied on vendors' architectural descriptions, and audits primarily confirmed process adherence rather than true security effectiveness. The incident also highlighted the need for comprehensive risk assessments and supply chain mapping to proactively identify vulnerabilities and implement safeguards. Furthermore, incident response plans lacked critical capabilities, particularly in physical hardware access planning, leaving many customers struggling to implement remediation steps despite CrowdStrike publishing guidance on the first day of the outage.

Technical Impacts

Confidentiality: The CrowdStrike outage did not directly contribute to confidentiality failures. While recovery process exposures or ancillary cybercriminal activity may have occurred, there were no publicized instances of data exposure due to the incident.

Integrity: As would be expected with a disruption of this magnitude, the CrowdStrike outage included numerous accounts of failed recoveries and corrupted backups. To restore functionality, affected systems required manual intervention, such as booting into safe mode or Windows Recovery Environment to delete specific configuration files. Additionally, devices protected with BitLocker encryption faced further complications. Recovery necessitated entering a unique 48-digit BitLocker recovery key for each device.

Availability: Loss of availability was far and away the biggest lesson reinforced by the headline-grabbing Delta Airlines. While CrowdStrike produced a fix for the situation within a day, Delta dealt with the ramifications for weeks. Affected too were government, healthcare, and other organizations.

Business Impacts

Financial: The losses associated with the outage were staggering. CrowdStrike reported 3rd quarter losses as $16.82 million USD. CrowdStrike stock losses amounted to a 45% drop over the 18 days following the outage. Fortune estimates the Fortune 500 impact included $5.4 billion USD in direct losses. As one of the highest profile impacts, Delta canceled 7,000 flights, estimating $500 billion USD in revenue losses and additional expenses.

Operational: CrowdStrike identified the issue and released a fix on the same day. However, the need for manual intervention on many affected computers created extended outages. Only Windows machines were impacted in the July incident.

Compliance: There were no reports of compliance fines for the incident.

Reputational: Global and negative coverage across media platforms was prominent and critical. Mainstream media such as Forbes, AP News, and many local news outlets more directly covered the incident, with generally negative sentiment towards the brand. The stock price rebounded within four months, reaching all time highs shortly thereafter.

Controls - Preventive Mitigation

CCC-02: Quality Control – Follow a defined quality change control, approval, and testing process with established baselines, testing, and release standards. Implementing better QA processes within CrowdStrike's release process could ensure all software updates follow a robust testing process with staged rollouts and rollback mechanisms that may have detected the faulty update before deployment.

CCC-03: Change Management Technology – Manage the risks associated with applying changes to organization assets, including applications, systems, infrastructure, configuration, etc., regardless of whether the assets are managed internally or externally (i.e., outsourced). CrowdStrike customers with a structured change management process with automated rollback could have minimized the spread of the faulty update.

STA-02: SSRM Supply Chain – Apply, document, implement, and manage the SSRM throughout the supply chain for the cloud service offering. Organizations using Falcon Sensor should have conducted regular security reviews and contingency planning for vendor failures.

AIS-05: Automated Application Security Testing – Implement a testing strategy, including criteria for acceptance of new information systems, upgrades, and new versions, which provides application security assurance and maintains compliance while enabling organizational speed of delivery goals. Automate when applicable and possible. Implementing gradual, phased rollouts instead of immediate global deployment of definition files would have reduced the scope of impact.

BCR-11: Equipment Redundancy – Supplement business-critical equipment with redundant equipment independently located at a reasonable minimum distance in accordance with applicable industry standards. Organizations should have had a tested disaster recovery plan to quickly switch to alternative endpoint protection.

Controls - Detective Mitigation

CCC-07: Detection of Baseline Deviation – Implement detection measures with proactive notification in case changes deviate from the established baseline, such as network shares, misconfiguration, and accessibility. Real-time monitoring of Falcon Sensor definition file updates could have triggered an alert when the faulty update was pushed globally.

LOG-03: Security Monitoring and Alerting – Identify and monitor security-related events within applications and the underlying infrastructure. Define and implement a system to generate alerts to responsible stakeholders based on such events and corresponding metrics. Endpoint behavioral monitoring could have flagged the unexpected system crashes immediately, enabling faster rollback.

SEF-05: Incident Response Metrics – Establish and monitor information security metrics. Monitoring security metrics, including the CrowdStrike agents offline, could detect sensor updates prior to complete distribution.

TVM-08: Vulnerability Prioritization – Use a risk-based model for effective prioritization of vulnerability remediation using an industry recognized framework. Threat intelligence feeds tracking vendor software stability could have warned organizations about issues with Falcon Sensor updates before deployment.

Controls - Corrective Mitigation

A&A-06: Remediation – Establish, document, approve, communicate, apply, evaluate, and maintain a risk-based corrective action plan to remediate incident and breach case findings, lessons learned, and improvement plans findings. Review and report remediation status to relevant stakeholders. This is particularly critical in cases like CrowdStrike, where a Linux outage occurred two months prior to the Windows outage.

SEF-03: Incident Response Plans – Establish, document, approve, communicate, apply, evaluate, and maintain a security incident response plan, which includes but is not limited to: relevant internal departments, impacted cloud service customers (CSCs), and other business critical relationships (such as supply chain) that may be impacted. Organizations should have had pre-approved legal and compliance frameworks for quickly engaging third-party vendors (CrowdStrike in this case) and coordinating remediation efforts.

STA-12: Supply Chain Service Agreement Compliance – Implement policies requiring all cloud service providers (CSPs) throughout the supply chain to comply with information security, confidentiality, access control, privacy, audit, personnel policy, and service level requirements and standards. While it might be a stretch for endpoint detection and response (EDR), organizations maintaining contracts with multiple product/service vendors could switch security providers in case of an outage.

TVM-03: Vulnerability Remediation Schedule – Define, implement, and evaluate processes, procedures, and technical measures to enable both scheduled and emergency responses to vulnerability identifications, based on the identified risk. Organizations could have enforced more robust patch rollback procedures to quickly disable problematic updates.

BCR-10: Response Plan Exercise – Exercise the disaster response plan annually or upon significant changes, including local emergency authorities if possible. Ensure disaster recovery drills include third-party software failures. Organizations with regular security software failure simulations would have responded faster to the outage.

Metrics

Key Performance Indicators

- Percent of Third-Party Vendor Assessment Coverage and Compliance with SLAs: Annually measures the percentage of vendors that undergo security and compliance assessments per year.
- Average Risk Score of Third-Party Vendors: Measure the risk levels associated with vendors based on security assessments and put additional controls against higher risk vendors.
- Percent of Incident Response Plans (IRPs) with Legal Review: Measures the percentage of IRPs that have been reviewed and approved by legal counsel.
- Mean-Time-to-Remediate (MTTR): Measures how long it takes to restore services after a change (e.g., network, code, API) or outage.

Control Effectiveness Measurements

- Change Request Approvals Before Implementation: Percentage of changes that are formally reviewed and approved before deployment.
- Documentation of Risk Assessments for Changes: Percentage of changes that include a documented risk assessment before deployment.
- Third-Party Compliance with Security Standards: Percentage of vendors meeting security and regulatory compliance requirements (e.g., ISO 27001, SOC 2, NIST, GDPR, CCPA)
- Third-Party Issue Resolution Speed: Average time to remediate security vulnerabilities in third-party vendors.
- On-Time Completion of Data Breach Regulatory Notifications: Percentage of data breaches that were reported within the legally required timeframe (e.g., 72 hours for GDPR).

Key Takeaways

- Understand the third-party (and fourth-party) supply chain risks associated with cloud shared responsibilities models and take steps to limit exposure where your control is limited but outcomes can potentially be disastrous.
- Staggered rollouts or critical infrastructure exceptions should be considered.
- While immediate patching for zero day vulnerabilities can quell an actively exploited vulnerability, quality assurance testing often pays significant benefits.
- Contracts may be the only enforceable method for correcting harm created by suppliers. Include legal teams to review implications or draft language for SLAs and breach of contract.

References

1. CrowdStrike Stock: Is 'Kitchen Sink' Guidance Cut Coming Amid Crisis? https://www.investors.com/news/technology/crowdstrike-stock-crowdstrike-earnings-kitchen-sink-guidance-cut
2. Widespread IT Outage Due to CrowdStrike Update https://www.cisa.gov/news-events/alerts/2024/07/19/widespread-it-outage-due-crowdstrike-update
3. CrowdStrike Outage Drained $5.4 Billion From Fortune 500: Report https://www.informationweek.com/cyber-resilience/crowdstrike-outage-drained-5-4-billion-from-fortune-500-report
4. CrowdStrike outage will cost Fortune 500 companies $5.4 billion in damages https://fortune.com/2024/08/03/crowdstrike-outage-fortune-500-companies-5-4-billion-damages-uninsured-losses/
5. Delta sues cybersecurity firm CrowdStrike over tech outage that canceled flights https://apnews.com/article/delta-airlines-crowdstrike-outage-lawsuit-43bb230d2edf235bb9f7928c4279fec2
6. CrowdStrike Swings to a Loss With Costs Tied to Massive Outage, Despite Revenue Gains https://www.investopedia.com/crowdstrike-q3-fy-2025-earnings-8751919
7. Southwest Airlines Saved From Global IT Outage Thanks To 32-Year-Old Microsoft System https://simpleflying.com/southwest-airlines-old-system-unaffected-it-outage/
8. Technical Details: Falcon Content Update for Windows Hosts https://www.crowdstrike.com/en-us/blog/falcon-update-for-windows-hosts-technical-details/
9. CrowdStrike issue impacting Windows endpoints causing a 0x50 or 0x7E error message on a blue screen https://www.asus.com/us/support/faq/1053681/
10. CrowdStrike's Falcon Sensor linked to Linux crashes, too https://www.theregister.com/2024/07/21/crowdstrike_linux_crashes_restoration_tools/

TOYOTA | 2023

Threat actor	Threat	Vulnerabilities	Technical impacts	Business Impacts	Controls
Internal Toyota's internal IT or cloud management teams that configured and managed cloud storage. No evidence of malicious intent existed, but operational missteps contributed to prolonged exposure. **External** Not applicable. No external adversary or malicious threat actor was identified. However, prolonged exposure increases the risk of exploitation by external actors (e.g., opportunistic hackers).	**Prolonged exposure of sensitive data due to a misconfigured cloud storage environment** The significant risks include unauthorized access, data exfiltration, and potential misuse of sensitive customer and vehicle information.	*TT1- Misconfiguration and Inadequate Change Control* Cloud configurations were set to public access, exposing sensitive data. *TT2- Identity and Access Management* Insufficient enforcement of least privilege and strong authentication allowed broader risk exposure. *TT4- Inadequate Cloud Security Strategy* Lack of routine audits and strategic oversight allowed misconfiguration to persist for a decade. *TT7- Accidental Cloud Disclosure* Sensitive data exposure was caused by human error in cloud management. *TT8- System Vulnerabilities* Unpatched software, outdated configurations, or inherent flaws in the system infrastructure may allow attackers to exploit vulnerabilities, further compounding the risks caused by misconfigurations and access control weaknesses. *TT9- Limited Cloud Visibility* Toyota lacked proper monitoring and visibility over its cloud environments for nearly a decade. *TT10 - Unauthenticated Resource Sharing* Sensitive cloud resources were exposed publicly without authentication, unintentionally disclosing sensitive data.	**Confidentiality** Sensitive user data, including vehicle location and identification numbers, was publicly exposed. **Integrity** No signs of data tampering were found, but weak controls and poor oversight undermined Toyota's ability to ensure the integrity of its systems and data. **Availability** While no direct availability impact occurred, incident response efforts strained operational resources temporarily.	**Financial** Costs incurred for investigation, remediation, and regulatory penalties. **Operational** Resources were diverted for incident response, disrupting normal operations. **Compliance** Anticipated regulatory scrutiny and potential penalties in Japan and other regions. **Reputational** Global criticism of Toyota's security practices damaged trust and brand reputation.	**Preventive** -CCC-03 -CCC-02 -HRS-11 -IAM-05 -IAM-14 -SEF-03 **Detective** -CCC-07 -IAM-08 -IVS-08 **Corrective** -A&A-06 -CCC-09 -IAM-01 -SEF-04

Attack Detail

During a recent investigation into Toyota's cloud environment conducted by a cloud service provider, it was discovered that part of the data was accessible externally due to incorrect cloud settings. Toyota did not clarify whether this investigation was part of a routine audit or a targeted special review. However, given the occurrence of related cloud security incidents both shortly before and after the May 2023 disclosure, it is

reasonable to consider the possibility that this investigation was triggered by broader concerns—potentially as part of a special audit or focused response to systemic cloud governance issues.

Threat Actor: No specific threat actor has been identified in Toyota's data leak incident. The root cause was human error in configuring the company's cloud settings. Unlike intentional cyberattacks by advanced persistent threats or hacking groups, this breach resulted from an internal misconfiguration. However, the prolonged exposure of sensitive data (from November 2013 to mid-April 2023) suggests a lack of oversight, and persistent vulnerabilities in Toyota's data management processes increased the risk of exploitation by external actors (e.g., opportunistic hackers).

Threat: The misconfigured cloud storage exposed sensitive data related to Toyota's T-Connect cloud service and Lexus's G-Link service for approximately 2.15 million users in Japan. The data included vehicle location information, identification numbers, and potentially personal user data. While there have been no reports of malicious exploitation, the public accessibility of this data for nearly a decade raises significant concerns about privacy risks and potential misuse if accessed by malicious actors.

Vulnerabilities: The Toyota data leak incident revealed several critical vulnerabilities contributing to the breach. A significant factor was human error in cloud configuration, where inadequate controls led to the exposure of sensitive data over an extended period. This issue was further exacerbated by a lack of monitoring and routine security audits, allowing the misconfiguration to persist undetected for nearly a decade. The incident also highlights a broader industry challenge of cloud mismanagement, as misconfigured cloud environments remain a prevalent concern across organizations. Additionally, the breach underscores the need for improved employee training in data management and security governance structures to mitigate similar risks in the future.

Technical Impacts

Confidentiality: Sensitive user data, including vehicle location data, vehicle identification numbers, and customer details, was exposed. Toyota has reported no evidence of malicious use, but the extent of the data's visibility raises concerns about privacy and potential long-term risks.

Integrity: No unauthorized modification or tampering of Toyota's systems or customer data was detected. However, the prolonged misconfiguration exposed weaknesses in data integrity safeguards—such as insufficient access controls, lack of policy enforcement, and missing audit mechanisms—that could have allowed for undetected alterations or corruption of data.

Availability: Toyota's cloud services and customer-facing operations were not significantly impacted. However, incident response efforts and data investigation activities may have temporarily diverted resources.

Business Impacts

Financial: While Toyota did not experience an immediate stock decline directly linked to the breach, the incident has significant financial implications that, to date, have not been quantified. The costs associated with investigating the root cause, implementing remediation efforts such as enhanced monitoring and employee training, and conducting comprehensive audits are substantial. The breach raises long-term concerns about regulatory scrutiny, potential fines, and legal liabilities, which could impact future financial performance. The erosion of customer trust may also influence sales and brand loyalty, further adding to the potential financial repercussions.

Operational: The breach required Toyota to reallocate resources toward incident response efforts, including investigating the root cause, assessing the extent of the exposure, and implementing immediate remediation measures. These efforts temporarily disrupted normal business operations, as technical teams were diverted to manage the fallout and ensure the security of cloud systems.

Compliance: Toyota publicly apologized for the breach and issued official statements to inform the public about the incident. While no immediate regulatory actions or fines have been reported, the company is expected to face heightened regulatory scrutiny in Japan (Japan's Act on the Protection of Personal Information (APPI)) and possibly other regions for failing to safeguard customer data. The prolonged exposure of sensitive information raises the likelihood of investigations and enforcement actions. Past incidents in the industry suggest that Toyota could encounter increased regulatory oversight and potential penalties in the future as authorities evaluate the adequacy of its security practices.

Reputational: The incident drew global attention and criticism, particularly for the prolonged exposure of sensitive data. News outlets such as Reuters, DarkReading, and The Stack covered the breach extensively, emphasizing the scale and duration of the misconfiguration. The event tarnished Toyota's reputation as a leading innovator in the automotive sector, raising questions about its cybersecurity maturity.

Controls - Preventive Mitigation

CCC-03: Change Management Technology – Manage the risks associated with applying changes to organizational assets, including cloud configurations, applications, and systems, whether managed internally or externally. Toyota's prolonged misconfiguration highlights the importance of using automation tools—such as Infrastructure as Code (IaC) frameworks like Terraform and AWS CloudFormation—along with IaC scanners, to enforce secure configurations during deployment and prevent long-term security gaps.

CCC-02: Configuration Hardening – Establish secure configuration baselines for all cloud environments and infrastructure, ensuring approved changes conform to these standards. The lack of enforcement in Toyota's case demonstrates how misconfigurations can persist for years, leaving sensitive data exposed.

HRS-11: Security Awareness Training – Establish regular training programs for employees focused on cloud security, proper data management, and recognizing configuration-related risks to reduce human error include hands-on labs and simulations in training programs to reinforce cloud security best practices. Toyota's case highlights how operational missteps in cloud security can result in prolonged data exposure.

IAM-05: Least Privilege – When granting access to cloud systems and networks, apply the least privilege principle. Toyota's security lapse shows how excessive permissions can expand the attack surface, making access controls crucial to reducing risk.

IAM-14: Strong Authentication – Define and implement multifactor authentication to ensure secure access to cloud environments and applications. The lack of strong authentication, as seen in Toyota's incident, increases the likelihood of unauthorized access to misconfigured cloud systems.

SEF-03: Incident Response Plans – Establish and maintain incident response plans that account for cloud-specific risks, including misconfigurations, to ensure proactive readiness. Toyota's extended exposure period underscores the need for well-coordinated escalation procedures with cloud providers and third-party consultants.

Controls - Detective Mitigation

CCC-07: Detection of Baseline Deviation – Implement proactive measures to detect deviations from established secure configurations. Toyota's failure to identify its misconfiguration for nearly a decade reinforces the need for automated alerts to rapidly detect security gaps.

IAM-08: User Access Review – Review and revalidate user access permissions regularly to maintain least privilege and prevent unauthorized access to sensitive cloud configurations. The extended risk in Toyota's case highlights how inadequate privilege reviews allow security lapses to persist unnoticed.

IVS-08: Logging and Monitoring – Implement robust logging and real-time monitoring for all cloud environments using tools like AWS CloudTrail or Azure Monitor to promptly detect suspicious activities and misconfigurations. Toyota's prolonged exposure illustrates the consequences of insufficient logging and the need for real-time visibility.

Controls - Corrective Mitigation

A&A-06: Remediation – Develop and maintain a risk-based corrective action plan to address gaps identified in incident responses. Toyota's case emphasizes applying lessons from past misconfigurations to prevent recurring security failures.

CCC-09: Change Restoration – Define and implement a process to proactively roll back changes to a previously known good state in case of errors or security concerns. The lack of rollback mechanisms in Toyota's cloud security approach allowed misconfigurations to remain in place for years without remediation.

IAM-01: Identity and Access Management Policy and Procedures – Document, approve, and maintain identity and access management policies to ensure consistent and secure practices. Toyota's incident highlights how weak IAM enforcement can result in excessive permissions that contribute to prolonged security risks.

SEF-04: Incident Response Testing – Develop and routinely test incident response plans tailored to cloud breaches. Toyota's security failures illustrate the importance of regular testing to ensure rapid detection and response to misconfigurations before they persist.

Metrics

Key Performance Indicators

- Access Provisioning Compliance Rate: Percentage of Toyota's cloud accounts and automated processes configured with least privilege access controls and MFA enforcement.
- Detection of Baseline Deviation: Percentage of Toyota's cloud environments where security settings deviated from approved configuration baselines, detected by audits or automated tools.
- Logging and Monitoring Coverage: Percentage of Toyota's cloud environments enabled by real-time logging, monitoring, and anomaly detection.
- Mean-Time-to-Detect (MTTD): Average time taken to detect misconfigurations, unauthorized access attempts, or cloud security incidents in Toyota's environment.

Control Effectiveness Measurements

- Cloud Configuration Compliance Rate: Percentage of Toyota's cloud assets (storage, networks, applications) that adhere to security configuration baselines.
- Audit and Access Review Coverage: The percentage of Toyota cloud accounts and access controls was reviewed and adjusted to the least privilege during security audits.
- Unauthorized Access Attempt Rate: Percentage of unauthorized access attempts to Toyota's cloud environments successfully blocked by authentication and access controls.
- Mean-Time-to-Remediate (MTTR): Average time to correct security misconfigurations in Toyota's cloud environments from detection to resolution.

Key Takeaways

- Toyota's data leak highlights the need for better cloud oversight: The Toyota data leak highlights the need for stronger oversight and proactive management of cloud configurations. Misconfigurations caused by operational missteps within Toyota's internal teams exposed sensitive data for nearly a decade, showing the importance of governance programs ensuring continuous monitoring, visibility, and control.
- Automated cloud monitoring and audits can prevent misconfigurations: Advanced cloud configuration monitoring, audits, and assessments using automation and machine learning can efficiently detect and reduce manual effort. Toyota's prolonged exposure resulted from the lack of automated monitoring systems, showing that reliance on manual processes risks overlooking critical gaps.
- Weak cloud governance exposes sensitive data: Systemic challenges in cloud governance, such as inadequate routine audits and monitoring, leave sensitive data vulnerable to prolonged exposure. Toyota's misconfiguration, which persisted undetected for nearly a decade due to insufficient audit processes and weak monitoring protocols, emphasizes the need for robust governance frameworks.
- Strong IAM practices, including least privilege and MFA, are critical: Enhanced identity and access management practices, including enforcing least privilege and implementing multifactor authentication, are critical to reducing the risks of future data leaks. Insufficient access controls, such as not enforcing MFA or least privilege, widened Toyota's attack surface, showing the importance of strong IAM practices.

References

1. More than 2 million Toyota users face the risk of vehicle data leak in Japan
   https://www.reuters.com/business/autos-transportation/toyota-flags-possible-leak-more-than-2-mln-users-vehicle-data-japan-2023-05-12

2. Apology & Notice Concerning Newly Discovered Potential Data Leakage of Customer Info Due to Cloud Settings
   https://global.toyota/en/newsroom/corporate/39241625.html

3. Yet Another Toyota Cloud Data Breach Jeopardizes Thousands of Customers
   https://www.darkreading.com/ics-ot-security/toyota-cloud-data-breach-jeopardizes-thousands-customers

4. Toyota spewed vehicle location data for millions onto unsecured cloud databases for ten years
   https://www.thestack.technology/toyota-data-breach-2023-t-connect-cloud
   https://www.techradar.com/pro/security/toyota-confirms-data-breach-after-info-leaked-on-cybercrime-forum

5. Toyota confirms another years-long data leak, this time exposing at least 260,000 car owners' information
   https://techcrunch.com/2023/05/31/toyota-customer-data-leak-years

DARKBEAM | 2023

Threat actor	Threat	Vulnerabilities	Technical impacts	Business Impacts	Controls
Internal The Elasticsearch and Kibana instances were exposed to the public internet, potentially due to binding the service to a public-facing IP address instead of a private or localhost IP or leaving the default configuration (no authentication or authorization). (IAM-12) **External** Not applicable. No external adversary or malicious threat actor was identified. However, prolonged exposure increases the risk of exploitation by external actors (e.g., opportunistic hackers).	*TT7- Accidental Data Disclosure* The Darkbeam incident involved the public exposure of over 3.8 billion email-password combinations due to a misconfigured Elasticsearch and Kibana interface. While there is no confirmed evidence of unauthorized exfiltration, the public accessibility of the data posed a significant risk.	*TT3- Misconfiguration and Inadequate Change Control* The primary issue was an unsecured database configuration, exposing sensitive data to the public. *TT1- Insufficient Identity, Credential, Access, and Key Management* Passwords stored in plaintext or without sufficient encryption exacerbated risks.	*TT8- Accidental Cloud Data Disclosure* The use of cloud-hosted systems without proper safeguards amplified the potential for data exposure.	**Financial** The acquisition by apexanalytix shortly after the incident suggests that the breach did not significantly impact Darkbeam's valuation or derail the transaction, indicating limited financial fallout. **Operational** The exposure was detected externally, rather than through internal security monitoring, highlighting gaps in misconfiguration detection and proactive cloud security posture. **Compliance** No known penalties or legal actions have been reported. **Reputational** The exposure received limited media coverage, mostly within cybersecurity circles, reducing widespread reputational damage.	**Preventive** -CCC-03 -IAM-04 -IVS-03 -NET-03 **Detective** -CCC-07 -LOG-01 **Corrective** -A&A-06 -CCC-02 -IAM-01 -CCC-10

Attack Detail

Threat Actor: No specific external threat actor has been identified in the Darkbeam data exposure. The threat was discovered by Bob Diachenko, CEO of SecurityDiscovery. Instead, the root cause was an internal failure to secure an Elasticsearch and Kibana interface (TT1 - Misconfiguration and Inadequate Change Control). This misconfiguration made the interface publicly accessible without authentication or authorization, creating an opportunity for exploitation by opportunistic actors. While there is no confirmed evidence of data exfiltration, the misconfigured system potentially exposed over 3.8 billion email-password combinations, some sourced from previous breaches and others of unknown origin. If malicious actors discovered the database before it was secured, the credentials could have been harvested for use in black market sales, credential stuffing, and other cybercrimes.

Threat: The public exposure of the Elasticsearch and Kibana interface was the result of a misconfiguration, likely during deployment or maintenance. The interface was bound to a public-facing IP address and lacked authentication, allowing unrestricted access. The dataset contained sensitive information, including email-password combinations, some of which may have been stored in plaintext or weakly hashed, exacerbating the risks. Threat actors could have easily discovered the exposed interface using automated scanning tools, which routinely identify misconfigured services exposed on the internet.

Vulnerabilities: The Darkbeam exposure was primarily caused by Misconfiguration and Inadequate Change Control (TT3), as the Elasticsearch instance was publicly accessible due to improper IP binding and a failure to apply authentication and role-based access controls (RBAC). Insufficient Identity, Credential, and Access Management (TT2) contributed to the risk, as there were no authentication mechanisms in place to restrict access, and sensitive data may not have been encrypted. Additionally, Accidental Cloud Data Disclosure (TT7) played a role, as the misconfiguration was likely an oversight in deployment or maintenance processes, reflecting inadequate security policies and review procedures. Lastly, System Vulnerabilities (TT8) were exacerbated by the aggregation of sensitive credentials from multiple breaches, making the exposed system a high-value target for attackers seeking to exploit reused credentials.

Technical Impacts

Confidentiality: The public accessibility of sensitive credentials created risks of unauthorized access, credential stuffing, and account takeovers.

Integrity: Although no evidence of data tampering was reported, the aggregation of data from disparate breaches may have included falsified or manipulated records.

Availability: No availability issues were directly reported, but the exposure may have led to diminished trust in Darkbeam's services.

Business Impacts

Confidentiality: The Darkbeam data exposure does not appear to have resulted in immediate financial losses, fines, or lawsuits. The acquisition by apexanalytix shortly after the incident suggests that the breach did not significantly impact Darkbeam's valuation or derail the transaction, indicating limited financial fallout.

Operational: The exposure was detected externally, rather than through internal security monitoring, highlighting gaps in misconfiguration detection and proactive cloud security posture. However, the swift acquisition by apexanalytix suggests minimal disruption to Darkbeam's operations, as the incident did not delay or complicate the transition.

Compliance: No regulatory penalties or legal actions have been reported, but compliance risks remain if the exposed data falls under GDPR, CCPA, or other data protection laws. The apexanalytix acquisition could result in a compliance reassessment, as the new parent company may enforce stricter data security and regulatory oversight.

Reputational: The exposure received limited media coverage, mostly within cybersecurity circles, reducing widespread reputational damage. However, for a company specializing in digital risk protection, the incident could raise concerns about its security practices.

Controls - Preventive Mitigation

CCC-03: Change Management Technology – This control ensures that changes to cloud configurations, infrastructure, and access controls are managed securely, reducing the risk of accidental misconfigurations. Had CCC-03 been properly implemented, Darkbeam's Elasticsearch and Kibana instances would have undergone security validation before deployment, preventing them from being exposed to the public internet without authentication.

IAM-04: Unauthorized Access Prevention – IAM-04 mandates strong authentication and authorization controls to prevent unauthorized access to cloud services. The lack of authentication on the Darkbeam database meant anyone could access the exposed credentials. Proper enforcement of IAM-04 would have required authentication mechanisms, such as role-based access control or API key restrictions, ensuring that only authorized personnel could access the system.

IVS-03: Network Access Control – IVS-03 requires organizations to implement network access controls to restrict connectivity to authorized entities and isolate systems based on sensitivity and trust level. In the Darkbeam case, Elasticsearch and Kibana were bound to a public-facing IP address with no access restrictions. Proper application of IVS-03 would have ensured that these services were isolated from the public internet using firewall rules, private subnets, or VPN gateways, reducing the risk of unauthorized exposure.

NET-03: Network Segmentation – Enforce network segmentation to isolate cloud resources, limiting the blast radius of potential breaches. Implementing network segmentation ensures that the Elasticsearch and Kibana instances are placed in a separate network segment, preventing direct access from the public internet and reducing the risk of unauthorized access.

Controls - Detective Mitigation

CCC-07: Detection of Baseline Deviation – This control emphasizes monitoring for unexpected changes in cloud configurations to detect security misconfigurations in real time. In the Darkbeam exposure, the public-facing access should have triggered an alert, allowing security teams to remediate the issue before an external researcher discovered it. Implementing CCC-07 would have enabled continuous security posture monitoring to flag unauthorized exposure.

LOG-01: Centralized Logging and Monitoring – Implementing centralized logging and monitoring to aggregate logs from all cloud resources, including Elasticsearch and Kibana instances. This enables real-time analysis of access patterns and configuration changes, facilitating the early detection of misconfigurations and unauthorized access attempts.

Controls - Corrective Mitigation

A&A-06: Remediation – This control mandates a structured remediation process to address security gaps and prevent recurrence. Once the Darkbeam exposure was discovered, an effective A&A-06 framework would have required a root cause analysis, updates to configuration policies, and a plan to prevent future unauthorized public access to cloud assets.

CCC-02: Configuration Security Management – CCC-02 ensures secure configuration management for cloud-hosted services, enforcing best practices such as default security settings, encryption, and proper access control policies such as mandating password rotation and enforcing strong password policies. In this case, if CCC-02 had been followed, the Elasticsearch and Kibana instances would have been configured securely from the start, reducing the risk of accidental exposure.

IAM-01: Identity and Access Management Policy and Procedures – IAM-01 focuses on establishing and enforcing IAM policies that define how access controls are implemented, reviewed, and maintained. The Darkbeam incident suggests a lack of strong IAM policies, as no authentication or access restrictions were applied. Implementing IAM-01 would require documenting security policies, enforcing authentication standards, and conducting regular compliance checks to prevent similar incidents in the future.

CCC-10: Configuration Rollback – Implement configuration rollback mechanisms to quickly revert to a known good configuration in the event of a misconfiguration or security incident. This ensures that the Elasticsearch and Kibana instances can be rapidly restored to a secure state, minimizing the exposure window and potential impact.

Metrics

Key Performance Indicators

- Incident Discovery Source: This incident highlights that the exposure was discovered externally, a metric that organizations should aim to minimize through internal detection mechanisms.
- Unauthorized Access Attempts: No known metrics exist for the number of unauthorized access attempts or whether malicious actors accessed the database before it was secured.
- Percentage of Encrypted Data: It is unclear whether the credentials in the database were stored in plaintext or encrypted. The absence of this information suggests an opportunity to establish encryption compliance as a KPI moving forward.

Control Effectiveness Measurements

- Misconfiguration Detection Rate: The misconfiguration (public-facing IP and lack of authentication) was not detected internally, pointing to gaps in automated scanning or manual audits.
- Access Control Effectiveness: The absence of access controls (e.g., authentication and role-based permissions) allowed unrestricted public access to the database.
- Audit Frequency of Cloud Configurations: No evidence suggests regular audits of cloud configurations were performed, a critical gap in Darkbeam's security program.
- Incident Escalation Time: Diachenko's prompt notification and Darkbeam's swift action highlight an effective escalation and remediation process once the exposure was brought to their attention.

Key Takeaways

- Misconfiguration risks are a leading threat: This incident highlights the critical need for robust configuration management processes. Public-facing misconfigurations remain one of the most significant contributors to cloud data exposures.
- Proactive monitoring is essential: A lack of monitoring allowed this exposure to persist until discovered by a third-party researcher. Organizations must invest in continuous monitoring tools such as Security Information and Event Management (SIEM) to prevent similar breaches.
- Supply chain implications: As a digital risk provider, Darkbeam's incident serves as a reminder that supply chain partners managing sensitive data must uphold the highest standards of security. The downstream risks of poorly managed data can affect all parties in the ecosystem.
- Aggregate breach data requires enhanced safeguards: Organizations aggregating data from external breaches must implement strict access controls, encryption, and regular audits to ensure this high-risk data does not itself become a target.
- Strategic focus on cloud security architecture and identity management: This case emphasizes the importance of addressing systemic security design issues by enforcing identity and access management policies (IAM-01), securing cloud services from public exposure (IAM-12), and ensuring proper remediation processes (A&A-06). Implementing automated security controls, periodic policy reviews, and technical training for cloud engineers can prevent similar incidents in the future.

References

1. More than 2 million Toyota users face the risk of vehicle data leak in Japan
   https://www.reuters.com/business/autos-transportation/toyota-flags-possible-leak-more-than-2-mln-users-vehicle-data-japan-2023-05-12

2. Apology & Notice Concerning Newly Discovered Potential Data Leakage of Customer Info Due to Cloud Settings
   https://global.toyota/en/newsroom/corporate/39241625.html

3. Yet Another Toyota Cloud Data Breach Jeopardizes Thousands of Customers
   https://www.darkreading.com/ics-ot-security/toyota-cloud-data-breach-jeopardizes-thousands-customers

4. Toyota spewed vehicle location data for millions onto unsecured cloud databases for ten years
   https://www.thestack.technology/toyota-data-breach-2023-t-connect-cloud
   https://www.techradar.com/pro/security/toyota-confirms-data-breach-after-info-leaked-on-cybercrime-forum

5. Toyota confirms another years-long data leak, this time exposing at least 260,000 car owners' information
   https://techcrunch.com/2023/05/31/toyota-customer-data-leak-years

RETOOL & FORTRESS | 2023

Threat actor	Threat	Vulnerabilities	Technical impacts	Business Impacts	Controls
Internal An employee fell victim to a combination of social engineering attacks, providing the threat actor with their credentials and MFA token. **External** An unknown threat actor infiltrated Retool's environment.	**Opportunistic** The threat actor took advantage of Retool's migration to Okta, using this transition to make their phishing emails and credential harvesting website appear legitimate.	*TT1- Misconfiguration and Inadequate Change Control* The threat actor was able to add a new MFA device to the employee's account, giving them persistent access. *TT2- Identity & Access Management (IAM)* Smishing, credential harvesting, and vishing led to the attacker obtaining authentication information. *TT5- Insecure Third-Party Resource* New features were introduced to Google Authenticator, which led to the employee's MFA tokens being synchronized to the cloud.	**Confidentiality** The attacker gained access to multiple applications within Retool's environment, as well as customer data and accounts. **Integrity** The email addresses and passwords of 27 customer accounts were modified. **Availability** Impacted customers were unable to access their accounts until Retool reversed the changes.	**Financial Loss** Due to the Retool breach, one of their customers, Fortress, suffered a loss of $15 million USD worth of cryptocurrency. **Operational** During the remediation phase, some customers were unable to access the Retool SaaS platform. **Compliance** There were no compliance violations reported. **Reputational Damage** Both Retool and their customers suffered reputational damage as the breach resulted in the theft of customer assets.	**Preventive** -IAM-04 -AM-05 -TVM-07 -CCC-04 -CCC-06 -HRS-11 **Detective** -CCC-07 -LOG-05 -IAM-08 **Corrective** -CCC-09 -DSP-17 -SEF-03

Attack Detail

Threat Actor: While the identity of those responsible for the breach has not been disclosed, it is suspected that it was carried out by the financially motivated group Scattered Spider (UNC3944), due to similar tactics used during the initial compromise.

Threat: The threat actor launched a sophisticated social engineering campaign involving smishing, credential harvesting, and vishing tactics, which led to an employee disclosing their one-time password (OTP) token. Armed with the employee's credentials and OTP token, the threat actor infiltrated Retool's environment, linked their device to the employee's Okta account, and gained ongoing access to the employee's Google account.

By exploiting a feature in Google Authenticator that syncs MFA tokens to the cloud, the threat actor gained access to additional MFA tokens, including one that allowed them to connect to Retool's VPN and access their admin systems. From there, they took over customer accounts, changing associated email addresses and resetting user passwords.

Vulnerabilities: The threat actor took advantage of Retool's migration to a new authentication platform, which allowed them to launch a more believable social engineering campaign. There were also no technical controls preventing unauthorized MFA devices from being added to an employee's account. Lastly, Retool failed to thoroughly review the Google Authenticator application, which led to the employee's MFA codes being synced to the cloud.

Technical Impacts

Confidentiality: The threat actor compromised the employee's admin account, granting them access to Retool's internal systems, applications, and sensitive data.

Integrity: The compromised employee's account was modified to add an unauthorized MFA device. The threat actor was also able to alter the information of 27 SaaS-based customer accounts, including their credentials.

Availability: Availability impacts were limited to SaaS based customers who may have been unable to access their accounts when their credentials were changed.

Business Impacts

Financial: Retool has not disclosed the total financial impact of the breach, but they likely faced costs associated with hiring a third-party forensics firm to investigate the incident. Additionally, one of Retool's customers, Fortress, suffered financial loss due to this incident, as the threat actor was able to steal $15 million USD worth of cryptocurrency.

Operational: The breach led to disruptions for both employees and customers. During the remediation phase, Retool took several actions: revoking internal authenticated sessions for employees, isolating the affected customer accounts, and notifying customers of the breach. Once the immediate concerns were addressed, they spent time reverting the changes made by the threat actor.

Compliance: There were no reported compliance violations relating to this breach.

Reputational: The breach was reported in several news outlets, resulting in Retool publishing a blog post explaining what happened. This could have affected existing and potential customers' confidence in Retool's ability to secure their systems and data.

Controls - Preventive Mitigation

IAM-04: Separation of Duties – No controls were in place to prevent the threat actor from adding a new MFA device to the compromised account. An additional step should have been implemented, requiring IT to review and approve any such change before it was allowed.

IAM-05: Least Privilege – A process should be implemented to prevent unauthorized customer data modification. Since the admin account could modify customer data, the threat actor was able to reset customer credentials, gaining full access to the affected customer accounts.

TVM-07: Vulnerability Identification – Critical third-party applications should be frequently reviewed to identify new features and their associated vulnerabilities. If Retool had identified the change Google made early on, they could have prevented the breach by ensuring their employees had turned cloud synchronization off or using an alternative OTP solution.

CCC-04: Unauthorized Change Protection – Technical controls should be in place to prevent unauthorized changes to accounts and systems. In Retool's case, this would include restricting employees' ability to add new MFA devices to their accounts without proper verification.

CCC-06: Change Management Baseline – A baseline should be established for user accounts, ensuring that all of the devices associated with the account are approved.

HRS-11: Security Awareness Training – Conduct regular training sessions to educate employees of the latest social engineering techniques.

Controls - Detective Mitigation

CCC-07: Detection of Baseline Deviation – Implement controls to detect deviations from established baselines. The addition of an unauthorized MFA device to the employee's account should have been flagged for review.

LOG-05: Audit Log Monitoring and Response – The employee's admin account was used to modify customer data, which could have signaled unusual activity for that account. Implementing monitoring to detect and alert such abnormal behavior could have helped identify the breach earlier.

IAM-08: User Access Review – Implement a process to frequently review and revalidate user least privilege access and separation of duty. This would help identify user accounts with access to data, applications, systems, and permissions that are not required for their role.

Controls - Corrective Mitigation

CCC-09: Change Restoration – Define and implement a process to proactively roll back changes to a previously known good state in case of errors or security concerns. This would ensure that Retool could quickly restore the customers' and employees' accounts to their original state.

DSP-17: Sensitive Data Protection – Implement procedural and technical measures to ensure that customer data cannot be modified without their approval.

SEF-03: Incident Response Plans – Establish a security incident response plan to ensure the response team is prepared to effectively handle and mitigate security incidents

Metrics

Key Performance Indicators

- User Education: The number of times security awareness training is updated within a year to include new threats and attack techniques.
- Security Awareness Training: The frequency of employees taking security awareness training and the percentage of those who have not completed it.
- Mean-Time-to-Detect (MTTD): The average time it takes to identify insecure misconfigurations affecting third-party applications.
- Mean-Time-to-Remediate (MTTR): The average time to address known insecure misconfigurations affecting third-party applications.
- Baseline Deviation Detection Rate: The percentage of assets that have deviated from the configuration baseline.

Control Effectiveness Measurements

- Reported Suspicious Activity: The number of employees who report suspicious activity such as phishing, vishing, or smishing.
- Social Engineering Tests: The percentage of employees who fell for social engineering tests and how many were repeat offenders.
- IAM Access Reviews: The percentage of privileged accounts audited to ensure they only have access to systems and data they need.
- Application Reviews: The percentage of applications assessed for vulnerabilities, misconfigurations, and security risks.

Key Takeaways

- The Retool breach highlights the risks of fully trusting third-party tools for internal authentication, as unexpected changes can impact security. If you rely on tools like Google Authenticator for OTPs, routinely review vendor/application updates for new potential security risks.
- Emerging technologies like deepfakes are making social engineering attacks more effective. In this breach, the threat actor used a deepfake voice to impersonate a Retool employee, leading the victim to lower their guard and reveal their OTP. Regular security awareness training and simulated social engineering tests can help employees better recognize and resist such threats.
- SaaS applications introduce additional risks, especially when used for critical operations. Retool's customers relied on them for security, yet the attacker could access and modify their data using the compromised admin account. If you use SaaS-based applications, conduct thorough vendor and application reviews to understand how the vendor handles access to your account and data.
- Effective change management controls need to be implemented to detect, alert, and prevent unauthorized changes within your environment.

References

1. When MFA isn't actually MFA
   https://retool.com/blog/mfa-isnt-mfa

2. Phishing Attack on Cloud Provider With Fortune 500 Clients Led to $15M Crypto Theft From Fortress Trust
   https://www.coindesk.com/business/2023/09/13/phishing-attack-on-cloud-provider-with-fortune-500-clients-led-to-15m-crypto-theft-from-fortress-trust

3. Identity of Ripple's Fortress Trust Hacker Who Stole $15 Million in Crypto Revealed
   https://u.today/identity-of-ripples-fortress-trust-hacker-who-stole-15-million-in-crypto-revealed

4. Retool Falls Victim to SMS-Based Phishing Attack Affecting 27 Cloud Clients
   https://thehackernews.com/2023/09/retool-falls-victim-to-sms-based.html

FTX | 2022

Threat actor	Threat	Vulnerabilities	Technical impacts	Business Impacts	Controls
External A group of 3 individuals without affiliation to FTX organized a SIM swap attack, seeking monetary gain.	**Monetary Theft** Reliance on two-factor authentication (2FA) with an OTP and SMS-based reset offered a relatively unsophisticated attack vector. FTX had no compensating identity management controls in place *(TT2)*, nor did FTX have embedded controls in its software to prevent unauthorized funds transfers *(TT6)*.	*TT2- Insufficient Identity, Credentials, Access, Key Management* 2FA-enabled account takeover. *TT6- Misconfiguration and Inadequate Change Control* 2FA was sufficient to grant enough access to enable money transfer.	**Confidentiality** Victims were not named, but keys and wallets were compromised. **Integrity** System in freefall and integrity uncertain. **Availability** Site pulled offline by legal actions; accounts were frozen.	**Financial** Major liquidity crisis forced FTX into Chapter 11 bankruptcy. **Operational** FTX accounts were frozen and ceased operations until liquidation under court supervision. **Compliance** The CEO was arrested and jailed partly due to lack of reasonable controls and lack of compliance with U.S. law. **Reputational** FTX ceased operating and has become a symbol of fraud, though its collapse did not undermine the crypto economy.	**Preventive** -IAM-06 -IAM-14 -CCC-04 -CCC-06 -HRS-11 **Detective** -CCC-07 -IAM-08 -IVS-09 -LOG-03 **Corrective** -A&A-06 -CCC-09 -SEF-03 -CEK-12 -BCR-08

Attack Detail

Several weak security measures, including SMS-based 2FA and limited cloud platform controls, enabled attackers to steal approximately $400 million USD worth of crypto assets within hours. The FTX Group did not have effective controls to detect or stop the compromise, leaving billions of dollars of additional assets at risk. The attackers accessed FTX's always-connected hot wallets, secret keys, and critical systems by exploiting FTX's reliance on OTP resets through SIM swapping. Once inside, they escalated privileges and transferred funds while remaining undetected.

Threat Actor: Unknown for the first year after the breach, in September 2023, an indictment was brought against three criminal co-conspirators (one of whom pleaded guilty, while the other two currently await trial). On January 24, 2024, the United States Attorney's Office for the District of Columbia unsealed an indictment, captioned United States v. Powell et al., following the arrest of the defendants named in that case (Robert Powell, Carter Rohn, and Emily Hernandez).

Threat: FTX's reliance on SMS-based 2FA provided a weak attack vector for credential resets, as the company lacked compensating controls (TT2) such as risk-based authentication and role-based access. FTX also did not implement adequate transaction monitoring or multi-level approval workflows (TT6), enabling attackers to authorize large-scale fund transfers without intervention.

Vulnerabilities: FTX was vulnerable to a SIM swap attack, in which attackers impersonated legitimate users and convinced the mobile carrier to transfer the victim's phone number to a new SIM card. This allowed the attackers to intercept OTPs, reset account credentials, and access FTX's cloud systems and wallets. Once the attackers had access, they exploited poor key management and insufficient internal segmentation, allowing lateral movement and broad access to funds.

Technical Impacts

Confidentiality: None of the victims have been named; however, the theft compromised the confidentiality of FTX's secret keys and wallet access credentials, leading to unauthorized transfers of over $400 million USD in crypto assets.

Integrity: The FTX platform has remained in bankruptcy as investigators still seek to identify and recapture some of the stolen assets. It appears from the court filings that the system integrity remained intact and that all the victims are identifiable, but the money transferred out of the exchange has been sent through several bitcoin mixers to remove any possibility of non-repudiation (tracing funds sent through mixers is currently a very challenging effort). The theft of private keys and the unauthorized execution of transactions raised integrity concerns in financial records.

Availability: Although FTX claimed the hack did not directly disrupt system uptime or operations, legal actions temporarily restricted exchange and customer funds access.

Business Impacts

Financial: The theft of over $400 million USD resulted in a major liquidity crisis that forced FTX into Chapter 11 bankruptcy.

Operational: The U.S. Bankruptcy Court for the District of Delaware appointed new FTX management. The new team transferred some funds to offline (cold) wallets to prevent additional losses. Customer accounts were frozen pending the investigation. The exchange and all of its funds were frozen through bankruptcy. Then, it was announced in October 2024 that the court-approved bankruptcy plan would provide a full refund, plus interest, for former FTX customers,mainly due to an enormous rise in the price of cryptocurrencies since the bankruptcy filing.

Compliance: The CEO was arrested and sentenced partly due to a lack of reasonable controls or compliance with U.S. law.

Reputational: Newly appointed CEO John Ray filed a statement with the Bankruptcy Court stating, "Never in my career have I seen such a complete failure of corporate controls and such a complete absence of trustworthy financial information as occurred here." Note: FTX's reputation may end up somewhat rehabilitated after all the customers receive full reimbursement. Still, those reimbursement funds result from a fortuitous rise in the price of crypto, not the proper custodial actions of the former management team.

Controls - Preventive Mitigation

IAM-06: User Access Provisioning – FTX lacked controls for properly managing and restricting access to sensitive systems like hot wallets. Implementing a user access provisioning and deprovisioning process ensures that access is only granted to authorized personnel, reducing the likelihood of unauthorized users gaining access to critical systems. This process includes regularly auditing user permissions and access rights to ensure compliance with the principle of least privilege and integrating access provisioning with HR systems to automatically revoke access upon employee termination.

IAM-14: Strong Authentication – Define and implement multifactor authentication to ensure secure access to cloud environments and applications. This reduces the likelihood of unauthorized access to misconfigured systems. OTP-based MFA has become less and less secure, requiring more effective methods such as passkeys or hardware security keys. Implement adaptive authentication that considers user behavior, location, and device posture to dynamically adjust authentication requirements.

CCC-04: Unauthorized Change Protection – Technical controls should be in place to prevent unauthorized changes to accounts and systems. In the case of FTX, this would have included restricting the ability to transfer funds out of accounts.

CCC-06: Change Management Baseline – A baseline should be established for user accounts, ensuring that all of the devices associated with the account are approved.

HRS-11: Training and Awareness – Human error (e.g., reliance on weak 2FA) played a major role in the FTX breach. Training would enhance staff awareness of risks associated with SIM swaps, privilege misuse, and fund transfer protocols.

Controls - Detective Mitigation

CCC-07: Detection of Baseline Deviation – Implement detection measures with proactive notification in case changes deviate from the established baseline, such as network shares, misconfiguration, and accessibility. A change in SIM card associations and OTPs from unfamiliar IPs and devices are deviations that could have been detected and rejected.

IAM-08: User Access Review – Review and revalidate user access for least privilege and separation of duties with a frequency commensurate with organizational risk tolerance. Consistent, periodic, access reviews can establish a baseline and then indicate deviations from that baseline.

IVS-09: Network Defense – The lack of sufficient defenses within FTX's network allowed attackers to access and move funds without being blocked. Implementing defense-in-depth techniques, such as monitoring for anomalous traffic and real-time threat detection, could help prevent or contain similar breaches.

LOG-03: Security Monitoring and Alerting – Identify and monitor security-related events within applications and the underlying infrastructure. Define and implement a system to generate alerts to responsible stakeholders based on such events and corresponding metrics.

Controls - Corrective Mitigation

A&A-06: Remediation – Establish, document, approve, communicate, apply, evaluate, and maintain a risk-based corrective action plan to remediate incident and breach case findings, lessons learned, and improvement plans findings. Review and report remediation status to relevant stakeholders. Banks have clawback processes in the event of unauthorized transfers. FTX had no recourse.

CCC-09: Change Restoration – Define and implement a process to proactively roll back changes to a previously known good state in case of errors or security concerns. This would have ensured that FTX could restore customer funds.

SEF-03: Incident Response Plans – Ensures that incidents involving unauthorized access or fund transfers trigger immediate containment and recovery steps, such as freezing accounts or halting transfers.

SEF-07: Security Breach Notification – Define and implement processes, procedures, and technical measures for security breach notifications. Report security breaches and assumed security breaches including any relevant supply chain breaches, as per applicable SLAs, laws, and regulations.

CEK-12: Key Rotation – FTX's compromised keys were never properly rotated, allowing attackers to maintain access to funds. Establishing key rotation policies based on cryptoperiods or detected threats would help limit the impact of compromised keys and prevent persistent access.

BCR-08: Backup (Recovery) – FTX's ability to recover critical customer funds was delayed due to poor backup and restoration processes. Periodically backing up sensitive financial data, keys, and configurations and ensuring their confidentiality, integrity, and availability would enable faster recovery after incidents.

Metrics

Key Performance Indicators

- Access Provisioning Compliance Rate: Percentage of user and programmatic accounts provisioned with least privilege and MFA enabled.
- Anomaly Detection Efficacy: Percentage of detected baseline deviations that result in actionable alerts.
- Baseline Compliance Coverage: Percentage of devices and accounts meeting established security baseline requirements, ensuring only authorized access.
- Mean-Time-to-Detect (MTTD): Average time taken to detect deviations from the established baseline, such as unauthorized access attempts or configuration changes.
- Mean-Time-to-Remediate (MTTR): Average time taken to remediate security incidents after detection, from initial containment to resolution.
- Training Completion Rate: Percentage of employees completing mandatory security awareness training.

Control Effectiveness Measurements

- Access Anomaly Detection Efficacy: Percentage of detected access anomalies that result in actionable alerts and investigations.
- Unauthorized Change Attempt Rate: Number of attempted unauthorized changes to critical system components, such as fund transfer processes, over a specified period.
- Change Restoration Success Rate: Percentage of successful restorations of systems and configurations to a known good state following detected incidents.
- Lessons Learned Implementation Rate: Percentage of corrective actions or security improvements implemented following post-incident reviews.

Key Takeaways

- 2FA is insufficient to prevent malicious actors from accessing accounts, and any financial institution holding money or crypto assets must protect deposits with substantially more security controls. Passkeys, hardware security keys, and/or biometric authentications are all current-generation approaches far superior to 2FA.
- Enhanced identity and access management practices, including enforcing least privilege and implementing MFA, are critical to reducing the risks of future data leaks. Insufficient access controls, such as not enforcing MFA or least privilege, widened FTX's attack surface, showing the importance of strong IAM practices. Regularly conduct access reviews and audits.
- To reduce the incidence of theft and restore trust, financial institutions must develop and maintain clawback processes, despite the incredible difficulty with Bitcoin and other similar financial instruments, or must otherwise insure their depositors, or they risk bankruptcy from a single successful hack.
- Strong corporate governance and effective internal controls are essential to detecting and mitigating security risks. Organizations must implement board-level cybersecurity oversight, conduct independent audits, and establish continuous monitoring to prevent large-scale breaches.
- Comprehensive incident response plans, tailored to crypto-specific risks, are crucial to limiting financial and operational damage. Organizations should prioritize rapid detection, containment, and recovery by developing playbooks that address hot wallet compromises, SIM swaps, and unauthorized transactions.

References

1. Bankrupt FTX's new CEO outlines fund abuses, untrustworthy records
   https://www.reuters.com/technology/new-ftx-ceo-slams-complete-failure-corporate-control-2022-11-17/

2. Public Cloud Security Breaches - FTX Bankruptcy
   https://www.breaches.cloud/incidents/ftx/

3. FTX Debtor Report Filed April 9, 2023
   https://www.scribd.com/document/637584994/FTX-debtor-report-filed-April-9-2023

4. Colorado Woman Pleads Guilty in SIM Swapping Scheme that Led to 400M FTX Crypto Hack
   https://blocktribune.com/colorado-woman-pleads-guilty-in-sim-swapping-scheme-that-led-to-400m-ftx-crypto-hack/

5. The FTX Hack: The Unsolved SIM Swap Mystery
   https://www.nasdaq.com/articles/the-ftx-hack:-the-unsolved-sim-swap-mystery

6. FTX Customers Will Get Back Billions After Judge OKs Bankruptcy Plan
   https://www.wired.com/story/ftx-bankruptcy-us-judge-confirms/

7. Samuel Bankman-Fried Sentenced to 25 Years for His Orchestration of Multiple Fraudulent Schemes
   https://www.justice.gov/opa/pr/samuel-bankman-fried-sentenced-25-years-his-orchestration-multiple-fraudulent-schemes

8. Case Study: FTX and Sam Bankman-Fried
   https://sevenpillarsinstitute.org/case-study-ftx-and-sam-bankman-fried/

MICROSOFT | 2024

Threat actor	Threat	Vulnerabilities	Technical impacts	Business Impacts	Controls
Internal An internal test account was accessed, which had access to an OAuth application with elevated access to Microsoft's corporate environment. **External** State-backed Cyber Espionage by Midnight Blizzard (aka Nobelium, or APT29) Stole email from leadership, cybersecurity, and legal teams.	**Data Theft** A test account had elevated access to Microsoft's corporate environment that allowed the threat actors elevation privileges to gain access to corporate mailboxes.	*TT2- Identity and Access Management (IAM)* Residential proxies and "password spraying" brute-force attacks targeted a small number of accounts. One account was a "legacy, non-production test tenant account." *TT3- Insecure Interfaces and APIs* Account had access to an OAuth application with elevated access to Microsoft's corporate environment. This elevated access allowed the threat actors to create additional OAuth applications to gain access to other corporate mailboxes. *TT4- Inadequate Selection / Implementation of Cloud Security Strategy* Microsoft has confirmed that MFA was not enabled for the user account. *TT6- Insecure Software Development* Account had access to an OAuth application with elevated access to Microsoft's corporate environment. This access allowed the threat actors to create additional OAuth applications to access other corporate mailboxes. *TT90 Limited Cloud Visibility/Observability* "After the Fact" – The company identified the malicious activity by retrieving traces in Exchange Web Services (EWS) logs, combined with known tactics and procedures used by Russian state-sponsored hacking groups.	**Confidentiality** Victims were not named, but keys and wallets were compromised. **Integrity** System in freefall and integrity uncertain. **Availability** Site pulled offline by legal actions; accounts were frozen.	**Financial** Major liquidity crisis forced FTX into Chapter 11 bankruptcy. **Operational** FTX accounts were frozen and ceased operations until liquidation under court supervision. **Compliance** The CEO was arrested and jailed partly due to lack of reasonable controls and lack of compliance with U.S. law. **Reputational** FTX ceased operating and has become a symbol of fraud, though its collapse did not undermine the crypto economy.	**Preventive** -IAM-06 -IAM-14 -CCC-04 -CCC-06 -HRS-11 **Detective** -CCC-07 -IAM-08 -IVS-09 -LOG-03 **Corrective** -A&A-06 -CCC-09 -SEF-03 -CEK-12 -BCR-08

Attack Detail

Threat Actor: Microsoft confirmed that Midnight Blizzard (aka Nobelium or APT29), believed to be a state-backed cyber espionage group tied to the Russian Foreign Intelligence Service (SVR), hacked into its executives' email accounts in November 2023, and also breached other organizations as part of this malicious campaign.

Threat: The threat actors used residential proxies and "password spraying" brute-force attacks to target a small number of accounts, with one of these accounts being a "legacy, non-production test tenant account." The password spray attack targeted a limited number of accounts, using a low number of attempts to evade detection and avoid account blocks based on the volume of failures.

Vulnerabilities: The test account had access to an OAuth application with elevated access to Microsoft's corporate environment. This elevated access allowed the threat actors to create additional OAuth applications to gain access to other corporate mailboxes, as explained below. MFA was not enabled for that account, allowing the threat actors to access Microsoft's systems once they brute-forced the correct password. Midnight Blizzard leveraged this initial access to identify and compromise a legacy test OAuth application with elevated access to the Microsoft corporate environment. The actor created additional malicious OAuth applications. They created a new user account to grant consent in the Microsoft corporate environment to the actor-controlled malicious OAuth applications. The threat actor then used the legacy test OAuth application to grant them the Office 365 Exchange Online *full_access_as_app* role. This permission programmatically grants an application full access to all mailboxes in the organization and is part of the Exchange Web Services API and allows the app to authenticate using OAuth to access mailbox data.

Technical Impacts

Confidentiality: The breach compromised the confidentiality of sensitive information, including email correspondence between Federal Civilian Executive Branch (FCEB) agencies and Microsoft. Midnight Blizzard exfiltrated email data, potentially exposing sensitive information and authentication details.

Integrity: The integrity of Microsoft's systems and data was compromised as the attackers used advanced techniques to compromise authentication mechanisms, potentially altering or tampering with data.

Availability: The attack did not significantly impact the availability of Microsoft's services. Microsoft's data resiliency and redundancy measures ensured that services remained available despite the breach.

Business Impacts

Financial: Due to the cyberattack, there was a noticeable financial impact on the company. Although specific figures detailing the financial consequences haven't been disclosed, Microsoft did incur costs related to investigation, remediation, and security enhancements. It's clear from Microsoft's statements that addressing this breach involved significant financial and operational efforts. However, in a Form 8-K filing with the SEC, Microsoft says that the breach has not had a material impact on the company's operations.

Operational: The breach disrupted Microsoft's operations, requiring significant resources to investigate and mitigate the attack. Microsoft's security team activated their response process to investigate and disrupt malicious activity.

Compliance: The breach raised compliance concerns, particularly regarding data protection regulations. Microsoft had to ensure compliance with relevant regulations and standards, such as GDPR and CCPA, while addressing the breach.

Reputational: The breach negatively affected Microsoft's reputation, highlighting vulnerabilities in security practices. The incident drew attention to Microsoft's security culture and practices, potentially impacting customer trust and confidence.

Controls - Preventive Mitigation

HRS-11: Security Awareness Training – Establish, document, approve, communicate, apply, evaluate, and maintain a security awareness training program for all employees of the organization and provide regular training updates to raise awareness of social engineering, OTP automation attacks, and insecure use of secrets on network shares.

IAM-02: Strong Password Policy and Procedures – Establish, document, approve, communicate, implement, apply, evaluate, and maintain strong password policies and procedures. Review and update the policies and procedures at least annually.

IAM-09: User Access Review – Define, implement and evaluate processes, procedures and technical measures for the segregation of privileged access roles such that administrative access to data, encryption, key management, and logging capabilities are distinct and separated.

IAM-14: Strong Authentication – Define, implement, and evaluate processes, procedures, and technical measures for authenticating access to systems, applications, and data asset multifactor authentication for at least privileged use and sensitive data access. Adopt digital certificates or alternatives which achieve an equivalent security level for system identities.

IAM-16: Authorization Mechanisms – Define, implement, and evaluate processes, procedures, and technical measures to verify access to data and system functions is authorized.

Controls - Detective Mitigation

CCC-07: Detection of Baseline Deviation – Implement detection measures with proactive notification in case changes deviate from the established baseline, such as network shares, misconfiguration, and accessibility.

IAM-08: User Access Review – Review and revalidate user access for least privilege and separation of duties with a frequency commensurate with organizational risk tolerance. Programmatic access to provisioned scripts and privileged access systems can help detect gaps and exploits similar to what happened here.

LOG-03: Security Monitoring and Alerting – Identify and monitor security-related events (e.g., account access, authentication attempts, anomalous access as in this case) within applications and the underlying infrastructure. Define and implement a system to generate alerts to responsible tenants, security teams, and stakeholders based on such events and corresponding metrics.

Controls - Corrective Mitigation

A&A-06: Remediation – Establish, document, approve, communicate, apply, evaluate, and maintain a risk-based corrective action plan to remediate incident and breach case findings, lessons learned, and improvement plans findings. Review and report remediation status to relevant stakeholders.

IAM-01: Identity and Access Management Policy and Procedures – Establish, document, approve, communicate, implement, apply, evaluate, and maintain policies and procedures for identity and access management. Review and update the policies and procedures at least annually. Numerous gaps leading to this breach case indicate a need for investment in foundational identity and access practices. A good foundational improvement would be uplifting the policy.

SEF-03: Incident Response Plans – Establish, document, approve, communicate, apply, evaluate, and maintain a security incident response plan, which includes but is not limited to relevant internal departments, impacted CSCs, and other business-critical relationships (such as supply chain) that may be impacted.

SEF-06: Event Triage Processes – Define, implement, and evaluate processes, procedures, and technical measures supporting business processes to triage security-related events.

SEF-07: Security Breach Notification – Define and implement processes, procedures, and technical measures for security breach notifications. Report security breaches and assumed security breaches, including any relevant supply chain breaches, as per applicable SLAs, laws, and regulations.

Metrics

Key Performance Indicators

- Mean-Time-to-Detect (MTTD): Microsoft identified the exposure, but the clearest identification of explicit timelines was that on January 12, 2024, Microsoft discovered their systems were breached in November 2023. Microsoft said the hackers accessed a "small percentage" of Microsoft's corporate email accounts for over a month. With the investments Microsoft had in prevention and detection, this indicates a lack of proactive monitoring or automated detection of misconfigurations across all internal systems and failure of low-key attack detection methods.
- Mean-Time-to-Remediate (MTTR): Microsoft reacted immediately to secure the breach. The exact MTTR timeframe from discovery to remediation is not available but is assumed to have been fast.
- Unauthorized Access Attempts: It is unknown what triggers are used to detect unauthorized access, but from the referenced information, the bad actors circumvented this through low-frequency attempts.
- Lessons Learned Implementation Rate: Percentage of corrective actions or security improvements implemented following post-incident reviews.

Control Effectiveness Measurements

- Access Provisioning Compliance Rate: Percentage of user and programmatic accounts provisioned with least privilege and MFA enabled.
- Unauthorized Change Attempt Rate: Number of attempted unauthorized changes to critical system components, such as fund transfer processes, over a specified period.
- Misconfiguration Detection Rate: The misconfiguration (lack of MFA and public-facing IP assumed to have been on the compromised cloud system) was not detected internally, pointing to gaps in manual and automated verifications, scans, and audits. Additionally, this measurement includes the percentage of applications assessed for vulnerabilities, misconfigurations, and security risks.
- Access Control Effectiveness: The absence of access controls (e.g., MFA, role-based permissions, standing access) allowed access to an OAuth application with elevated access to Microsoft's corporate environment.
- Audit Frequency of Cloud Configurations: Percentage of privileged accounts audited to ensure they only have access to systems and data they need (least privilege validation). No evidence was shown that any standard or scheduled audits of cloud environments were performed, a critical gap in Microsoft's security program.

Key Takeaways

- **2State-backed cyber espionage groups have more readily available resources:** In comparison to cyber criminals, state-backed actors host far more available resources. Regardless of the security maturity of a company, the weakest link is the key. Microsoft has a robust and mature security team with policies, yet the failure occurred in a seemingly low-risk test cloud subscription by an unassuming user due to a professional hacking group.
- **Simple and seemingly dated attack methods remain prevalent:** Well-known attack methods, even though dated, are still effective and can still penetrate mature and seasoned companies, as Microsoft learned being breached with residential proxies and "password spraying" brute-force attacks.
- **Test (non-prod) accounts are not exempt from security policies:** This attack was focused on and penetrated a legacy, non-production test tenant account. Had the company enforced consistent policies across all environments, including test and alpha/beta/gamma environments, or imposed least privilege, zero standing privileges, and standard security policies such as MFA, this may have been avoided. Policies, for example, to remove or disable test accounts after they are no longer needed. Companies have to invest in developing tools like these which basically detect unused accounts/instances and delete them.
- **Don't wake the dragon:** It was made clear that sneaking in unnoticed under the radar works. While many companies target detection for large and broad attacks, Microsoft learned that adversaries can use a passive and patient approach. This was evidenced in the password spray attack that targeted a limited number of accounts. In this manner, a low number of attempts helped evade detection through a low volume of failures. This avoided blocks of accounts with what looked like residential addresses, and helped sneak past the layers of detection Microsoft has in place. Slow and steady won this race.
- **Least privilege is more than a buzz term:** Given that the test account had access to an OAuth application holding elevated access to Microsoft's corporate environment, the threat actors were allowed to roam and create additional applications furthering their access. Had the privileges in the test account been restricted to bare minimum or removed with technologies such as zero standing privileges, Just-in-Time (JIT) access, or Temporary Elevated Access (TEA), this incident may have been avoided. In particular, TEA involves granting users elevated privileges or access rights only for a specific period of time, just when they need it to perform a particular task. The elevated access is automatically revoked once the task is completed or the time limit expires.

References

1. Midnight Blizzard: Guidance for responders on nation-state attack | Microsoft Security Blog https://www.microsoft.com/en-us/security/blog/2024/01/25/midnight-blizzard-guidance-for-responders-on-nation-state-attack/
2. CISA Publishes 'Emergency' Order On Microsoft Breach By Russian Group, Confirms Stolen Emails https://www.crn.com/news/security/2024/cisa-publishes-emergency-order-on-microsoft-breach-by-russian-group-confirms-stolen-emails
3. Microsoft Actions Following Attack by Nation State Actor Midnight Blizzard | MSRC Blog | Microsoft Security Response Center https://msrc.microsoft.com/blog/2024/01/microsoft-actions-following-attack-by-nation-state-actor-midnight-blizzard/
4. Exchange Online Data Resiliency - Microsoft Service Assurance | Microsoft Learn https://learn.microsoft.com/en-us/compliance/assurance/assurance-exchange-data-resiliency
5. Russian hackers stole Microsoft corporate emails in month-long breach https://www.bleepingcomputer.com/news/security/russian-hackers-stole-microsoft-corporate-emails-in-month-long-breach/

Appendix 1 - Deep Dive Use Case Explanation[1]

Attack Detail

Threat Actor: A threat actor is an entity, person, group, or organization that accomplishes the threat. Threat actors can be categorized as external or internal, malicious or non-malicious.

Threat: Threats are events or actions by a threat actor that can damage an organization's operations, assets, employees, or reputation through unauthorized access, destruction, disclosure, modification of information, or denial of service.

Vulnerabilities: A vulnerability is a deficiency in a process, system, application, IT asset, system security procedure, or internal control that can be used to accomplish a threat. Vulnerabilities make the threat actor's goals achievable. They generally relate to missing, weak, or misapplied security control.

Technical Impacts

Data Breach: Data breach is an incident in which an unauthorized individual or entity obtains sensitive data through unauthorized access to a system or network. A data breach can be accomplished through various methods, such as hacking, phishing, or social engineering.

Data Loss: Data loss is an incident in which sensitive data is unintentionally destroyed, lost, or misplaced. Various factors, such as human error, natural disasters, or technical failures, can cause this.

Confidentiality: Confidentiality ensures that information is protected from unauthorized access or disclosure.

Example: An insider who has accepted a job at a competitor downloads new product information onto a laptop before taking the laptop home and downloading the information onto their personal computer. The disclosure of technical information to a competitor for a new product might be severe if it significantly reduces the company's competitive advantage.

Integrity: Integrity ensures that information is complete, accurate, and up-to-date, is not subject to unauthorized modification or destruction, and ensures its non-repudiation and authenticity.

Example: An inexperienced IT consultant new to a boutique investment bank misconfigures logical storage units, granting unrestricted access and modification rights. This storage unit contains proprietary financial formulas used by in-house bankers, corporate investment departments, and high-net-worth individuals who perform analyses. A hacker discovers the unprotected storage unit and decides to delete the contents, causing a halt to the bank's trading operations. This incident might be considered severe depending on the investment bank's losses and those of its customers.

Availability: Availability refers to ensuring that information, systems, facilities, networks, and computers are available to authorized individuals or groups when they need to access them.

Example: A phishing campaign leading to a ransomware infection that prevents a bank from accessing 10,000 high-value customer accounts unless a ransom is paid might be considered severe depending on the length of unavailability, customers' losses, and the bank's loss of customers.

1 Cloud Security Alliance, Certificate of Cloud Auditing Knowledge Study Guide, 2021

Attack Detail

Financial: These impacts concern the increase in costs that result from an incident (e.g., ransomware, insurance premium increase, litigation, penalties/compensation to customers/partners, investigations).

Operational: These impacts concern disruptions to business processes, systems, and data (e.g., production/service delays, poor product/service quality).

Compliance: These impacts concern violating applicable laws and regulations (e.g., GDPR, HIPAA), which can result in fines and penalties.

Reputational: These impacts relate to perceptions of the company as a whole but lean toward internal factors (e.g., management issues and brand value, stakeholders' perceptions of products, services, and processes owned, licensed, or provided by an organization). In practice, brand value and reputation are often used interchangeably.

Controls - Preventive

Preventive controls exist to stop a threat from impacting a system or asset.

- Technical controls, such as MFA, and denying access to the system or data pending authentication.
- Administrative controls, such as bring your own device (BYOD), and user policy training to help ensure that devices compatible with the system are securely attached.
- Physical controls, such as guards and badges, and preventing unauthorized access to the grounds of a data center.

Controls - Detective

Detective controls identify an incident while in progress or uncovered or when one has already achieved its objective.

- Technical controls, such as intrusion detection system (IDS), for monitoring a network for malicious activity or policy violations.
- Administrative controls, such as reviewing logs, to help uncover suspicious access or activity leading to the discovery of an incident.
- Physical controls, such as motion detection systems and closed-circuit television cameras, to detect an intruder's presence after entry.

Controls - Detective

Corrective controls exist to restore the system or process to its state before the incident.

- Technical controls include backup and restoring a system to its pre-incident normal state.
- Administrative controls, such as incident response plans, ensure that staff can coordinate a timely and proper response to incidents requiring restoring systems and/or data.
- Physical controls include renewing access cards or canceling unused cards and restoring users to their original states before an incident.

Metrics

This section considers a) key performance indicators (KPIs) generated as a product of control performance and b) control effectiveness measurements (CEMs), which involve the monitoring and testing of the controls.

Key Performance Indicators

Key performance indicators are quantifiable metrics (usually as numbers, percentages, or averages based on system activity) used to measure the performance and progress of an organization's security program. KPIs are typically high-level indicators that help stakeholders assess the overall security posture and track improvements over time. They often focus on business-oriented outcomes and can be used to gauge the success of security initiatives.

Example KPIs:
Recovery Time Objective (RTO), Recovery Point Objective (RPO), Mean-Time-to-Detect (MTTD), Mean-Time-to-Remediate (MTTR), untrusted classified connections attempted/all connections, percentage of untrusted classified connections allowed continuously, incident priority, incident status (not processed, in process, resolved), and time elapsed for each step in the incident process and the incident resolution process as a whole.

Control Effectiveness Measurements

Control effectiveness measurements assess the efficacy of specific security controls (usually as numbers, percentages, or averages based on system activity or audits) implemented within an organization's security infrastructure. Unlike KPIs, CEMs are more granular and technical, providing insights into the performance of individual security controls.

Example CEMs:

- *Firewall Rule Hit Count: Measures the number of times specific rules in the firewall are triggered to block or allow traffic.*
- *Antivirus Detection Rate: Measures the percentage of malware or malicious files detected and blocked by the antivirus software.*
- *Password Strength Assessment: Evaluates the strength and complexity of user passwords to identify weak ones.*
- *IDS Alert Analysis: Assesses the number of alerts generated by the IDS and their accuracy in detecting actual threats.*
- *Phishing Email Click Rate: Measures the percentage of employees who clicked on simulated phishing emails during security awareness testing.*

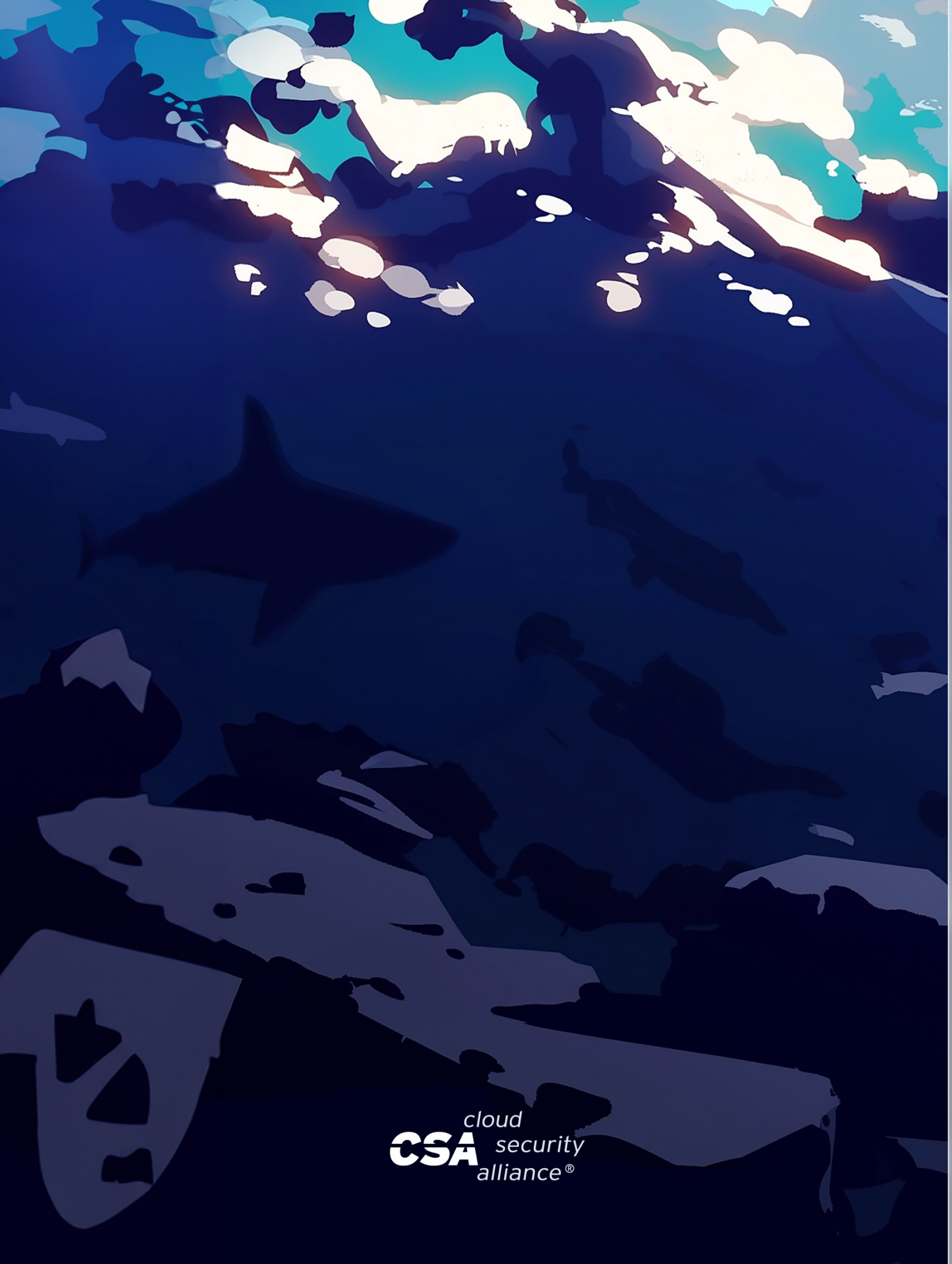
In summary, KPIs provide an overall view of the security program's performance and progress toward strategic objectives. CEMs focus on evaluating the effectiveness of specific security controls and technical aspects of the cybersecurity infrastructure. KPIs and CEMs are essential for organizations to understand their security strengths and weaknesses and make data-driven decisions to enhance their security posture.

Key Takeaways

A key takeaway is a significant point or lesson learned from the analysis of the incident. It often relates to a particular control issue, general best practices, or recommendations related to incident management and points to the solution of an issue or challenge.

Example key takeaways:

- *Vet third-party security service providers to ensure they are trustworthy and follow standard security practices.*
- *Require SLAs/contracts to provide additional network and filter capacity in emergencies such as a DDOS attack.*
- *Recall that the least privilege principle and segregation of duties are key to incident prevention.*
- *Have a detailed, tested incident response plan at the ready.*


cloud
CSA security
alliance®