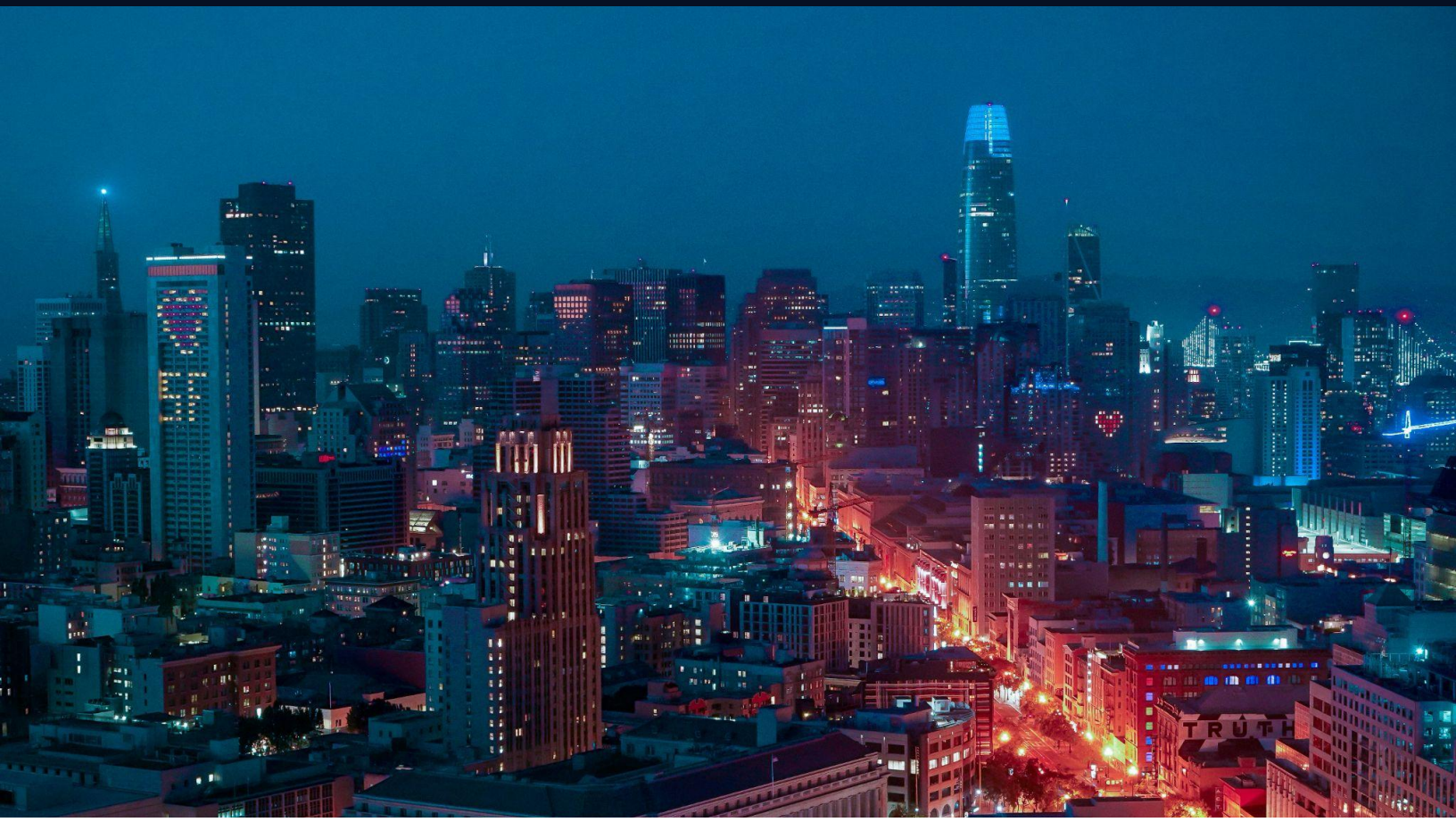
DAYBLINK CONSULTING

Incident Response Plan Redevelopment

How DayBlink Consulting redefined the Incident Response Plan for the cybersecurity organization of a major media and technology company



Introduction

A major media and tech company's cybersecurity organization faced a large, growing challenge: its Incident Response Plan (IRP) and associated procedures were misaligned with current processes, and not useful / ineffective during live incidents. As our client had evolved, some of its response processes failed to keep up. This became a major barrier to effective cyber response.

Recognizing these gaps, the organization initiated a comprehensive overhaul of its incident response procedures, including its IRP. The goal was to develop consistent, actionable, up-to-date IRP processes and procedures that improved response times, ensured compliance, and provided clear guidance to our client's cybersecurity professionals.

Problem

After various organizational changes and natural process drift, our client needed to revamp its outdated and inconsistent cybersecurity incident response processes and procedures

Over time, the company's cybersecurity org had accumulated a variety of obsolete IRP processes and procedures. They did not reflect current tooling, workflows or best practices, which created confusion and inefficiencies during live incident investigations. Compounding the issue, there was no centralized, cohesive catalog to track procedural updates and changes, making it nearly impossible to manage updates.

The IRP itself was the largest pain point: it did not align with actual response procedures and was riddled with legal and administrative language that served as a distraction during live incidents. The lack of clarity hindered effective incident response and increased the risk of delays and missteps when conducting cyber threat response activities.

Without a functional IRP and all of its associated processes, our client lacked a reliable foundation for cyber incident response. The organization required a solution that ensured up-to-date, actionable guidance so team members could perform their work effectively.

DayBlink Consulting revamped and optimized each level of incident response planning

Incident Response Plan ("IRP")

A strategic plan that defines how an organization detects, responds to, and recovers from security incidents.

- Strategic and Cross-Functional
- Framework for Coordination
- Tiered Response Integration

Standard Operating Procedures ("SOP")

A repeatable procedure for handling a specific type of incident or operational scenario referenced in the IRP.

- Process-Focused
- Repeatable and Auditable
- L1/L2 Decomposition

Runbooks

A detailed, technical guide that supports SOPs by outlining how to execute specific tasks during an incident.

- Tactical and Detailed
- Troubleshooting/How-To Guides
- L3+ Decomposition

Less — ***LEVEL OF DETAIL*** — *More*

10K+ Feet — *1K Feet* — *1 Foot*

DAYBLINK CONSULTING

Solution

Our team updated the incident response processes and procedures to be easy to understand, accurate and actionable

DayBlink Consulting modernized a Fortune 500 technology company's outdated Incident Response Plan (IRP) and all adjacent processes and procedures, focusing on clarity, usability, and alignment with current cybersecurity operations. We began with a detailed discovery phase that included 30+ stakeholder interviews across the org, a review of existing procedures, and an L1/L2 decomposition of ~25 critical cybersecurity investigation and response processes. This deep dive revealed key steps, dependencies, and decision points, which laid the groundwork for more consistent and effective IRP processes.

We restructured the IRP, one of the most critical artifacts in any cybersecurity ecosystem, into a practical, high-impact guide for live incidents. In doing that, first we rebuilt the high-level IRP framework to ensure a solid response foundation.

Then, we refined the specifics of the IRP methodology by redefining the processes and procedures that make up much of the IRP. Workflows were refined into clear, step-by-step instructions tailored to real-world scenarios, and excess legal language was removed to simplify usage. The result: faster, more confident incident response built to stand the test of time in an always-evolving cybersecurity threat landscape.

To streamline management and ensure accurate and accessible content around the clock, we created a centralized process catalog to keep response procedures updated with their evolving security needs. The catalog included clear guidance for update tracking and publishing changes in addition to general maintenance, ensuring our client could quickly and seamlessly refine and evolve their processes and procedures.

Outcome

We improved cyber readiness resulting in a ~12% reduction in response time

After modernizing our client's Incident Response Plan, they now have the ability to respond to incidents more effectively and efficiently, reducing response times and eliminating confusion during critical situations involving, in some cases, over 100 people. The new IRP achieved unanimous stakeholder approval following a company-wide roadshow, with key leaders—including the C-Suite—endorsing the plan and unifying the company in its incident response strategy.

The updates to our client's detailed IRP-related processes and procedures also had a significant impact. The updates provide clear, consistent guidance for various cybersecurity incident events, enabling uniform processes across the team.

Additionally, the introduction of new supplementary resources such as a 'lessons learned' template and a detection lifecycle guide filled in crucial gaps, further strengthening the team's ability to capture insights and improve incident response across the board.

These enhancements strengthened our client's cyber incident maturity, enabling more effective responses to emerging threats and positioning the organization to address evolving risks with a more unified approach for the present *and* the future.

25

Standard Operating Procedures Updated and Created, including the IRP

1,000+

Unique Process Steps Refined and Optimized

~12%

Reduction in Average Incident Response Time

WASHINGTON D.C. (Headquarters)

8609 Westwood Center Dr., Suite 110,
Tysons Corner, VA 22182

CONTACT US

Jacob Rosner, Manager
jacob.rosner@dayblinkconsulting.com

Connor Parkinson, Sr. Consultant
connor.parkinson@dayblinkconsulting.com

DAYBLINK CONSULTING

www.dayblinkconsulting.com