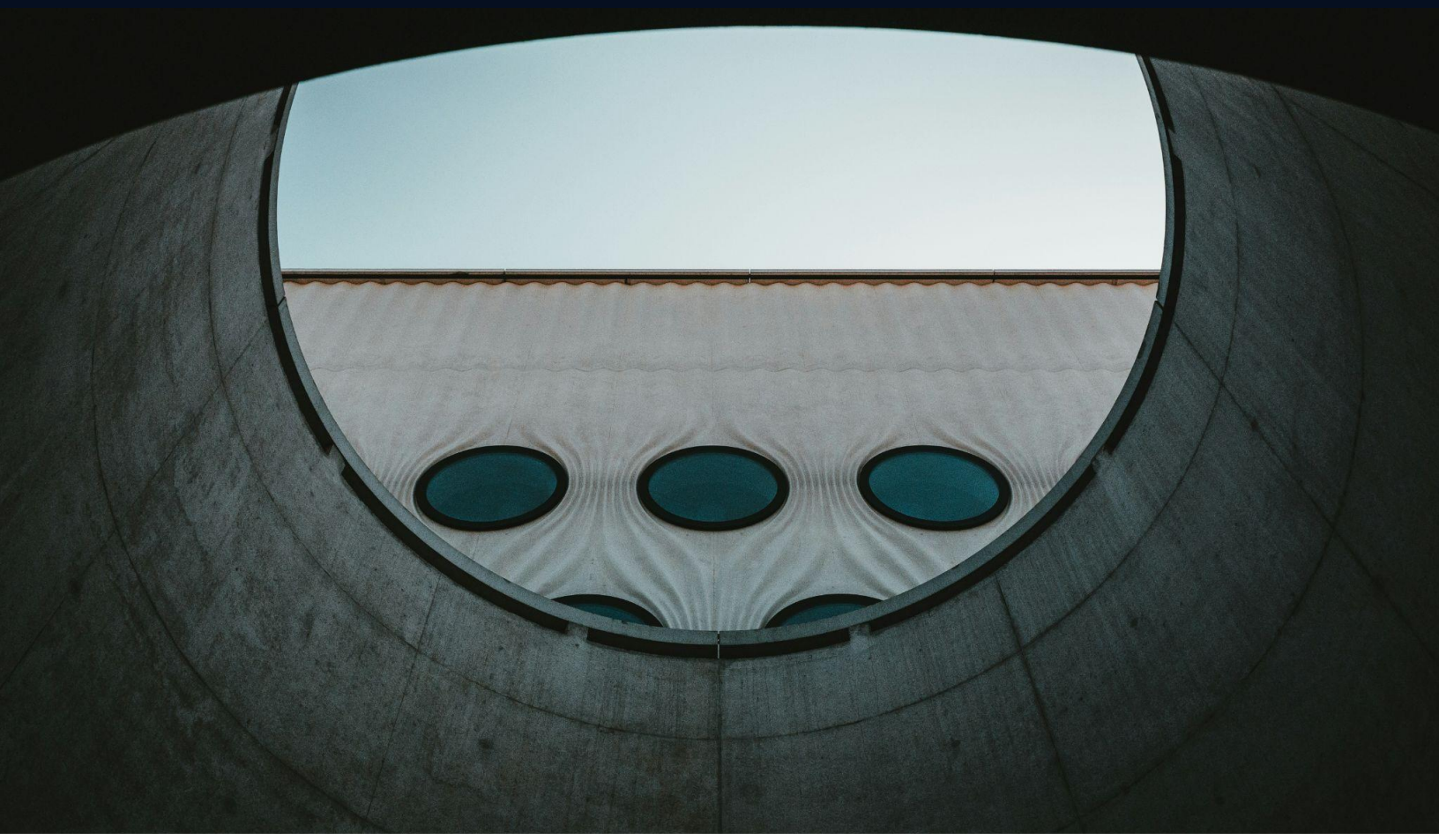
DAYBLINK CONSULTING

# Cyber Sourcing Strategy & Ops Model Design

DayBlink Consulting provided strategic support to the cybersecurity leadership of a global chip manufacturing & technology organization looking to transition away from a managed service provider for its cyber defense operations



## Introduction

A global chip manufacturing and technology organization found itself at a critical crossroads with its cybersecurity operations. The company's Cyber Defense Operations team responsible for monitoring, responding to, and mitigating cyber threats—had been fully outsourced to a managed security service provider (MSSP). While outsourcing initially appeared to be a cost-effective and scalable solution, the organization began experiencing a steady decline in service quality and effectiveness.

# Problem

## The MSSP was unable to provide the quality service required to confidently support the organization

Multiple issues emerged under the MSSP's stewardship. One of the most pressing problems was a market skills gap. The MSSP struggled to keep pace with rapidly evolving cybersecurity threats and modern technologies. This led to stagnation in service capabilities, particularly in areas such as automation, threat intelligence integration, and response agility. Compounding the issue was a significant lack of knowledge sharing. The MSSP did not foster an effective transfer of institutional knowledge, leaving the internal Cyber Defense team ill-equipped to manage or even understand the full scope of operations. The organization saw a number of alarming metrics including a 45% increase in the true-positive rate of alerts since onboarding the vendor, a full 40 hours of additional effort per week spent meeting with or resolving issues on behalf of the vendor than were expected in the contract, and finally a 20% rate of missed Mean Time to Detection (MTTD) SLAs.

Service degradation was evident to internal stakeholders and external customers alike. Escalation paths were unclear, and incident resolution timelines lagged behind industry expectations. Key metrics pointed to a lack of proper task administration and ownership, with critical alerts and vulnerabilities left unaddressed or handled inefficiently. Strategic decision-making suffered due to poor visibility into threat landscapes and incident histories.

The contract with the MSSP was nearing expiration, forcing the organization to quickly consider a new operational model. The internal Cybersecurity leadership recognized the need not only to terminate the existing contract but also to chart a path forward that would enhance capabilities, reduce risk, and regain operational control; however, they lacked a coherent transition strategy, including a sourcing plan, budget justification, staffing approach and roadmap for modernization.

### Sourcing Strategy Tactics

| | BUILD PHASE | | RUN PHASE | | | |
|---|---|---|---|---|---|---|
| | **Design** | **Build** | **Operate** | **Support** | **Situational Example** | **Staffing Model** |
| **Capability #1** Low-Level Current Maturity | Hybrid | Outsourced | Insourced | Insourced | Interested in industry support to build, but an important capability to be managed internally | Slow ramp of hiring to support capability |
| **Capability #2** High-Level Current Maturity | Insourced | Insourced | Hybrid | Hybrid | Mature internal function that has many low-level operating functions | Steady-state staffing from current-state |
| **Capability #3** Low-Level Current Maturity | Insourced | Outsourced | Insourced | Insourced | Internally designed, but requires quick ramp-up before managed internally | Prof. Services hired to be transitioned to internal hires |
| **Capability #4** Moderate-Level Current Maturity | Insourced | Outsourced | Outsourced | Outsourced | Internal requirements provided to a service that is fully outsourced | Low-level staffing for management of vendor |
| **Capability #5** Moderate/High-Level Current Maturity | Hybrid | Hybrid | Hybrid | Hybrid | A hybrid service that is developed and managed with a service partner | Moderate, consistent staffing support by vendor |

# Solution

## The client required support in developing a new target operating model and the roadmap to achieve it

To support this complex transition, the organization engaged DayBlink Consulting to help design and implement a strategic pivot away from the current MSSP model. DayBlink Consulting began the engagement by conducting a comprehensive current-state assessment, which revealed over 30 critical pain points and capability gaps. These issues were either directly tied to the MSSP or exacerbated by the organization's reliance on the vendor and were identified across not only the defense organization, but also the additional technology and support teams throughout security.

With a solid understanding of the operational landscape, DayBlink worked closely with the Cyber Defense team to define a new sourcing strategy. The approach emphasized the repatriation of core strategic cybersecurity services—such as threat hunting, incident response, and detection engineering. Recognizing that not all services required the same level of in-house expertise, DayBlink recommended retaining commoditized or low-security services, like Level 1 alert triage and certain monitoring tasks, though with new more specialized vendors.

To mitigate the risks associated with relying on a single provider, DayBlink introduced a multi-vendor sourcing model. This approach reduced single-source dependency, encouraged competitive pricing, and allowed for specialized vendors to be selected based on unique capabilities aligned with the organization's specific needs.

These sourcing decisions manifested in the deployment of a Target Operating Model (TOM) that redefined how the Cyber Defense Operations team would function post-transition. The TOM focused on resourcing strategic core functions internally while ensuring cost efficiency by outsourcing lower-tier activities. We created a detailed resource hiring plan was created, outlining roles, skill sets, and timing to fill approximately 15 new positions necessary for the revamped in-house operations.

To support executive-level planning and budgeting, DayBlink produced a three-year cost model. This model demonstrated the financial implications of the transition and supported the case for an additional $2 million in budget allocation. The analysis factored in costs associated with hiring, new tooling requirements, vendor contracting, and capability enhancements. It provided a defensible forecast of how the investments would increase maturity and reduce long-term operational risk.

Another critical output of the engagement was a six-month MSSP turndown and service transition plan. DayBlink mapped out a phased exit strategy that included knowledge transfer protocols, system access revocation, shadowing procedures, and checkpoints for validating internal team readiness.

The transition plan was designed to ensure zero disruption in service continuity while empowering the internal team with increasing control at each milestone - it was composed of four key phases:

1. **De-Risk the Vendor:** hire resources immediately to support the incumbent vendor team in areas that are currently identified as critical risks for support to avoid potential incidents or issues.

2. **Uplift to Remove the Vendor:** repatriate all target state services from the MSSP, mature capabilities through professional services including planning and beginning automation & integration activities.

3. **Transition from the Incumbent Vendor to the Target Operating Model:** implement Target Operating Model, align roles & responsibilities to target operating model, complete knowledge transfer from the MSSP and roll off.

4. **Mature Capabilities and Run the Operating Model Steady-State:** mature work management practices, continue automation and integration efforts, hire non-critical resources, align to support teams, and increase the overall maturity of the organization.

Finally, to anchor the transition in strategic improvement, DayBlink Consulting synthesized the identified pain points into seven thematic transformation activities. Each theme—ranging from automation and tooling upgrades to knowledge management and vendor governance—was supported by a concrete action plan. These initiatives were designed to modernize the security organization, positioning it to be more agile, responsive, and resilient in the face of future threats.

# Outcome

DayBlink Consulting helped to align on the future-state Operating Model and conduct the necessary proposal development and review for the new Hybrid Vendor Set

The engagement resulted in a clear, actionable path forward for the cybersecurity team and a tangible improvement in operational strategy. With DayBlink Consulting's guidance, the client now had a comprehensive roadmap to exit the legacy MSSP relationship and regain ownership of its cyber defense functions.

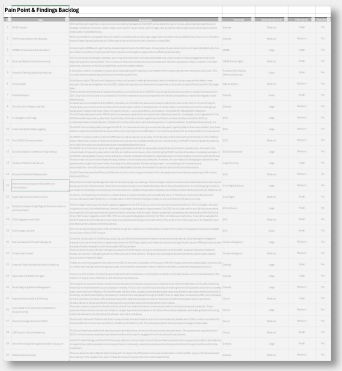
The new Target Operating Model enabled the organization to differentiate between strategic and commoditized work allowing for smarter resource allocation. By focusing internal talent on high impact areas and using specialized vendors for basic tasks, the team was better positioned to scale its capabilities efficiently and cost-effectively.

The three-year cost model provided leadership with a strong financial narrative that justified the $2 million increase in defense operations budget. This budget enabled the hiring of critical cybersecurity roles, the onboarding of new vendors, and the procurement of advanced tools that would have been out of reach under the previous MSSP arrangement.

## Findings & Recommendations Approach

### OBSERVATIONS

Collected feedback, challenges, highlights, or other key points of note from stakeholders



Discovery Observations are used to support a summarized list of Findings - this is typically a many to one relationship where there were many instances of similar observations. Findings are then mapped to the model, categorized, and weighted based on the Level of Effort and cost to the organization

### FINDINGS

Summarized outcomes of the current state assessment

**DIscover**

**Analyze**

**Thematic Grouping**

### POTENTIAL OPPS

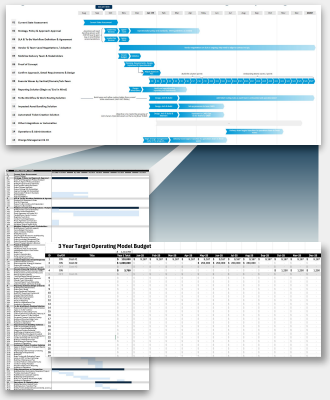
Work opportunities to get to Future State supported by Findings

1. Consider Short-Term Prof. Services Support Priority Automation Opportunities
2. Ensure All Tooling is Integrated with Planet Systems
3. Consider Replacement of the MSSP In all Strategic or 'Thoughtful' Areas
4. Harden Work Management Capabilities
5. Replace & Enhance Tooling to Improve Performance
6. Establish Formal Dotted-Line Integration with Support Teams
7. Mature the Organization Through Targeted Hiring

Recommendations may have a many to many relationship with Findings - but are typically designed to solve gaps in the Current-State

### PLAN & ROADMAP

Defined projects that comprise the solution set for achieving a Recommendation




Initiatives will typically be plotted on a strategy and planning roadmap and cost model over the short to long term for project planning & budgeting

The organization successfully began execution of the six-month turndown plan, including comprehensive knowledge transfers, platform changes, and phased assumption of responsibilities. As a result, the transition was smooth and disruption-free, with services seamlessly moving from the incumbent MSSP to the new hybrid model.

The effort launched modernization efforts across the Cyber Defense Operations organization and beyond. These included initiatives to improve automation, incident response times, data-driven decision-making, and vendor management. Not only did the organization strengthen its defenses, but it also fostered a culture of continuous improvement and accountability within its security function.

Ultimately, the project delivered a complete strategic reset of the client's Cyber Defense Operations. It empowered the organization to take charge of its cybersecurity posture, increase operational maturity, and reduce reliance on third-party vendors. Most importantly, it laid the groundwork for a more secure, agile, and resilient future.

**15+**

Critical & High Risks Mitigated Through Detailed Transition Planning

**25%**

Reduction in Expected Transition Time Through Detailed Prioritization & Planning

**$2M+**

Budget added due to identified and verified opportunities

## Making the Case for Cyber Strategy & Execution

Each organization has a unique set of needs as it relates to defining its sourcing strategy. Priority capabilities, cost, and business needs all play key roles in identifying the right strategy for your Security Organization. DayBlink Consulting is not tied to any one strategy or vendor, we focus on identify the needs of our clients and developing the best-fit strategy for your team.

## WASHINGTON D.C. (Headquarters)

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

## CONTACT US

**Harry Baker, Manager**
harry.baker@dayblinkconsulting.com

DAYBLINK CONSULTING

*www.dayblinkconsulting.com*