Cybersecurity in space is mission-critical

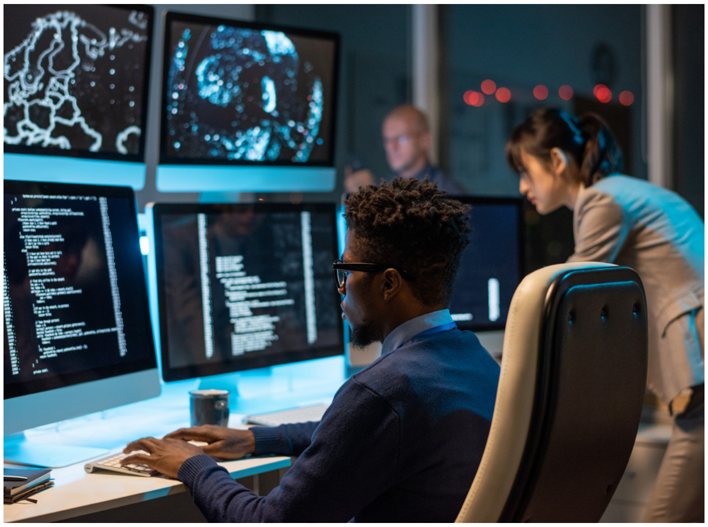
Building and running a next-generation SOC for our space manufacturing client

The challenge

When you're building solutions that go to the edge of space, cybersecurity is a matter of life or death

Our space and technology client's cyber operations were incredibly complex. The company was growing rapidly—as was the sophistication of its cyber threats and intricacy of its interconnected Operational Technology (OT) and IT systems. With an ever-expanding defense perimeter, the client needed a security operations center (SOC) just as leading edge as its space development work. And that SOC needed to provide strong threat detection and response throughout a digitally dispersed manufacturing ecosystem that included multiple third-party suppliers.

The client's mission was far too ambitious for a transactional approach to cybersecurity. It was looking for a collaborative advisor to build a next-generation security model tailored for the organization. And because of a previous negative experience with the managed service model, the client wanted to run it themselves.



The solution

A cutting-edge SOC that's FedRAMP-compliant and cost-efficient

To help the company accurately assess its threat landscape and cast a vision for a next-generation SOC, we invited them to an innovation workshop in our Houston Greenhouse. There, a team of professionals with diverse skillsets and experiences worked closely with the client's team to shape a roadmap that integrated leading practices and technologies. We also connected the client team with our Federal Space leader, who shared the work we are doing in missile defense and space defense. Together, this cross-disciplinary team uncovered the crucial intersections of space and cyber.

Drawing on this rich knowledgebase, we co-developed a vision for a next-generation SOC team: fluent in aeronautical OT and Department of Defense (DoD) specifications; with a track record of designing and deploying cybersecurity operations with detection, response, and threat hunting—all with a US-based, cloud-native approach to security operations.

It was clear that our Managed Extended Detection & Response ("MXDR") managed services solution was the answer—but what of the client's skepticism to managed service? Based on previous experience, the client's team didn't believe that a managed service provider could deliver the level of ownership and accountability they needed. We proposed an outcomes-based model; the client would only pay for our results, not the effort. That model, combined with the trust and confidence established during our workshop, convinced the client to engage us not only to design and implement the new SOC, but also to run it.

The outcome

Delivering what the CEO called the "gold standard" in managed services

Our sophisticated approach to cybersecurity and our outcomes-based model won over not only the client's cyber team, but also the CEO. He called Deloitte's MXDR offering their new "gold standard" for how to do managed services—not an outsourced transaction, but collaboratively with both sides committed to the right outcomes.

We quickly stood up a team to design, build, run, and manage the SOC, delivering a scalable MXDR solution with:

- A suite of leading technology in a single platform for IT and OT environments, which provided turnkey operations and operated as a service.
- Proactive 24/7/365 threat monitoring, threat hunting, incident response, vulnerability management, and asset mapping—Delivered with US personnel and FedRAMP-certified technology.
- Enhanced cyber resiliency—an improved ability to prevent and recover from business-disruptive events.
- A modular, cloud-native solution to support flexibility and the business's evolution.
- A tech-enabled approach to cyber that helps reduce total cost of ownership and increase value for the business.
- A long-term strategic cyber companion committed to helping securely launch space missions

And we're not finished: We're fine-tuning the alert volume so that our client can triage by severity; expanding into more OT environments; enhancing identity access management; and engaging in more hands-on engineering solutions.

Our outcomes include:

- **Increased visibility and protection of attack surface—from less than 75% to 99%**
- **Increased cyber maturity in more than 13 NIST Cybersecurity Framework subcategories**

By delivering MXDR services tailor-made to exacting DoD requirements and built to scale with the company's expected growth, our client gained a trusted collaborator to help proactively identify threats and prevent technology obsolescence. Because when you're redefining the future of space, you can't let cyberthreats stand in your way.

Our capabilities

Native cloud Saas delivery of unified, integrated modular services.

Extended Detection and Response (XDR)

OT Prevention, Detection, and Response (OTPDR)

Adversary Threat Hunting

Cloud Security PDR (CSPDR)

Endpoint Prevention, Detction, and Response (EPDR)

Incident Response (IR)

Digital Risk Protection (DRP)

Insider Threat Detection

Saas Prevention, Detection, and Response (SPDR)

Identity Prevention, Dection, and Response (IPDR)

Attack Surface and Vulnerability Management

Cybersecurity Intelligence (CSI)

This document contains general information only and Deloitte is not, by means of this document, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This document is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this document.

As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.