D3 SECURITY

D3 CASE STUDY

PUBLIC SECTOR

U.S. STATE GOVERNMENT

POPULATION: 5M+
20+ DEPARTMENTS
30K EMPLOYEES

THE BACKGROUND

Like many government entities, this State Government was facing the huge challenge of streamlining cybersecurity operations across multiple geographically distributed departments and agencies. They needed to better utilize their people, make their processes more efficient, and get more from limited budgets. Ultimately, their strategic goal was to mature their cyber operations, moving them from a reactive stance to a more proactive posture.

Their centralized SOC was responsible for monitoring the entire network and offering support to various state agencies when a threat vector had been identified. Initial triage and remediation steps were conducted by the centralized SOC, with network actions requiring collaboration with the IT team or the agency in which the threat had been detected. Typical communication channels were managed through either email or a third-party ticketing system. This provided very little visibility into actions taken, and the lack of enforced processes resulted in largely ad hoc remediation steps.

The Government decided that a security orchestration, automation, and response (SOAR) platform could be an ideal solution for many of their challenges.

THE EVALUATION

Over the course of a competitive, six-month evaluation period, D3 was selected to be the vendor for the Government's cybersecurity project. D3 was uniquely able to meet their requirements for a SOAR platform, including:

CORE REQUIREMENTS

Point-and-Click Configurability
The SOAR platform needed to be able to mirror the Government's existing internal processes and organizational structures, while also offering the flexibility to evolve alongside ever-changing threats, regulations, and processes.

Unlimited Automated Actions
The government wanted a SOAR platform that would allow them to accurately predict costs while taking all unnecessary manual actions off the desks of their analysts, freeing up time for more important tasks without the worry of rising fees.

Full-Lifecycle Response Capabilities
The SOAR platform needed to have the case management features to escalate incidents into investigations, whether for internal data leaks or incidents involving sensitive data types like PII, PCI, or PHI. Case management was also needed for cross-departmental investigations involving data privacy, compliance, legal, and HR investigators.

Built-In Guidance
Some government agencies were less mature than others and most were understaffed in terms of qualified analysts. Therefore, the SOAR platform needed to help ensure that consistent, best-practice procedures were being followed through each step – no matter the expertise of the individual analyst.

THE SOLUTION

D3 Security's SOAR Platform was selected following an in-depth competition that involved four leading SOAR vendors, as well as an incumbent solution.

Since implementing D3, the client has reported many additional benefits, including:

CENTRALIZED TOOLS

They integrated their SIEM, email exchange, phishing tools, sandbox, and ticketing systems via D3, creating a centralized platform for managing every step in the incident response process. This also provided them with a comprehensive audit trail, which was vital in ensuring compliance.

FULL-LIFECYCLE PLAYBOOKS

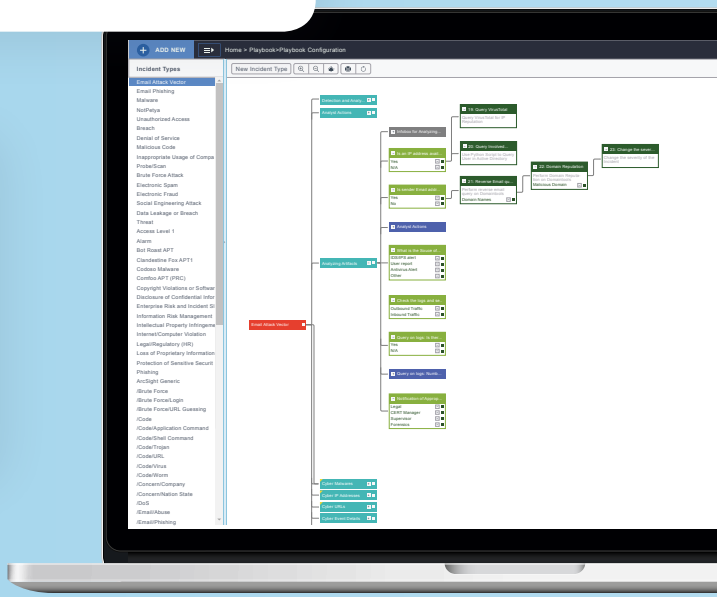
D3's full-lifecycle playbooks—based on the NIST framework—acted as the initial building blocks for response procedures, and over time the Government has used D3's configurability to tailor these playbooks and workflows in consultation with their top analysts and their D3-assigned CISSP.

AUTOMATED TRIAGE

One quick win was automating the triage and data contextualization of incidents. In the past, each incident required around 15 minutes of copying and pasting data between security tools and manually querying IOCs against threat intelligence platforms. With D3 SOAR, the incident records are now automatically contextualized with threat intelligence. The integration with the Government's ITSM means that tickets can be created from D3 with the click of a single button and updated based on actions taken within D3.

INTEGRATIONS

- ServiceNow ITSM
- McAfee ESM
- Microsoft Office 365
- VirusTotal
- Cuckoo
- DomainTools



FINAL METRICS AND COMMENTS

ANALYST HOURS SPENT ON INVESTIGATIONS PER WEEK

INCIDENT REPORT ENRICHMENT

> Since implementing D3, we've been able to bring our response times way down, eliminate operational and communication silos, and save hundreds—if not thousands—of analyst work-hours per year.
>
> CISO

> Our security tools have to cover more than 20 departments, which can create huge miscommunications and gaps between teams, especially because the experience level of people on each team varies quite a lot. D3 has made it a lot easier to get us all on the same page.
>
> CISO