D3 SECURITY

D3 SOAR CASE STUDY

FINANCIAL SERVICES

INTERNATIONAL BANK

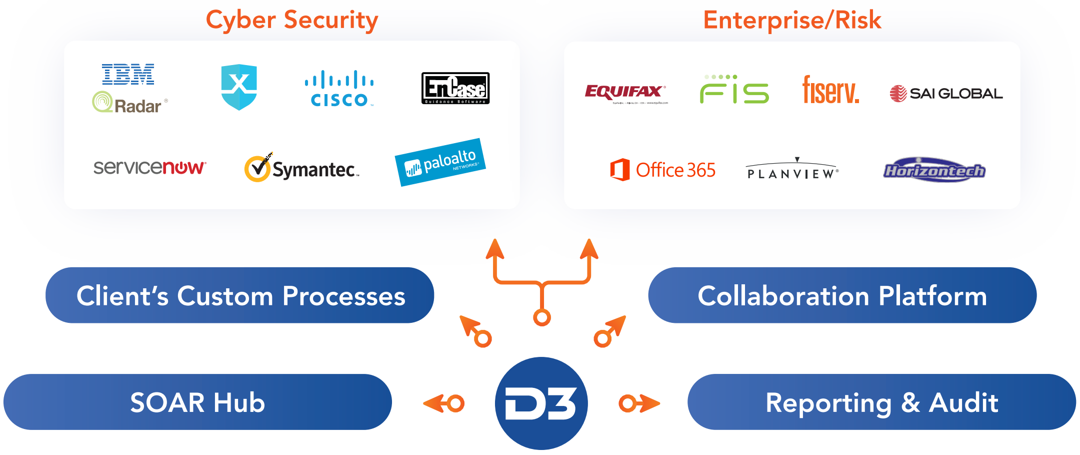
$1 TRILLION AUM
100,000 EMPLOYEES

THE BACKGROUND

In 2017, this major international bank reviewed its security, risk management, and compliance processes and came to the conclusion that it needed faster and better-coordinated incident response, while providing the strict documentation, tracking, and reporting required by compliance departments in the financial services industry.

Also tasked with securing endpoints, networks, facilities, plus protected information, the bank's global security leadership identified two overarching priorities that would achieve the project's goals. First, they needed to offset the SOC's lack of skills, resources and budget by leveraging technology to establish connective tissue among security tools and automate workflows.

Second, they needed cross-departmental incident management processes so that any threat could be seamlessly escalated, managed, and tracked. Their existing security infrastructure created rigid separation between teams and did not support collaboration for cases that required it, such as security incidents with privacy implications, "cyber SARs", or retail, account, or ATM fraud. The bank's highly siloed ecosystem made it impossible to get a cohesive view of security operations and active investigations, or to retrieve specific incident data when needed. The bank determined that a security orchestration, automation, and response (SOAR) platform would need to be at the core of the project.



Cyber Security

Enterprise/Risk

Client's Custom Processes

Collaboration Platform

SOAR Hub

Reporting & Audit

THE EVALUATION

During a lengthy 6-month competitive POC process, D3 outperformed all other vendors with its unique ability to meet the bank's complex orchestration and automation, case management, and collaboration requirements. Key factors in the decision included:

CORE REQUIREMENTS

Unlimited Configurability
Because of the bank's wide-ranging requirements, the SOAR platform had to be agile and configurable without relying on vendor support to make changes. A narrowly focused cybersecurity automation platform would not suffice; the platform needed to seamlessly integrate other systems, such as enterprise and risk management tools that were required by the bank's anti-fraud, corporate security, and risk departments.

Support for Larger Investigations
As a major bank that faced sophisticated attackers, the SOAR tool needed to be as strong at handling larger cases as it was at remediating individual incidents. Thus, the tool needed to be able to bring incidents together into case folders, support collaboration between analysts, and be able to extend access across teams and departments like Legal and Compliance.

Full-Lifecycle Analytics and Security Metrics
In order to break down the information silos that the bank had identified as problematic, the SOAR tool had to be able to provide important data to personnel at every level of the organization. This included SOC performance metrics like MTTR, as well as broader trend reporting.

Audit and Compliance Readiness
Because of the financial sector's strict regulatory requirements, the bank needed a SOAR tool that could track and present evidentiary-quality data to demonstrate proper procedures. This included complete chains-of-custody, audit logs, and "canned" compliance reports that covered all of the bank's needs.

THE SOLUTION

D3 now serves as the bank's security operations backbone, providing orchestration and automation across the security infrastructure, enhancing analysts' IR and decision-making abilities, and ensuring seamless, and accountable, investigation management for compliance, privacy and forensics teams who collaborate on key cases.

The D3 SOAR Platform integrates the functions of 15 separate solutions into a single operating console. The consolidation provides greater administrative control, and a comprehensive security operations framework for 500 users with role-based access controls that reflect data privacy rules. The common data taxonomy for all incident types supports accurate and easy audits. D3 trained the bank's administrators so that they can use D3's limitless configurability to adapt to any changes in their needs—no vendor involvement required.

DEPARTMENTS USING D3

- Cyber
- Privacy
- Corporate Security
- Fraud
- Compliance
- Risk
- Computer Forensics

INTEGRATED TOOLS INCLUDE

- IBM Qradar SIEM
- IBM XForce TIP
- ServiceNow ITSM
- Symantec DLP
- Palo Alto Networks
- EnCase
- Office 365

REPORTED ADDITIONAL BENEFITS

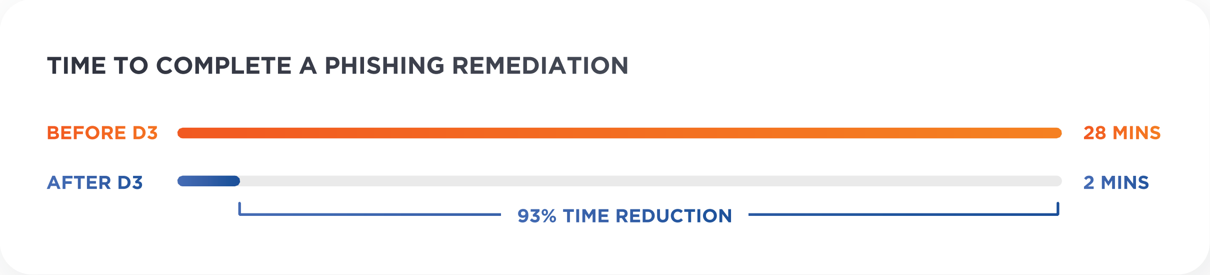
SOAR-POWERED RESPONSE

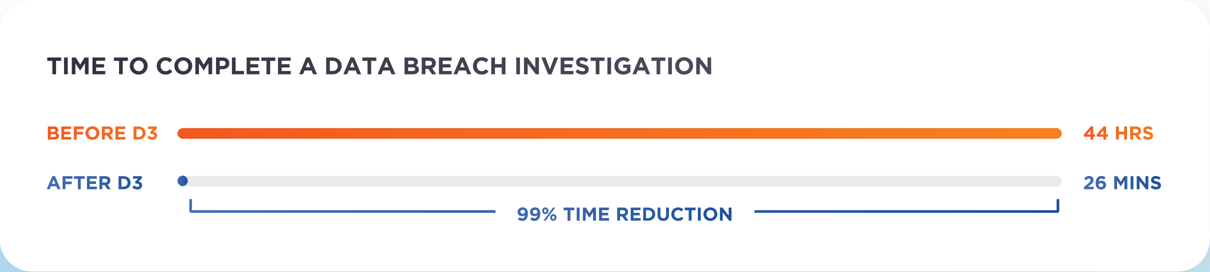
D3 reduced the bank's mean time to resolution by 90% for key incident types, largely thanks to adding automated steps to playbooks, and orchestrating across intelligence sources to gather contextual data for every alert.

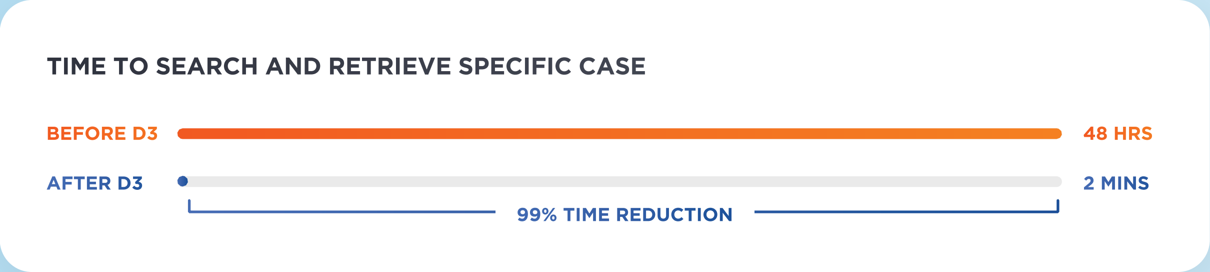
BREAKING DOWN SILOS

D3 has also eliminated the information silos that existed previously, by empowering analysts with case management and data protection controls. This facilitates cross-departmental ownership and accountability within cases. Because everyone is using D3, teams can work on the same records from any team and any physical location.

FINAL METRICS AND COMMENTS


TIME TO COMPLETE A PHISHING REMEDIATION


TIME TO COMPLETE A DATA BREACH INVESTIGATION


TIME TO SEARCH AND RETRIEVE SPECIFIC CASE

> “
>
> D3 is our primary incident response, case management, and investigative platform. We use IR across information and corporate security, fraud, and privacy. The case management module provides a common language for all security and risk teams to collaborate, while maintaining access controls for protected data. Through D3, we have completely elevated our incident response, audit, and compliance capabilities.
>
> Chief Security Officer (CSO), International Bank