D3 SECURITY

D3 SOAR CASE STUDY

HEALTHCARE

MULTI-STATE HEALTH SYSTEM

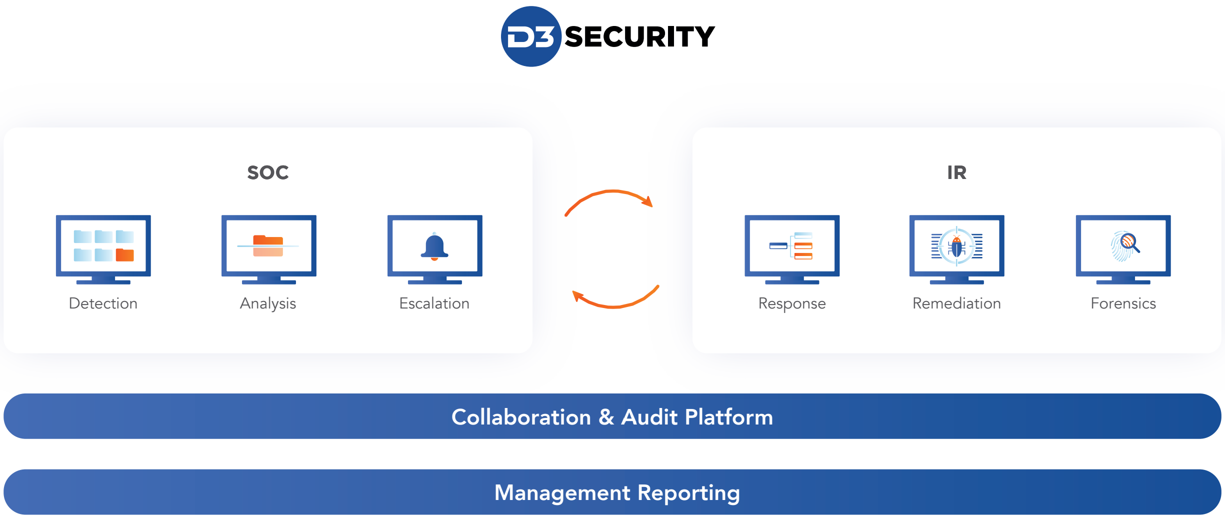
$8.8 BILLION REVENUE

50,000 EMPLOYEES

THE BACKGROUND

In 2016, this large health system operating 30 hospitals and employing 50,000 people experienced a data breach that exposed personally identifiable information (PII) of millions of people. The fallout damaged the organization's reputation and financial standing. The incident investigation alone cost $2M.

The incident led to the health system re-imagining their security operations, incident response and digital forensics, bringing each practice fully in-house. The security leadership was empowered to build a modern SOC and IR team, providing greater control over their environment and visibility of the full incident lifecycle. Knowing they were facing skills and resources shortages, the leadership identified Security Orchestration, Automation and Response (SOAR) technology as an important force-multiplier for security operations, incident response, and digital forensics case management.



THE EVALUATION

Because they were building a SOC from scratch and would invest in several tools in the years to come, the health system sought an open SOAR Platform that could easily integrate with any tool from any provider.

CORE REQUIREMENTS

A Hub for Network, Email, Endpoint and SIEM Alerts

The SOAR Platform had to be able to consolidate alerts from each source and rapidly correlate for proactive analysis. To achieve the highest level of visibility and workflow automation, the SOAR tool also had to provide feature-rich integrations and bi-directional information flow.

Easy Creation of End-to-End Playbooks

Following the breach, a new policy required the SOC to have a playbook for every conceivable incident type—from threats like ransomware to lost devices. In order to comply, the SOAR tool had to come with a library of out-of-the-box playbooks, while supporting agile playbook building and modification.

Granular Access Control for Sensitive Data

The SOAR Platform had to have strong information access controls and encryption options. Locking down certain fields or making them available to approved investigators on a need-to-know basis was critical in this healthcare setting. The tool also needed to be capable of storing employee information for multiple years.

Predictable Cost Structure/Pricing Model

The SOAR Platform needed to offer significant return-on-investment through the elimination of manual tasks, while offering price consistency for yearly budget planning purposes. The hospital network did not want to incur the per-action pricing fees associated with some SOAR tools.

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:

IMPROVED COST-TRACKING AND MANAGEMENT-LEVEL METRICS

Using D3, we are able to track the time we spend on tasks and data processing for the legal department, and bill that back. I'm able to say, here's how much time we've spent on this case, here's the cost, and here is the investigator working on it.

- IT Security Manager

CREATING NEW PLAYBOOKS IN SECONDS

If there's a playbook I need built, or a change made in the system, I can go and do that right now. Admin stuff is so simple and easy. I can manage incidents on the fly, and react to new information, without having to reconfigure or write scripts.

- SOC Team Leader

COHESION BETWEEN SECOPS, IR AND FORENSICS CASE MANAGEMENT

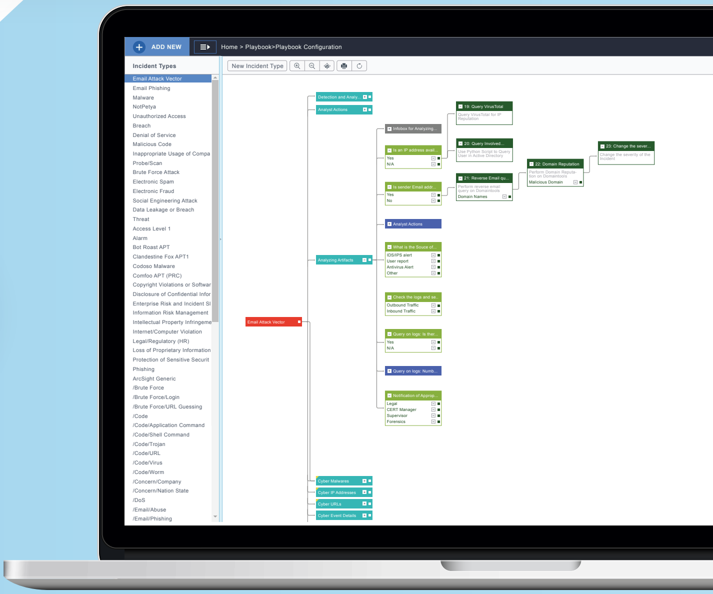
Prepare, discover, respond, track, remediate and report—we manage and track all six of our investigative phases in D3. It gives us cohesion between the SOC, the incident response and forensics teams. They shouldn't be using different ticketing systems.

- VP of IT Security

INTEGRATIONS

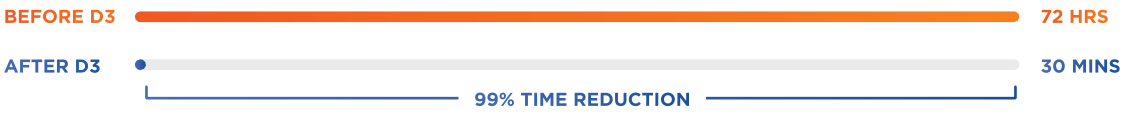
- Splunk ES
- Cisco ThreatGrid
- Symantec EDR
- Carbon Black EDR
- PhishMe Reporter
- Fortinet FortiGate

11 SOC USERS

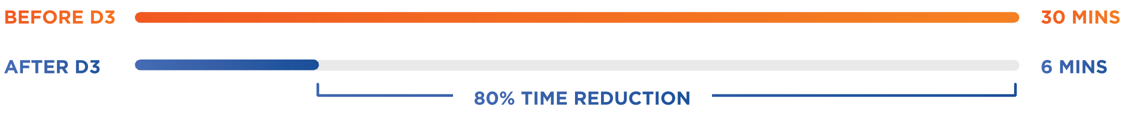


FINAL METRICS AND COMMENTS

TIME TO COMPLETE A DATA BREACH INVESTIGATION



TIME TO COMPLETE A PHISHING REMEDIATION



D3 TECHNOLOGY

> The fact is D3 gives me a solution that's as flexible as I am creative… I can customize playbooks and pivot responses on the fly, which is so important because we're growing our SOC. While we developed our own playbooks and procedures, the library of NIST and MITRE workflow solutions is invaluable. They allowed me to look at my own playbooks from a different angle, and helped us get more 'meat' into our SOAR solution.

SOC Team Leader

D3'S CUSTOMER SUCCESS TEAM

> D3's hands-on approach is invaluable. Our D3 Customer Success Manager is a directly responsible resource that understands cyber security—he's not just a guy in a room of engineers. It's a huge difference-maker; he knows what I'm doing, how I need to do it, and if he doesn't know, he gets the answer right away. It's the best vendor relationship our SOC has.

SOC Team Leader