D3 SECURITY

D3 SOAR CASE STUDY

10X FASTER = 10X EASIER

How a Global FinTech Company Elevated Security Operations and Response Using D3 NextGen SOAR

GLOBAL FINANCIAL TECHNOLOGY COMPANY

$6 BILLION
Annual Revenue

18,500+
Employees

WHEN SECURITY TOOLS AREN'T FAST, OR SMART, ENOUGH

Today, when a security alert is received by this FinTech Company's Cybersecurity team, they know it will be triaged and resolved in a minute. But this wasn't always the case. In fact, when they were handling alerts manually, it took 10 times longer, which meant that analysts from their small team could regularly spend an entire day just managing new alerts.

Now, with D3 NextGen SOAR, the Company is able to perform better enrichment across more integrated tools, so that even when they need to provide an alert and its context to their MSSP for resolution, the whole process takes 1-3 minutes, and can happen in real time—not daily batches that leave dangerous threats uninvestigated for hours.

BEFORE SOAR: MANUAL PROCESSES AND DATA SILOS

Dave, Manager of Security Operations at the FinTech Company, had to work hard to get things where they are today. He was part of a 10-person team around the globe that was dealing with thousands of alerts per day. No one had time to even look at them all. By improving their filtering in Splunk, they eventually got it down to hundreds of alerts per day, but Splunk couldn't meet all their needs. They added IBM QRadar to correlate alerts, but because they had no automated enrichment, Dave's team still spent a ton of time manually scraping other tools and figuring out what to do next.

A new engineer wrote some Python scripts to automatically query Splunk, but the solution wasn't sustainable because it relied entirely on the knowledge of that engineer. If he left the company, they would be back to square one.

The FinTech Company was part a larger enterprise in those days, which had built its own security orchestration, automation, and response (SOAR) platform, so Dave was able to get a sense of what an automated solution might look like. Unfortunately, when the enterprise sold its majority stake in the Company in 2018, Dave's team was once again left without the tools they needed to handle alerts and investigations.

CHOOSING THE RIGHT SOLUTION

Dave tried to find the right solution to increase orchestration and automation, while improving the Company's overall security posture. He also needed a tool to act as a bridge between his team and an MSSP, with which they had just begun working. Dave asked himself these questions:

1. How can we most effectively deal with the rising number of threats and alerts in our environment?

2. How can we scale our processes and automate them through product integrations?

3. How can we operationalize the MITRE ATT&CK framework in order to create an early warning system for serious threats?

Dave and his team conducted an RFP, and initially were primarily interested in D3's NextGen SOAR Platform for its case management capabilities. But when Dave saw a demo, the D3 sales engineer showed how D3 could provide case management, security operations automation, and correlation of attacker techniques, all in one platform. It was these qualities, along with flexibility and the ability to provide NIST-compliant incident response and case management workflows, that led the Company to choose D3 as their SOAR vendor.

PRODUCTS IN THE AUTOMATED ENVIRONMENT

SIEM

TWO VULNERABILITY MANAGEMENT TOOLS

REPORTING

CLOUD ORCHESTRATION

ITSM

ENDPOINT SECURITY

THREAT INTELLIGENCE

A TOOL TO SUPPORT THE ENTERPRISE SOC AND THE MSSP

Shortly before implementing D3, the FinTech Company had begun working with an MSSP partner for tier one security activities. At first, the MSSP struggled to provide value, because they constantly had to consult with, or escalate incidents to, Dave's team for guidance and approvals.

When the FinTech Company implemented D3 NextGen SOAR, Dave introduced it to the MSSP. With D3's full enrichment, end-to-end playbooks, and product integrations, the MSSP now rarely has to consult with Dave's team to resolve alerts. Because the MSSP can access D3, which aggregates alerts and intelligence, and orchestrates across tools, Dave doesn't need to grant them access to all his internal tools, which makes his data more secure. With D3, the MSSP has become a much more cost-effective and accountable partner for Dave's Company.

The reporting benefits of D3 have also helped FinTech Company stay on top of critical metrics, which can be filtered by SOC, MSSP or a combined view.

Dave receives an automated report every day, generated by D3 via a bidirectional integration Snowflake. The report can be configured to run as often as every 15 minutes, and includes important metrics like:

- Total/Open/Closed Incidents
- Average Response/Closure Time
- Incidents by Stage/Type
- Incident Volume Trends

Finally, D3's NIST-based incident response playbooks help Dave generate incident-handling performance data associated to specific stages of incident response, giving the team valuable data on which to base training or focus on for improvement.

SOME OF THE COMPANY'S MOST VALUED FEATURES IN D3 ARE:

GUIDED SETUP FOR INTEGRATIONS

Helps the FinTech Company manage and grow their complex automated environment without wasting time setting up connectors and writing scripts.

ATT&CK MONITOR

Achieves the FinTech Company's goal of establishing the MITRE ATT&CK Framework as their way of classifying threats.

CODELESS PLAYBOOK BUILDER

Enables Dave and his team to easily build and edit workflows that include their entire security stack.

AUTOMATED ALERT ENRICHMENT

Saves the FinTech Company as much as 90% of the time they used to spend on alert triage.

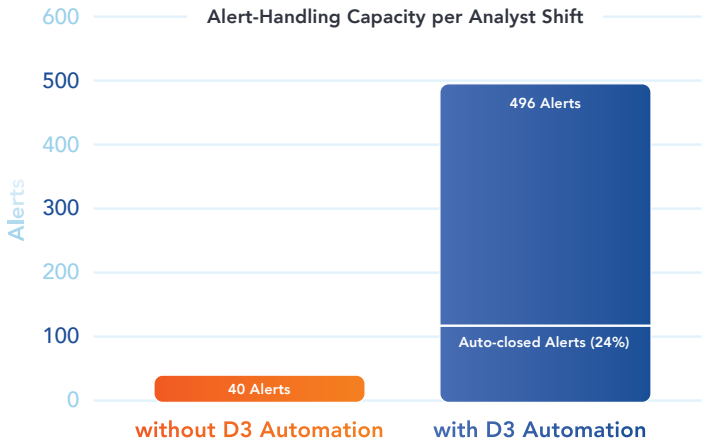
KEY OUTCOMES AND PERFORMANCE METRICS

Since adding D3, Dave's team has seen considerable gains, and it's only getting better as they become more familiar with the system. Response times are 10x faster for the cybersecurity team, and MSSP response and closure times have improved 3-4x just in the last few months. Automation allows FinTech Company to auto-close as many as 24% of their monthly alerts when they are identified early on as false positives.

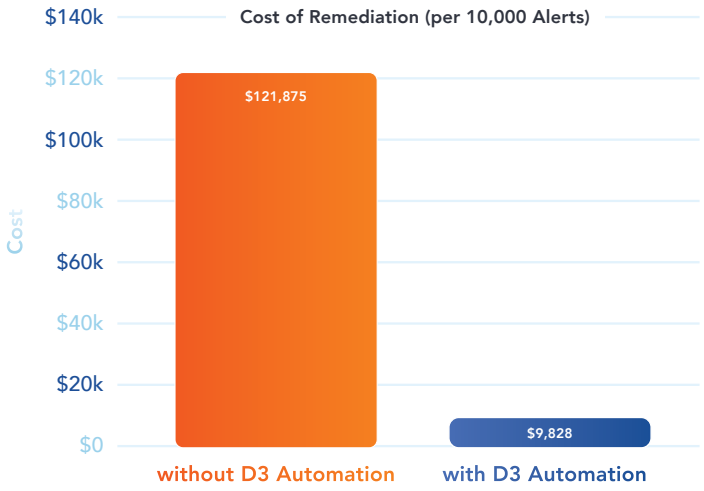
> **Before SOAR, our analysts spent 10 minutes on each basic alert, so closing 40 alerts took over six-and-a-half hours... but with SOAR, we've got it down to a minute, meaning we can handle 10 times more alerts than before."**

DAVE
Manager of Security Operations

ALERT-HANDLING VOLUME



AVERAGE REMEDIATION COST PER ALERT

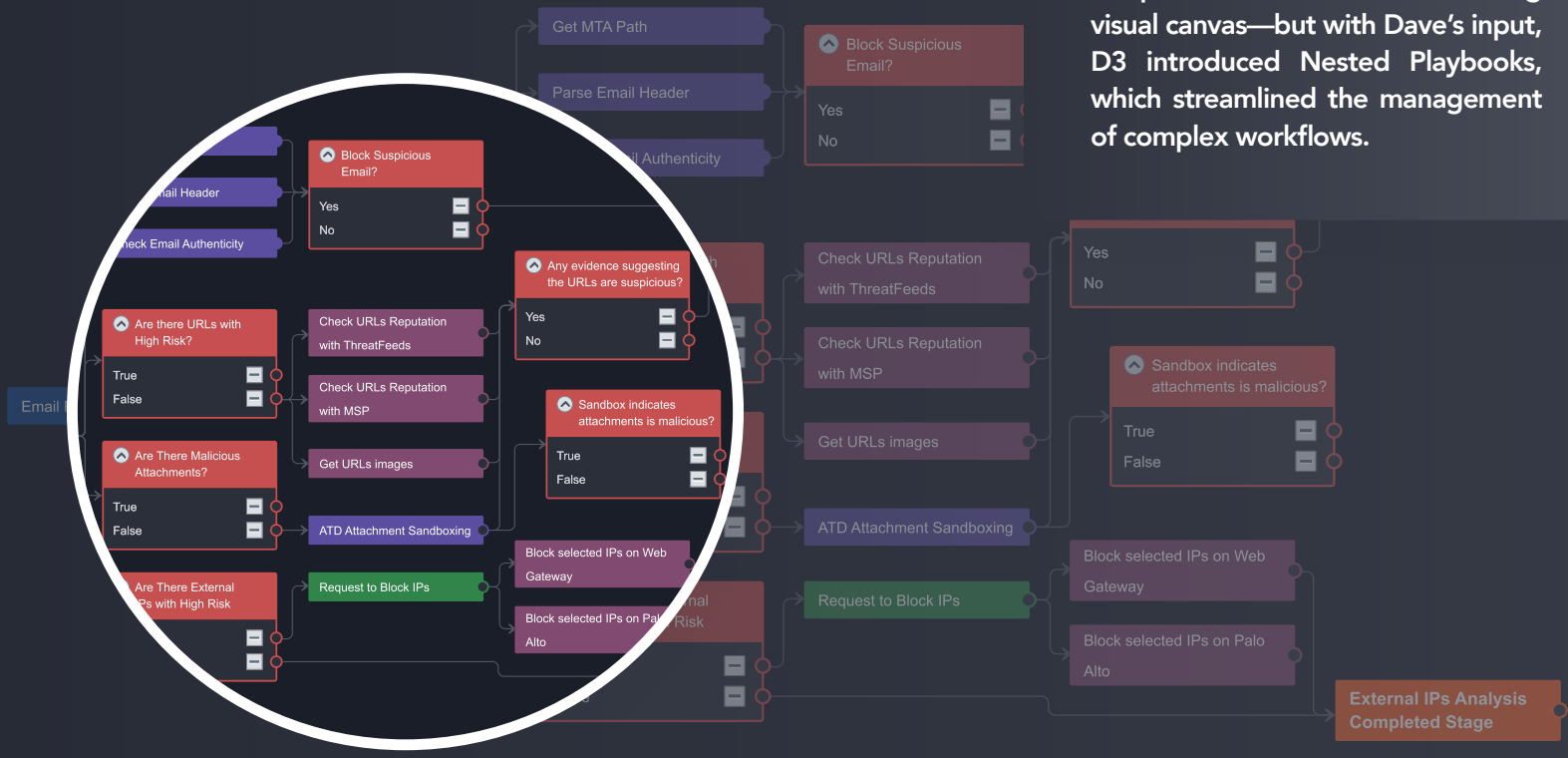


ENABLING A MITRE ATT&CK-BASED "EARLY WARNING SYSTEM"

During the selection process, Dave knew he wanted D3's ability to correlate QRadar events against the MITRE ATT&CK Framework, as well as the Monitor Dashboard to show the frequency of each adversary technique in the environment. The FinTech Company is currently working with D3 to put this into practice, and Dave sees it as a valuable way to focus efforts and ensure analysts know what threats to expect. "For managers, they'll be able to see the techniques that are happening towards the end of the kill chain and figure out why it's happening and why the other tools failed to catch it," says Dave.

DAVE'S EPIC PLAYBOOK

D3 is easy to implement and operate, but there is an extremely high ceiling on how it can be utilized by a skillful operator like Dave. When the FinTech Company replaced its IDS tool, it inadvertently created a spike of 150 alerts per day, which threatened to overwhelm the MSSP's monthly alert quota in a matter of days. Using D3's Codeless Playbook Builder, Dave created a playbook to filter out those alerts before they got to the MSSP. The playbook evolved, eventually becoming capable of automating triage and remediation for many different types and sources of alerts. It was getting a bit too big at one point—taking up a lot of space in D3's horizontal-scrolling visual canvas—but with Dave's input, D3 introduced Nested Playbooks, which streamlined the management of complex workflows.



WHAT'S NEXT?
EXPANDING D3 ACROSS DEPARTMENTS

The FinTech Company has already been able to break down informational and operational silos using D3 NextGen SOAR, but Dave has plans to go even further.

> **We have opened D3 to other security pillars beyond the SOC, CSIRT, and our MSSP. Our Data Loss Prevention, Cyber Threat Intelligence, Threat and Vulnerability Management, and Threat Detection Operations departments are already starting to use D3 as a common framework**

DAVE
Manager of Security Operations

In addition to expanding D3 usage across departments, Dave and his team are always collaborating with D3 to optimize their deployment and push the platform further. They are constantly refining playbooks, fine-tuning workflows to reduce false positives, and finding ways to improve or replace existing APIs.

A global organization like Dave's never sits still, and neither does D3. But with 10X faster response times, maybe Dave and his team can finally take a few minutes to relax.