D3 SECURITY

THE ROI OF D3 XGEN SOAR

WHITEPAPER

D3 Security provides a security orchestration, automation and response solution called XGEN SOAR that helps its customers triage, validate and remediate security threats quickly and consistently.

Customers gain intelligence through integration with their security stack and eliminate the need for manual labor and workarounds thanks to orchestration and automation. With a streamlining and optimizing effect across the full incident response lifecycle, including within the SOC team and beyond it (e.g. CTI, DLP, etc.), XGEN SOAR provides significant benefits by dramatically reducing response times, and strengthening the organization's overall security posture.

CHALLENGES

It's hard not to feel like today's cyberattackers have the advantage. Analysts are faced with too many alerts, leading to missed or mishandled security incidents, some of which result in operational issues, monetary losses, data breaches, and other nightmare scenarios. The growing number of tools in the typical SOC only adds complexity and creates more data and workflow silos. With the cybersecurity skills gap showing no signs of improvement, security leaders need to find ways to increase efficiency and effectiveness without adding more personnel.

RECOMMENDATIONS

Security leaders looking to understand the value of D3 should:

- Determine the threats and challenges which are facing your SOC today and in the future
- Understand the types of qualitative and quantitative benefits which D3 XGEN SOAR can deliver
- Review recent examples of the positive impact experienced by real-world D3 customers

UNDERSTAND THE BENEFITS

Productivity Gain

One of the fastest ways D3 SOAR buyers see ROI is through the time saved on high-volume repetitive tasks like alert triage. By automating ingestion, contextual enrichment, and risk scoring of alerts, SOAR users quickly reduce the time spent on security alerts by 90% or more. This automation eliminates the biggest hurdles to fast and effective Tier 1 security operations and helps SOC managers get more value from Tier 1 analysts.

Operational Improvements

Implementing D3 SOAR enables more mature security operations and strategic improvements that help users protect against costly security incidents. This is achieved through means that include codifying and automating effective procedures via playbooks, documenting security activities by incident stage to identify problem areas, and providing visibility through granular reporting. By starting with key use cases and gradually expanding your use of automation and optimized processes, you can continue to make steady operational improvements.

MTTR Reduction

D3 can combine triage, conviction, and remediation and orchestrate response across the full security stack, including auto-remediation of events at machine speed. When a cyberattack does occur, nested playbooks keep analysts focused on a single workflow and reduce wasted time. MTTR dashboards give SOC managers valuable visibility. D3 users can catch incidents earlier and resolve them quicker, minimizing their harm and cost to the business.

Detection and Response

D3 SOAR correlates the TTP data in incoming alerts against the MITRE ATT&CK framework to identify other traces of attacks. D3 cross-references against other tools to confirm the TTP analysis automatically runs queries on the IOCs. This enables D3 users to rapidly detect and respond to stealthy, fast-moving attacks.

Agility and Resilience

D3 SOAR saves users time and money through agility. With D3, you can quickly create playbooks, connect to new tools and data sources, bring on new analysts, extend workflows beyond the SOC, and even change MSSPs with minimal disruption.

Risk Avoidance

Faster and more thorough incident response reduces risk of all kinds: security, data privacy, financial, operational, and reputational. Some D3 features address financial and compliance risk even more directly. For example, for companies subject to GDPR, D3 can drastically reduce breach response times, making it possible to maintain compliance. Privacy risk is also reduced by features like granular role-based access controls and encryption options.

SOAR METRICS

TIER 1 | TRIAGE

Manual alert triage has been bogging down SOCs for years and without intervention it's only getting worse. D3 users automate the entire ingestion, enrichment and prioritization process, eliminating the need for manual coordination.

	WITHOUT D3 (MINS.)	WITH D3 (MINS.)
Gather and Review	2	0.25
Contextualize	10	0.25
Analyze	10	0.25
Decide to Cost/Escalate	3	0.25
TOTAL	25 Minutes	1 Minute

RESULTS: 96% REDUCTION. 25X FASTER.

TIER 2 | INCIDENT REMEDIATION

Incident response is much faster with D3, thanks to premium integrations and powerful Tier 2/ MDR playbooks with single-click remediation approvals.

	WITHOUT D3 (MINS.)	WITH D3 (MINS.)
Review Assignment	10	0.5
Validate	10	0.5
Contain and Eradicate	15	2
Remediate	8	2
Report	10	0
TOTAL	53 Minutes	5 Minutes

RESULTS: 91% REDUCTION. 11X FASTER.

TIER 3 | THREAT HUNTING

D3's ability to extract IOCs, as well as TTPs, from incident data and then query other tools and logs for traces of threats makes it a valuable threat hunting tool.

	WITHOUT D3 (MINS.)	WITH D3 (MINS.)
Identify Devices and Admins	15	5
Search for Indicators of Attack	15	2
Correlate Network Logs	15	2
Correlate Endpoint Data	15	3
Gather IOCs (processes, IPs, command line files, etc.)	12	2
Analyze Collected Data and Identify Threat	20	10
Notification	8	1
TOTAL	100 Minutes	25 Minutes

RESULTS: 75% REDUCTION. 4X FASTER.

PLAYBOOK MANAGEMENT

Without the right tools, building and maintaining workflows—especially when they involve connecting to multiple tools—can be a significant cost. D3's low-code playbooks and visual playbook editor make it fast and easy.

	WITHOUT SOAR (MINS.)	WITH TRADITIONAL SOAR (MINS.)	WITH D3 (MINS.)
Workflow Planning	30	30	30
Workflow Implementation	80	25	20
Integrations	60	30	10
Change Control (e.g. R&R firewall vendor)	60	30	2
Playbook Testing	60	15	10
TOTAL	290 Minutes	130 Minutes	72 Minutes

RESULTS: 75% REDUCTION. 4X FASTER.

VULNERABILITY MANAGEMENT

By coordinating the process through D3, clients can make it easier to assess, verify, and remediate vulnerabilities.

	WITHOUT D3 (MINS.)	WITH D3 (MINS.)
Setup and Run Asset Discovery	10	0
Vulnerability Assessment (Run in VM tool. Not counted in totals)	60	60
Identify High-Risk Assets	10	1
Notification	16	1
TOTAL	36 Minutes	2 Minutes

RESULTS: 94% REDUCTION. 18X FASTER.

REAL-WORLD EXAMPLES

CASE STUDY 1

AUTOMATED PHISHING PLAYBOOK

One D3 client used to rely on five tools and 13 steps to complete a simple phishing response workflow. They would receive an alert from PhishMe, download the MSG file, upload the file into their Sandbox, get a manual review from an analyst, and then ban the hash, do a network scan and quarantine the endpoint. Those steps equaled 30 minutes on average.

D3 was able to automate almost the entire process, with all the relevant information presented to the analyst so they can easily determine if it's a true positive. The entire process happens on one interface with full documentation for compliance purposes.

On average the client received 200 suspected phishing events from their end-users per week. For the approximately 164 of these that were false positives, D3 was able to drive the response time down from 15 minutes to three minutes. For the real incidents, D3 reduced the response time from 30 minutes to six. Each week, this organization saved 49 analyst-hours, resulting in annual savings of almost $200,000—all from automating their phishing response.

	BEFORE	AFTER
Phishing Events Per Week	200	200
False Positives	164	164
Minutes to Close Each FP	15	3
True Positives	36	36
Minutes to Close Each TP	30	6
Hours Per Week	59	10
TOTAL	$230,100	$39,000

SAVINGS: 49 HRS/WEEK. $191, 100/YEAR.

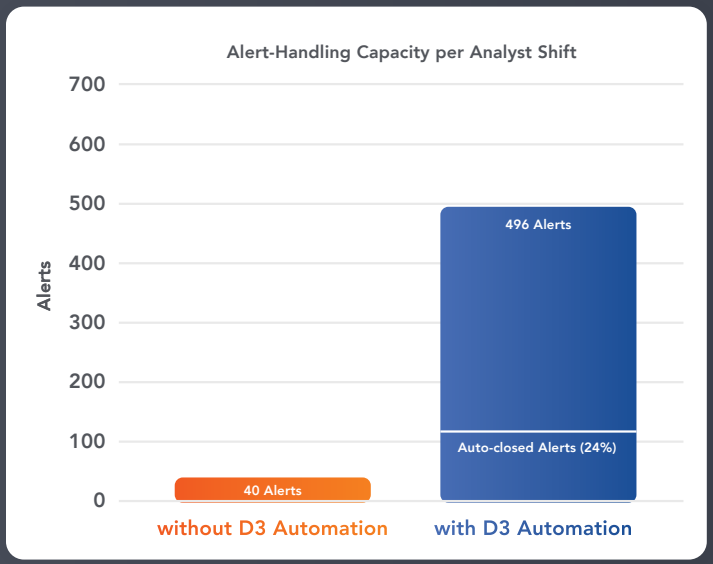
CASE STUDY 2

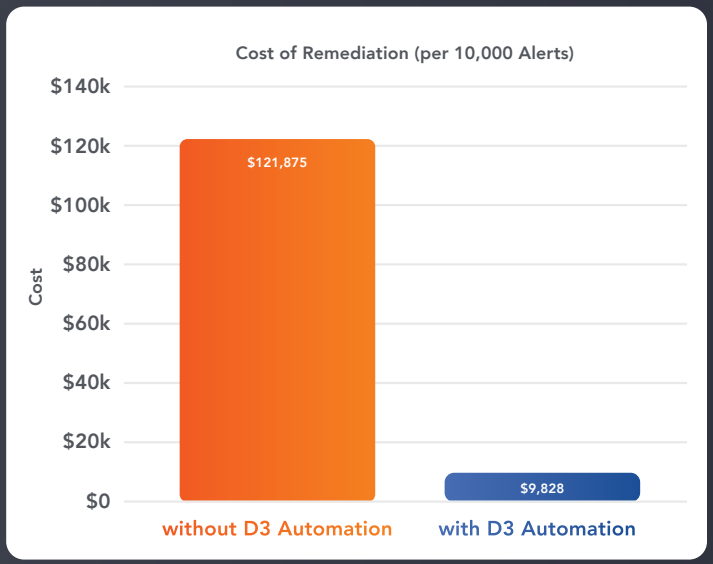
SOC INTEGRATION AND OPTIMIZATION

A global FinTech company added D3 to replace its manual solutions, integrate its many security tools, and provide an alert-handling platform for its MSSP. With D3 helping to automate triage and orchestrating across 10+ tools, the client quickly saw major improvements.

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 the client 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," says Dave, the client's Manager of Security Operations. "But with SOAR, we've got it down to a minute, meaning we can handle 10 times more alerts than before."





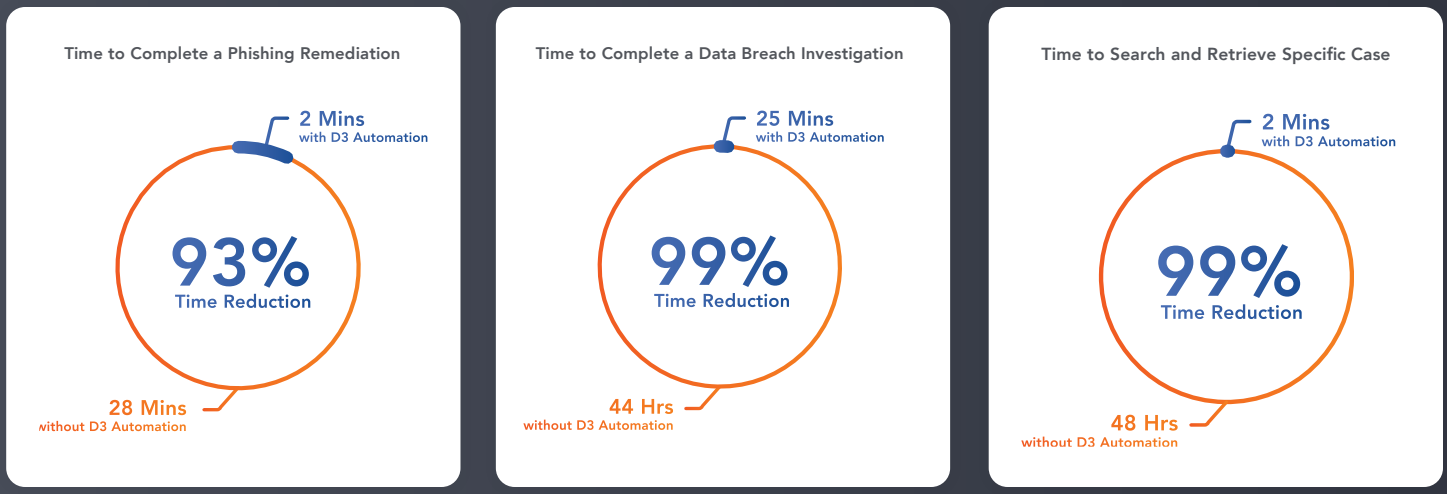
CASE STUDY 3

MULTI-DEPARTMENTAL INCIDENT RESPONSE

A major international bank was in dire need of faster and better coordinated incident response processes that could also meet strict compliance requirements. Their existing security infrastructure created rigid separation between teams and did not support collaboration for cases that required it, such as "cyber SARs", fraud, or security incidents with privacy implications. 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 implemented D3 to act as the backbone for their security operations, integrating the functions of 15 separate solutions into a single console, and providing secure role-based access to 500 users. Seven separate departments use D3, including Privacy, Risk, Compliance, and Computer Forensics.

D3 eliminated the information silos that existed previously, by empowering analysts with case management and data protection controls. This facilitated cross-departmental ownership and accountability within cases. With everyone using D3, teams could work on the same records from any team and any physical location. These operational improvements, combined with the addition of automation-powered playbooks, reduced MTTR by 90% for key incident types.



ABOUT D3 SECURITY

D3 Security's XGEN SOAR platform combines the proactive analysis of MITRE ATT&CK with rapid, end-to-end automation, orchestration and response. Using D3's advanced capabilities, SOC operators around the world have expanded the speed and scale of their security operations, while strengthening their ability to identify suspicious behaviors, conduct efficient investigations, and remediate critical threats.

D3 SECURITY

www.d3security.com

SALES CONTACT

1-800-608-0081 (Ext. 2)
sales@d3security.com

FOLLOW US