



PRODUCT GUIDE

D3 SECURITY NEXTGEN SOAR PLATFORM

NEXTGEN SOAR HAS ARRIVED.

D3 NextGen SOAR with MITRE ATT&CK is the industry's #1 vendor-agnostic security orchestration, automation, and response (SOAR) platform with 300+ integrations, low-code/no-code playbooks, and automated correlation of attacker techniques.



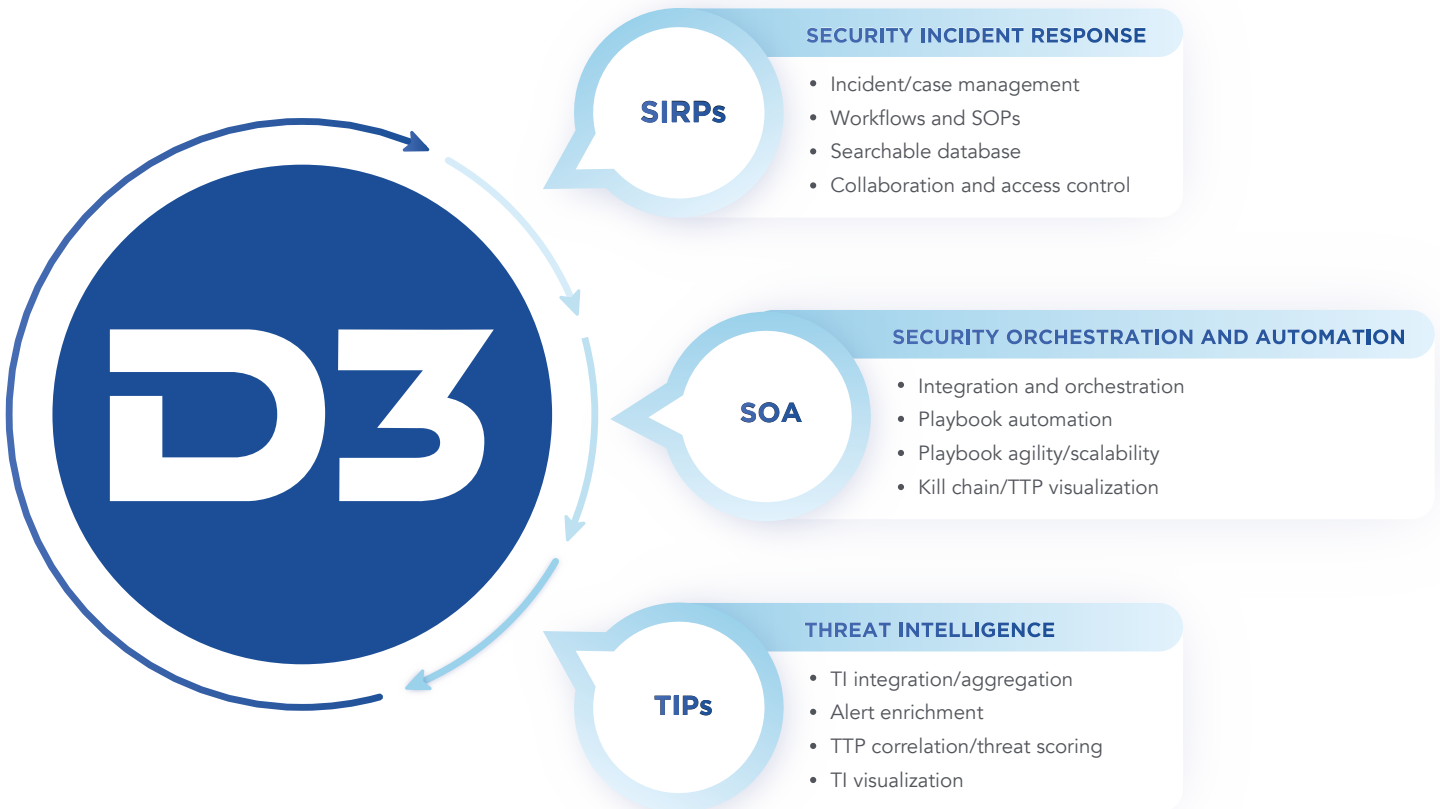
100x
FASTER RESPONSE

300+
OOTB INTEGRATIONS

96%
LESS CODING

EVERYTHING YOU NEED.

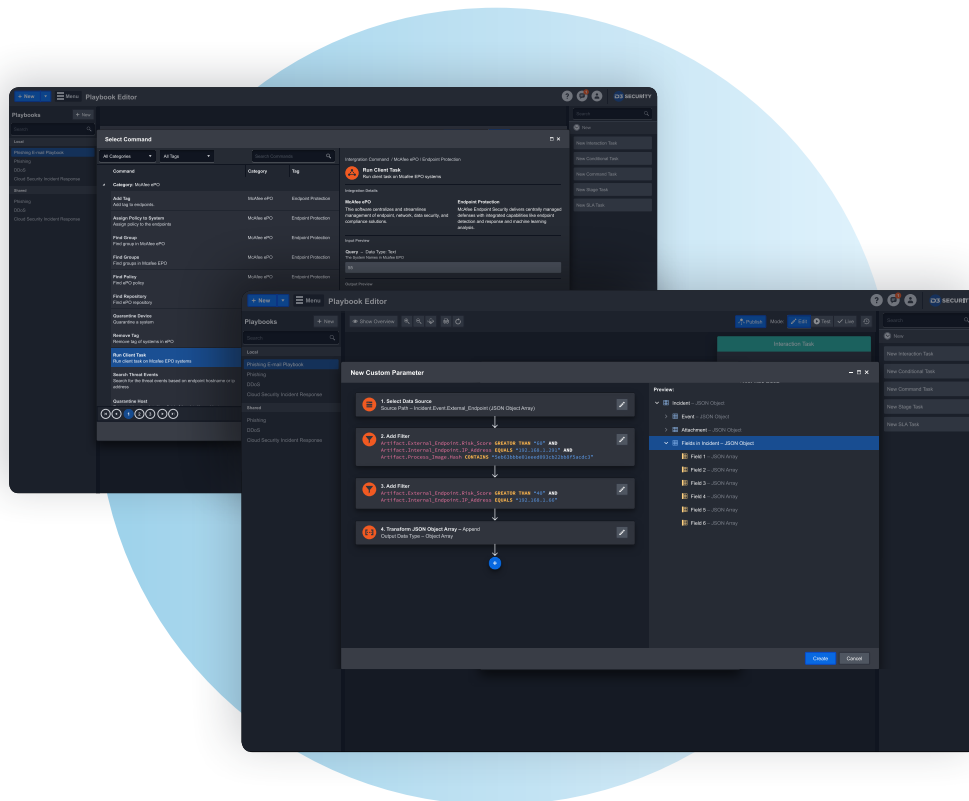
With Security Incident Response, Security Orchestration and Automation, and Threat Intelligence in one platform, D3 provides an all-in-one solution for SOCs and CSIRTs.



D3 brings these capabilities together, dramatically improving the speed, efficiency, and accuracy of security operations, incident response, and threat hunting.

WHAT IS NEXT-GENERATION SOAR?

NextGen SOAR was developed by and for security professionals, to reduce SOAR's operational burden and keep pace with the next generation of fast-moving and evasive threats.



HOW'D WE DO IT?

D3's SOAR experts worked with a council of security leaders who had operated competitive SOAR products as well as previous versions of D3.

The result was deep insight into how "SOAR 1.0" is used in Enterprise and MSSP environments. With the council's help, D3 developed a SOAR product that enhanced valuable existing features and addressed problem areas identified with SOAR 1.0.

On the next page are common complaints regarding playbook management, kill chain context, and integration usability, which are three areas in which NextGen SOAR provides a vastly superior solution.

SOAR 1.0 COMPLAINT

“ BUILDING, UPDATING, AND MANAGING PLAYBOOKS TAKES TOO MUCH TIME AND EFFORT. ”

NEXTGEN SOAR UPGRADE

NextGen SOAR has a codeless playbook editor with drag-and-drop integrations and actions. You don't need Python experts or expensive consultants to create or edit workflows, and you can easily replace tools or data sources, and scale changes across all or some of your playbooks.

SOAR 1.0 COMPLAINT

“ INVESTIGATING IS DIFFICULT BECAUSE SECURITY EVENTS ARE PRESENTED SEPARATELY, WITHOUT TACTICAL CONTEXT.”

NEXTGEN SOAR UPGRADE

NextGen SOAR correlates events using the MITRE ATT&CK Matrix to build out the "kill chain" of cyberattacks, enabling more efficient and focused investigations. NextGen SOAR also presents events in an ATT&CK-based dashboard, providing highly contextualized, at-a-glance management of threats against your environment.






SOAR 1.0 COMPLAINT

“ MY SOAR PLATFORM ISN'T AS VENDOR-NEUTRAL AS I WAS TOLD IT WOULD BE”

NEXTGEN SOAR UPGRADE

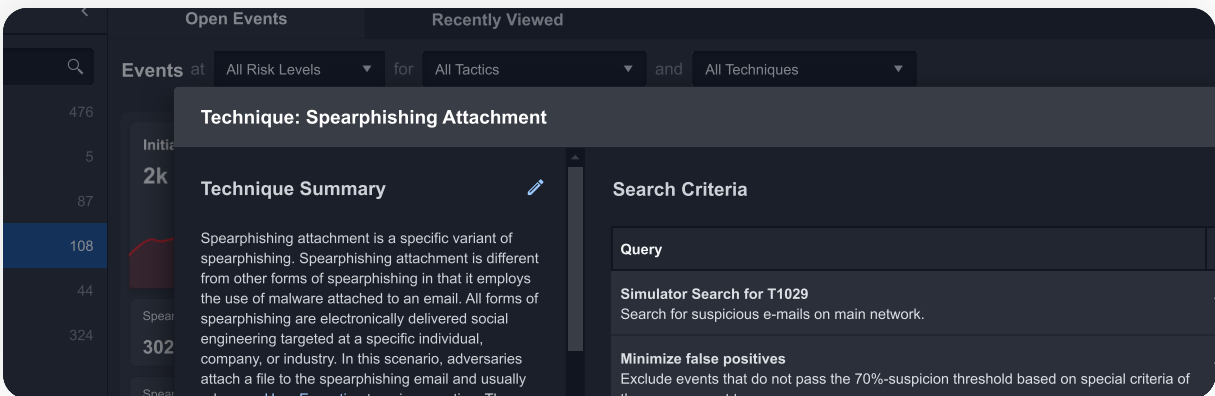
NextGen SOAR is the most widely used vendor-neutral SOAR platform. With 300+ integrations and a 100% focus on SOAR, D3 maintains fully featured integrations and strong client-focused relationships with vendor-partners.

KEY USE CASES.

Integrations Name	Configured
>  McAfee Advance Threat Defense	✓ Yes
>  McAfee ePolicy Orchestrator	✓ Yes
>  McAfee ePolicy Orchestrator	✓ Yes
>  Cisco Umbrella, Secure Internet Gateway in the cloud	✓ Yes
>  Symantec ATP	✗ Mixed

SOC AUTOMATION & INTEGRATION

D3 integrates with more than 300 tools, including SIEM, threat intelligence, ticketing, firewall, endpoint protection, and other systems, so you can consolidate signals, manage tasks, and act on insights from a single pane of glass. D3 uses these integrations to automate actions across your environment, gathering data and orchestrating playbooks with no user intervention required for rote tasks.



The screenshot displays the D3 interface with a search filter for 'Technique: Spearphishing Attachment'. The interface shows a list of events on the left and a detailed view of the selected technique on the right. The detailed view includes a 'Technique Summary' and 'Search Criteria'.

Technique: Spearphishing Attachment

Technique Summary

Spearphishing attachment is a specific variant of spearphishing. Spearphishing attachment is different from other forms of spearphishing in that it employs the use of malware attached to an email. All forms of spearphishing are electronically delivered social engineering targeted at a specific individual, company, or industry. In this scenario, adversaries attach a file to the spearphishing email and usually rely upon User Execution to gain execution. These

Search Criteria

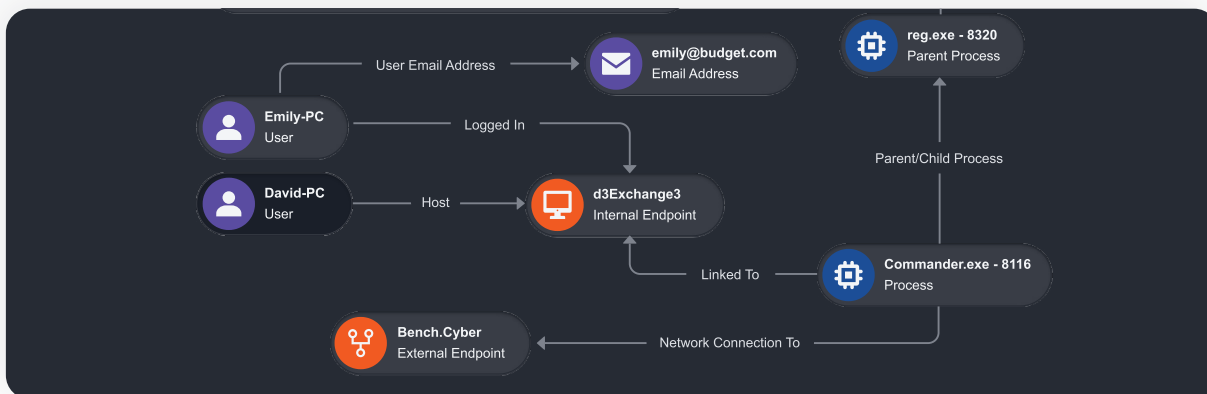
Query

Simulator Search for T1029
Search for suspicious e-mails on main network.

Minimize false positives
Exclude events that do not pass the 70%-suspicion threshold based on special criteria of the management team.

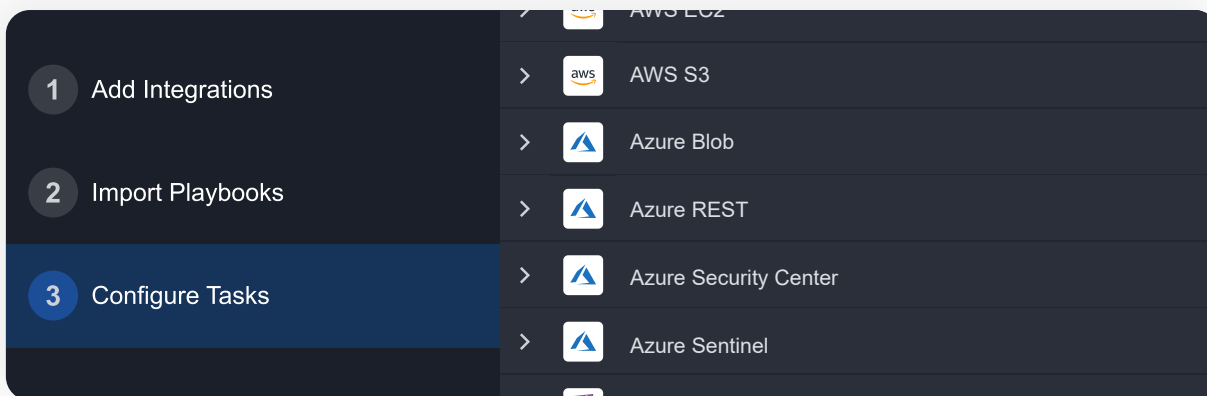
EVENT ENRICHMENT

By the time you see an event in D3, it has already been enriched with contextual data from threat intelligence platforms, past incidents, and the MITRE ATT&CK matrix (or other TTP framework). This allows you to make quick, well-informed decisions that eliminate false positives and zero in on genuine threats.



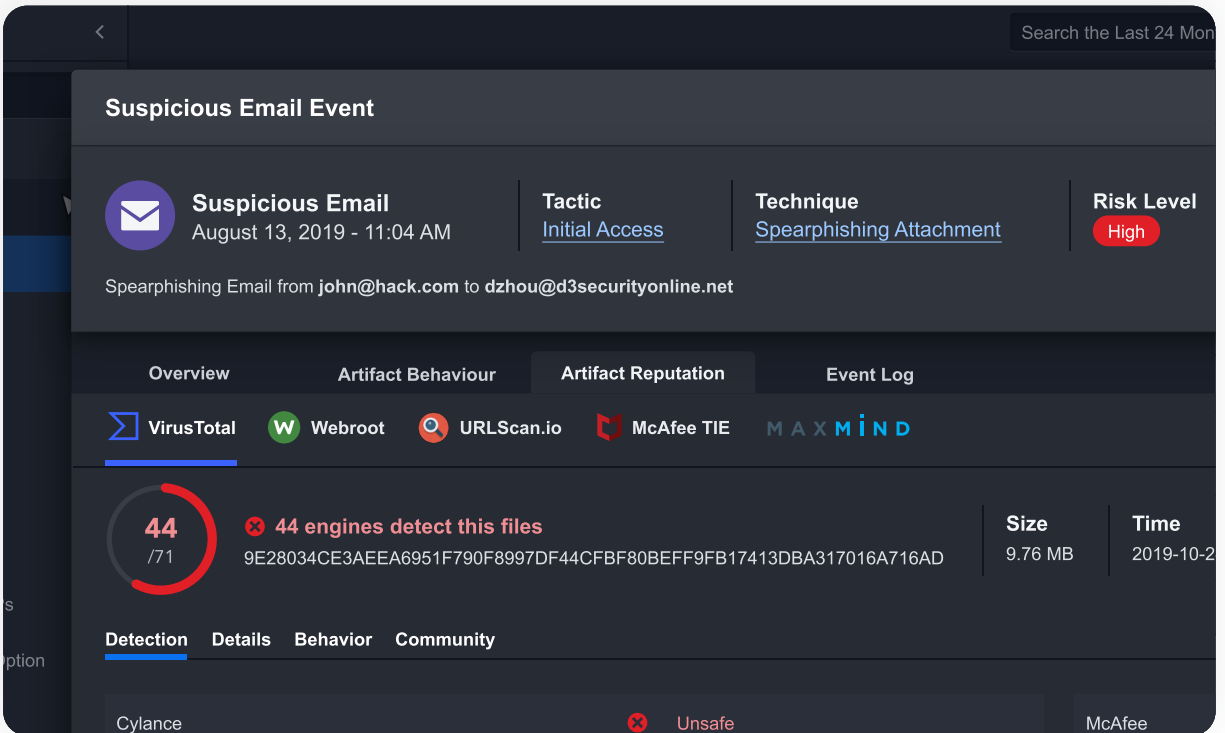
INVESTIGATION MANAGEMENT

Serious security incidents like data breaches require thorough investigations that extend beyond simple remediation to address their full implications. D3 gives you the tools you need to close incidents and address their root causes. With D3 you can escalate incidents and group them together into cases to collaborate with colleagues, conduct link analysis, build out timelines, and even loop in other teams, such as Compliance, Legal, and HR.



CLOUD SECURITY ORCHESTRATION

Most organizations now host some of their systems and data in the cloud, which complicates their security with gaps and redundant toolsets. D3 can orchestrate across cloud and local environments seamlessly, enabling automated response to complex threats such as cryptojacking.



PHISHING INCIDENT RESPONSE

For most SOCs, phishing attempts are the most common security incident. D3 streamlines and automates phishing response by monitoring phishing inboxes, extracting the IOCs from flagged messages, and correlating against integrated threat intelligence sources. If the message is confirmed to be malicious, D3 orchestrates a response action to isolate affected endpoints, block the URL, notify employees, and more.

INTEGRATIONS.

Customers rely on SOAR for their integrations, which is why NextGen SOAR integrates with 300+ products, ranging from SOC and InfoSec tools, to IT forensics, DevOps, cloud operations, physical security, privacy and more. Our breadth of integrations ensures that you will be able to leverage your entire tech stack—without compromise. Out-of-the-box integrations are “codeless”, meaning they can be set up in just a few clicks.

FEATURED PARTNERS

We have established technology partnerships that ensure our certified integrations are always fully featured and easy to leverage. These featured integrations include:



SIEM, threat intelligence, endpoint protection, and network security



Graph Security API, Azure cloud security tools, Exchange, and more. D3 is a member of the Microsoft Intelligent Security Association.



Endpoint protection, email security, threat protection, data loss prevention, and more.



Endpoint protection, network security, malware analysis, and threat intelligence.



Cloud security and application monitoring



Firewall, SIEM, and more



Cloud SIEM



Threat intelligence

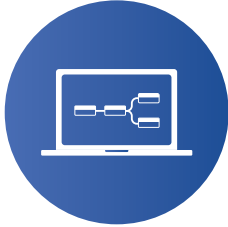


Endpoint protection



Network security

BENEFITS AND CAPABILITIES.



Enable a SOC Workbench

- Single platform for the SOC
- Monitor, ingest and enrich events; convict incidents
- Trigger remediation playbooks
- Manage tasks and cases



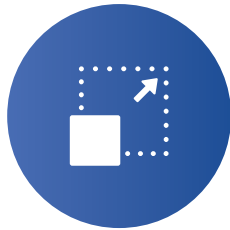
See Beyond Individual Events

- Put events in kill chain context
- Focus SOC resources on riskier events (e.g. those closest to network access, data access)
- Leverage MITRE ATT&CK to better prioritize events and assignments
- Use MITRE ATT&CK to understand the weak points in your security



Identify the Root of the Problem in Seconds

- Reveal the who, what, where, and when of security threats
- Visualize relationships between entities and IOCs
- Enable timelines, link analysis, and storylines
- Drill down on elements to reveal the source event/data



Build Consistent, Automated, Scalable Processes

- Guide analysts, boost productivity
- Eliminate costly busy work and workarounds
- Create custom workflows or use built-in libraries
- Grow your SOC processes seamlessly as your organization grows
- Easily onboard new analysts and processes



Make Working Together Easy

- Collaboration made easy
- Access controls
- Automatically route notifications and updates
- Make sure everyone is working off the latest information
- Stay aligned

ADVANTAGES FOR MSSPs.

D3 NextGen SOAR is the ideal platform for MSSPs who want to increase profit margins, streamline their operations, and enhance their offering to clients. D3's multi-tenancy and robust access controls make it easy to securely segregate each client's data and workflows for easy management of multiple environments.

Playbooks and reports can be applied to individual clients, groups of clients, or scaled across all clients. This allows for complete customization when necessary while supporting efficient bulk deployment that eliminates redundant work.

D3 is a valuable tool whether the MSSP is fully or partially managing a client's security, because D3 aggregates data and orchestrates actions across the entire security stack, regardless of whether the MSSP has direct access to every tool. This closes gaps in security workflows and reduces the reliance on communication between the MSSP and the client's internal security team.

The screenshot displays the 'Set Default Integrations' configuration screen in the D3 SECURITY Guided Setup. The interface is dark-themed with a sidebar on the left and a main content area on the right. The sidebar includes 'User Management' (checked), 'Playbook Configuration', and a numbered list of steps: 1. Add Integrations, 2. Add Playbooks, and 3. Set Default Integrations (highlighted). The main content area shows 'Integrations Categories' with expandable sections for 'Communications', 'Email', and 'Endpoint Protection'. Under 'Endpoint Protection', there is a table with columns for 'Actions' and 'Integration'. The table lists several actions and their corresponding integrations: 'Isolate Host' (Cisco AMP for Endpoints), 'Release Host By Hostname' (Cisco AMP for Endpoints), 'Get Alerts' (CylancePROTECT), 'Get Host Info' (CylancePROTECT), and 'Get Hash Info' (Cisco AMP for Endpoints). A circular inset on the right shows a dashboard with various charts and data points.

Set Default Integrations

D3 SECURITY
Guided Setup

User Management

Playbook Configuration

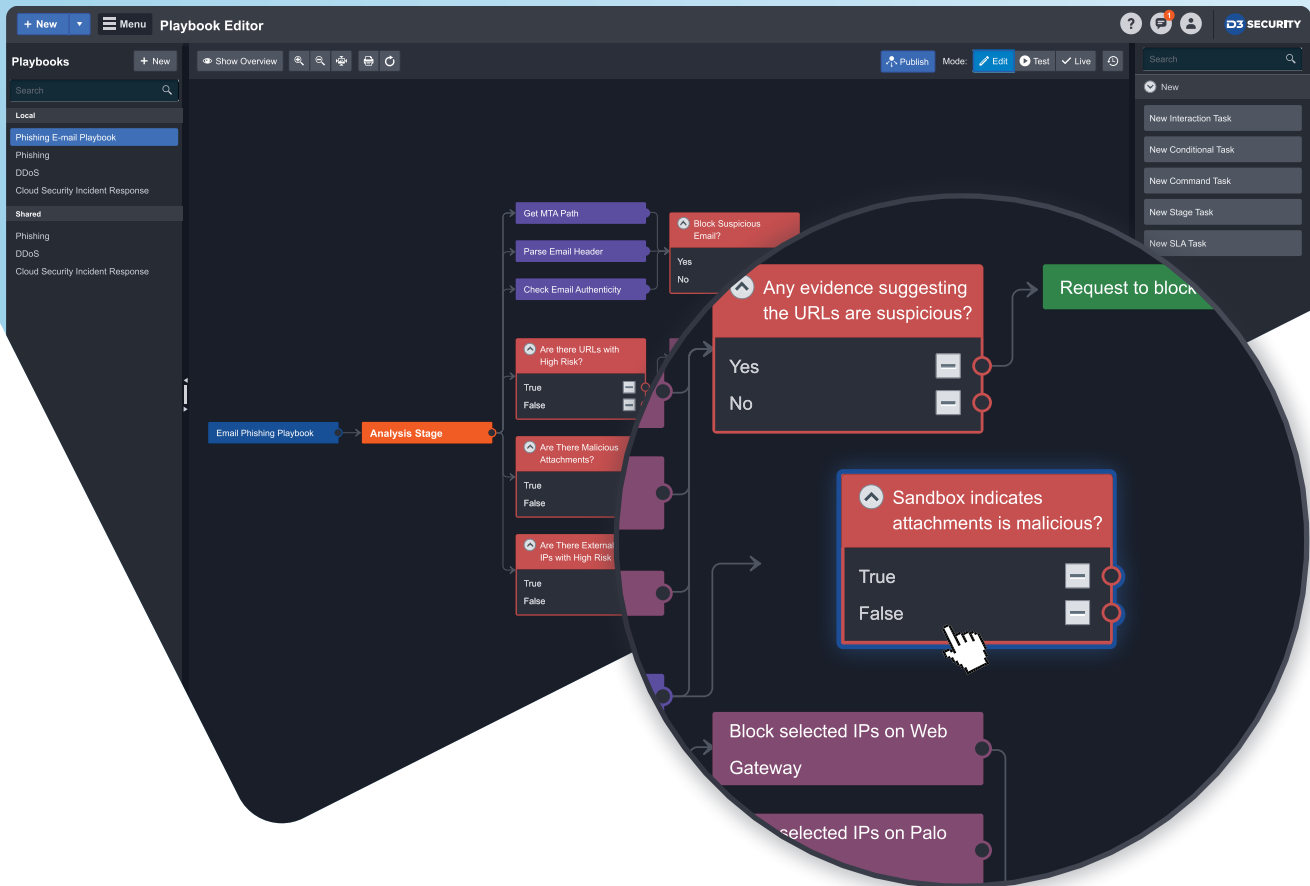
- 1 Add Integrations
- 2 Add Playbooks
- 3 Set Default Integrations

Integrations Categories

- ▶ Communications
- ▶ Email
- ▼ Endpoint Protection

Actions	Integration
Isolate Host	Cisco AMP for Endpoints
Release Host By Hostname	Cisco AMP for Endpoints
Get Alerts	CylancePROTECT
Get Host Info	CylancePROTECT
Get Hash Info	Cisco AMP for Endpoints

KEY FEATURES.



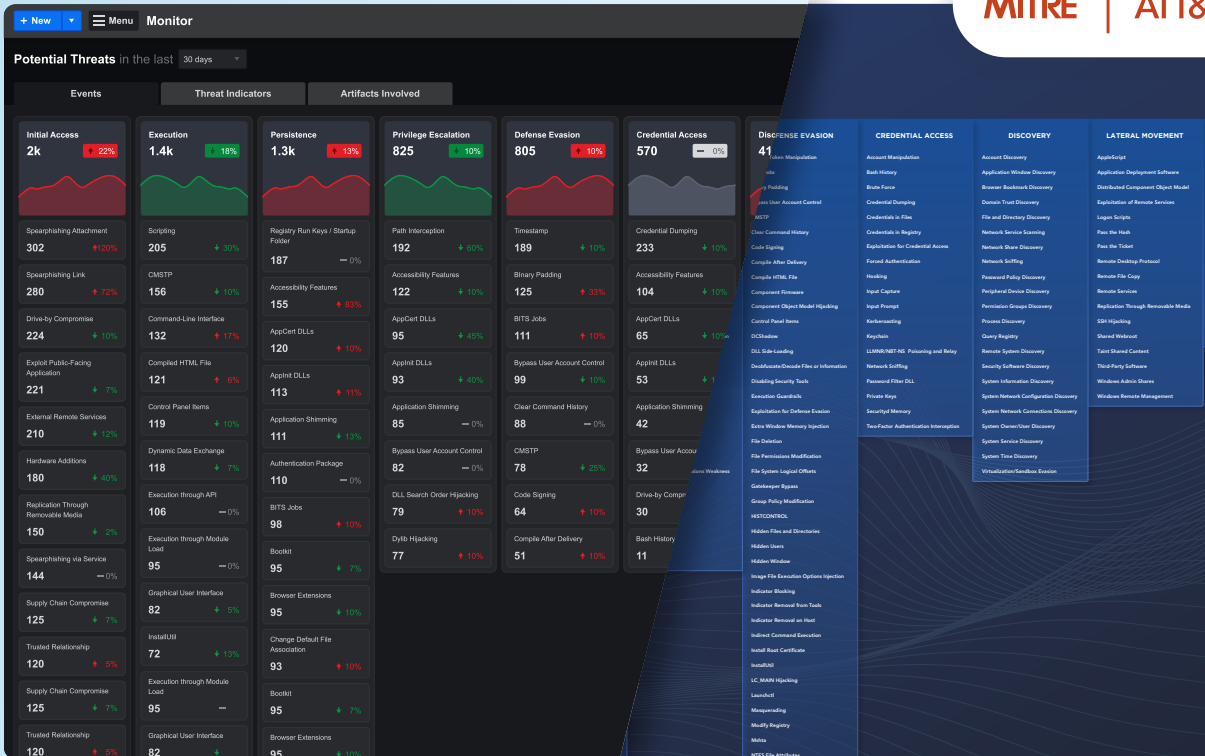
CODELESS PLAYBOOKS

D3's playbooks are the heart of the platform, with fully customizable workflows that automate tasks and coordinate actions across your tools and workforce.

The visual canvas allows users to simply drag and drop automated actions and manual steps into their workflows, with no coding required. This eliminates most of the time and expense required to create and maintain playbooks, which is a huge hidden cost for most SOAR platforms.

Nested playbooks make the visual canvas even simpler by enabling smaller automated sequences to be dropped into playbooks as a single step.

Where most SOAR playbooks end, D3's full-lifecycle playbooks keep going to standardize the complete investigation, ensuring efficient, compliant, and legally sound procedures are applied to sensitive matters like insider threats, regulatory issues, and digital evidence management.

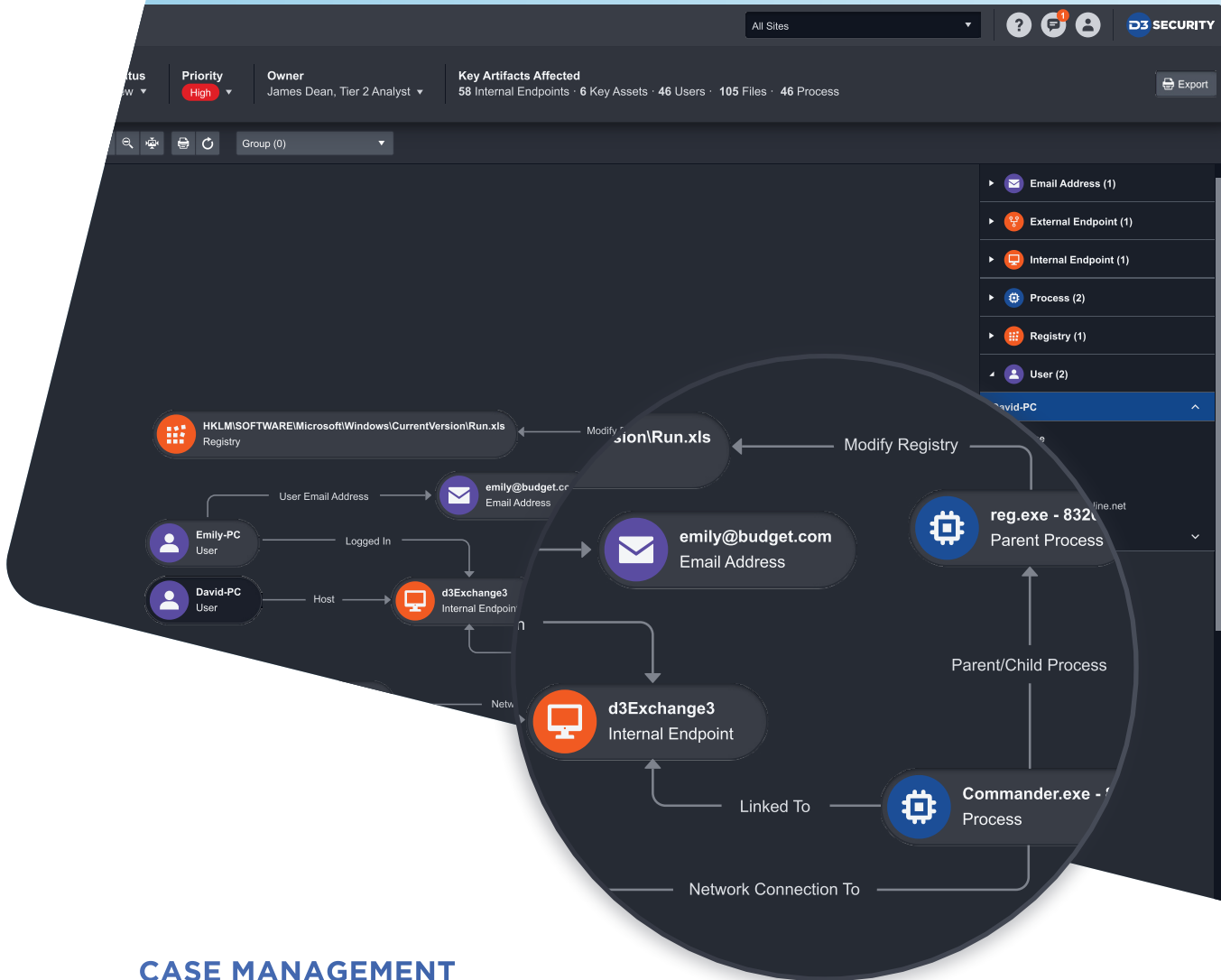


MITRE ATT&CK

Understanding what your adversaries are trying to do empowers you to get a step ahead and disrupt their attacks. D3 uses the MITRE ATT&CK Matrix, the world's largest knowledgebase of cyber adversary tactics, techniques, and procedures (TTPs), to make sense of threats and vulnerabilities.

All events go through TTP correlation against MITRE ATT&CK. Instead of deciphering the raw event data, D3 users immediately know what technique is being used against them, how it connects to a larger objective, and how to stop it.

The Monitor Dashboard gives analysts the perfect "at-a-glance" home screen from which to monitor the occurrence of TTPs in their environment. Other screens provide detailed lists of the indicators and artifacts extracted from those events, along with a map view representing their source locations.



CASE MANAGEMENT

D3 goes beyond simple triage to manage larger cases and investigations. Related incidents can be grouped together into cases, where the connections between them can be revealed through link analysis, timelines, and correlations across the artifacts database.

D3 extends case management to digital forensics use-cases, with evidence tracking and chain-of-custody capabilities for digital and physical artifacts.



REPORTING AND ANALYTICS

Having visibility into your security operations is the best way to make continuous improvements and identify problem areas.

D3 provides a comprehensive set of SOC metrics that can be compared against predetermined benchmarks, including average response times, number of incidents by type or timeframe, and open and closed tickets for each analyst.

All of the many fields in D3 can be reported on, enabling custom dashboards, charts, trend reports, and summaries. Reports can be automated, scheduled, and shared securely, with the ability to save custom reports for reuse.

Because D3 eliminates data silos and aggregates security data from the entire infrastructure, it also makes compliance reporting much easier. Compliance reporting templates for common reports are even provided in the system.

CUSTOMER STORIES.



“ THROUGH D3, WE HAVE COMPLETELY ELEVATED OUR SECURITY ORCHESTRATION, INCIDENT RESPONSE, AUDIT, AND COMPLIANCE CAPABILITIES.”

— The Bank’s Chief Security Officer

INTERNATIONAL BANK

This international bank conducted a review of its processes and determined that it needed a new technology solution to the challenges posed by the volume of cyberthreats facing its SOC combined with the burden of documentation and collaboration inherent in the financial industry.

CHALLENGE

Ad hoc and manual processes created enrichment and remediation bottlenecks.

Disparate tools made it difficult for the SOC to coordinate with other teams.

Complex investigations were too slow to keep pace with sophisticated attackers.

SOLUTION

D3 reduced the bank’s MTTR by 93% for key incident types by automating steps and orchestrating intelligence gathering.

D3 provided case management and data protection controls that facilitate cross-departmental ownership and accountability within cases, regardless of team or location.

D3 reduced the time to complete a data breach investigation from 44 hours to 26 minutes by centralizing the functions of 15 separate tools onto one interface.



“ THE D3 SOAR PLATFORM HAS SCALED EFFECTIVELY TO HELP AUTOMATE AND ORCHESTRATE SECURITY OPERATIONS AND INCIDENT RESPONSE ACROSS MULTIPLE SIEMS, THREE TEAMS OF ANALYSTS, AND DOZENS OF BLUE-CHIP LEVEL CUSTOMERS.”

— The MSSP’s CSIRT Leader

APAC-BASED MSSP

This MSSP provides outsourced IT and managed security services to energy, finance, government, manufacturing, and telecom organizations. Its SOC manages day-to-day security operations, while its 40-analyst CSIRT is responsible for incident remediation for approximately 50 clients. Before D3, the MSSP had another SOAR solution in place, but found that platform could not meet their automation, reporting, and scalability needs.

CHALLENGE

Ad hoc and manual processes created enrichment and remediation bottlenecks.

Disparate tools made it difficult for the SOC to coordinate with other teams.

Complex investigations were too slow to keep pace with sophisticated attackers.

SOLUTION

D3 reduced the bank’s MTTR by 93% for key incident types by automating steps and orchestrating intelligence gathering.

D3 provided case management and data protection controls that facilitate cross-departmental ownership and accountability within cases, regardless of team or location.

D3 reduced the time to complete a data breach investigation from 44 hours to 26 minutes by centralizing the functions of 15 separate tools onto one interface.

WE'RE HERE TO HELP

D3 Security's SOAR platform empowers many of the world's most complex organizations with a full-lifecycle solution to standardize, automate, and accelerate incident response and case management processes to reduce risk and combat threats.

D3 SECURITY

www.d3security.com

SALES CONTACT

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

FOLLOW US

