

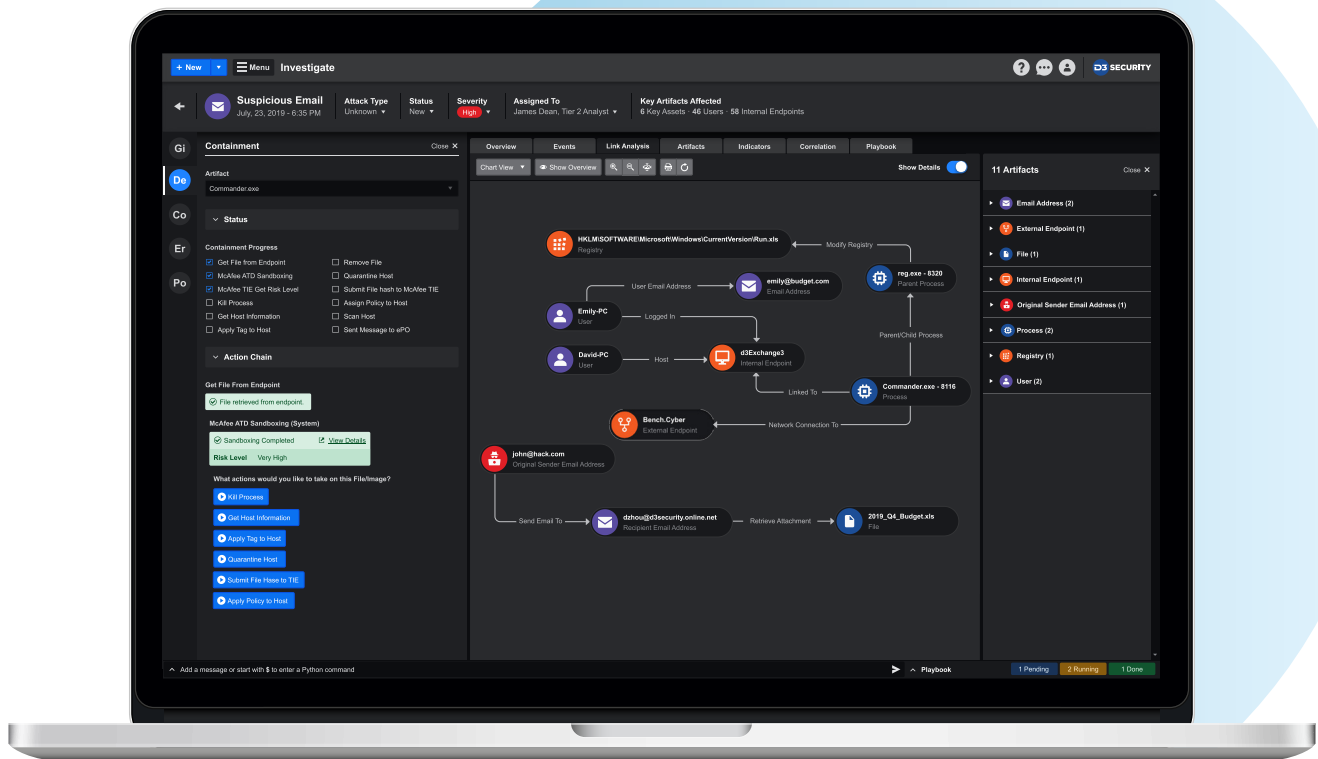


PRODUCT GUIDE

D3 SOAR

Automated Incident Response & Security Orchestration

1. WHY D3?



1.1 SOC CHALLENGES

There are several challenges that are nearly universal in SOCs. The well-documented “skills gap” in cybersecurity makes it difficult and expensive to hire and retain a team of skilled employees. This is exacerbated by the fact that SOC analysts end up spending most of their time chasing after false positives and performing repetitive tasks like gathering contextual data. This results in high levels of analyst burnout, and wasted potential across the SOC.



1.2 LEGAL AND COMPLIANCE CHALLENGES

Incident response is also complicated by legal and regulatory compliance requirements. Depending on the industry and region, organizations may be subject to multiple strict obligations surrounding data privacy, incident documentation, suspicious activity reports, and more. In scenarios like audits, lawsuits, or major data breaches, organizations will be required to produce detailed data related to incidents. The complex and dynamic nature of compliance makes the risk of fines or other punitive measures significant for most organizations.

1.3 THE BUSINESS CASE FOR D3

Given the daunting challenges that SOC's are facing, the business case for D3's Cyber Incident Response Platform should be clear. As will be described in more detail throughout this guide, D3's value includes:



Increasing the effectiveness of analysts at all levels of experience, while severely reducing the time they spend on menial tasks and false positives.



Helping organizations avoid compliance violations.



Preventing costly and damaging incidents, such as ransomware attacks and data breaches, by identifying root causes and vulnerabilities.

1.4 WHAT MAKES D3 DIFFERENT?

D3 is unique among SOAR vendors for many reasons. Some of our key differentiators include:



MITRE

SOAR 2.0

D3 is the only SOAR platform to support intelligent correlations and intent-based response through the MITRE ATT&CK matrix.



\$

Pricing

D3 offers simple and predictable per-user pricing. We do not charge based on data volume or number of automated actions.



No Coding Required

All integrations are built in the back end, with no reliance on user-built Python scripts.



Visual Playbook Editor

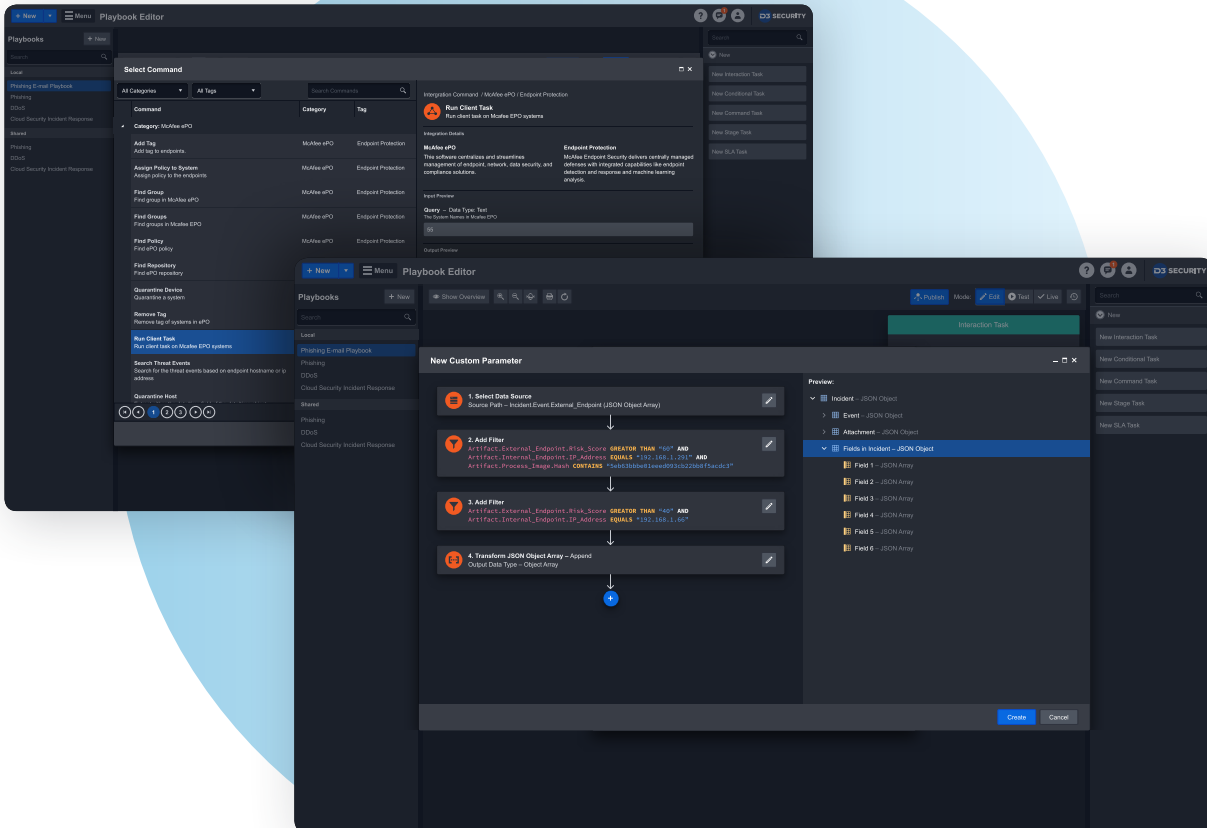
D3 playbooks can be edited on the fly with an intuitive drag-and-drop interface, including to add automated actions to workflows.



Deep Case Management

D3's case management features go further than any other SOAR platform, including support for audit and compliance requirements.

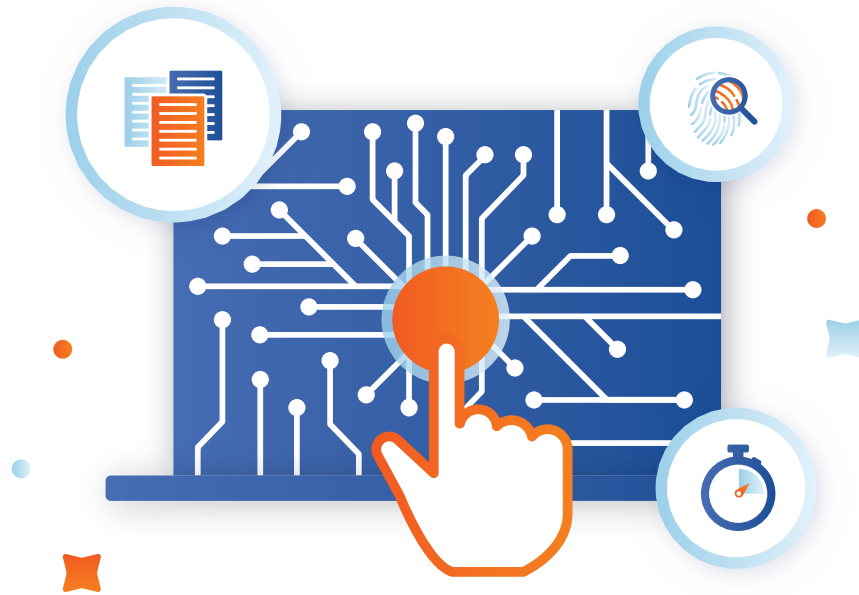
2. AUTOMATION & ORCHESTRATION



2.1 DATA ENRICHMENT

D3's automated data enrichment helps contextualize, prioritize, and streamline your incident response processes. When an event is ingested into D3, via a SIEM, email protection system, ITSM, or other tool, D3 parses the elements of the event, such as IP addresses, domains, and attack techniques. These elements are then automatically correlated against threat intelligence sources, historical data, and D3's embedded MITRE ATT&CK matrix to enrich the event with full contextual information and a risk score that can be used to direct the event to an appropriate analyst or flag it as a likely false positive.

See Section 4 for more on how D3 leverages the MITRE ATT&CK matrix.



2.2 AUTOMATED ACTIONS

D3's automation of security actions shuts down threats at machine speeds and frees up analysts from busywork. D3 users can trigger actions across integrated tools such as endpoint protection systems and firewalls, all without leaving the D3 interface. Automated actions might include blocking a hash, disabling a User ID, blacklisting an IP address, or any other task that can remediate a threat before it does further damage.

See Section 5.2 for how automated actions fit into D3's Visual Playbook Editor.

2.3 TASK ORCHESTRATION

D3 supports collaboration and coordination in real time to ensure that everyone has the latest data. D3 can send automated tasks assignments, notifications, approval requests, and other communications. Uniquely, D3 supports collaboration throughout the entire organization, not just within the security team. Orchestrating through D3 allows you to loop in Legal, Compliance, HR, and PR teams, or even the board of directors, while maintaining information security and privacy standards.

See Section 7 for more on D3's dashboards.

3. INTEGRATIONS

D3 integrates with 200+ tools, making it the central nervous system of the SOC. D3's integrations include all of the major SIEMs, dozens of threat intelligence sources, and hundreds of other security tools, including leading endpoint protection systems, firewalls, email protection systems, sandboxes, and more. D3 has many certified partnerships with key vendors, enabling feature-rich bidirectional integrations.



Carbon Black.



4. ATTACKBOT

4.1 THE MITRE ATT&CK MATRIX

The MITRE ATT&CK matrix is an evolution of the intrusion kill chain, which was developed by Lockheed Martin in 2011 to describe the steps that an adversary is likely to take during a cyberattack. ATT&CK specifically focuses on aiding post-compromise detection, and instead of phases, breaks attacks down into 12 “tactics” (what the adversary is trying to accomplish), each with a number of “techniques” (the specific methods they might use to achieve that goal). Some tactics have dozens of associated techniques, making the ATT&CK matrix a deep database of adversary behavior, based on real-world cybersecurity incidents and detailed research.



4.2 MONITOR: INTELLIGENT CORRELATION, ANALYSIS, AND THREAT HUNTING

D3 has embedded the entire MITRE ATT&CK matrix into its software to create a unique vision of SOAR that exists in no other platform. When an event is ingested into D3 from a SIEM, EDR, firewall, or other tool, ATTACKBOT parses the indicators of the event and checks them against search criteria for ATT&CK tactics and techniques. The occurrence of every tactic and technique are displayed on the primary dashboard in the Monitor module, giving Tier 1 analysts a clear view of the most important threats in the environment.

See Section 7.1 for more on D3's MITRE ATT&CK dashboard.

4.3 INVESTIGATE: INTENT-BASED RESPONSE

Any event can be escalated to the Investigate module for a closer look. When an event is escalated, ATTACKBOT pulls in all the correlated techniques, events, and artifacts, building the possible kill chain of the larger incident. All the correlated elements are placed under continuous surveillance, revealing more about the attack as time goes on. Using the ATT&CK framework to reveal the kill chain enables “intent-based” response, whereby analysts can anticipate the attacker's next steps to prevent them from reaching their goals. At any point, the analyst can trigger a playbook that is automatically built out based on what information is known about the incident.

See Section 5 for more on D3's playbooks.

5. PLAYBOOKS



5.1 FULL LIFECYCLE PLAYBOOK ENGINE

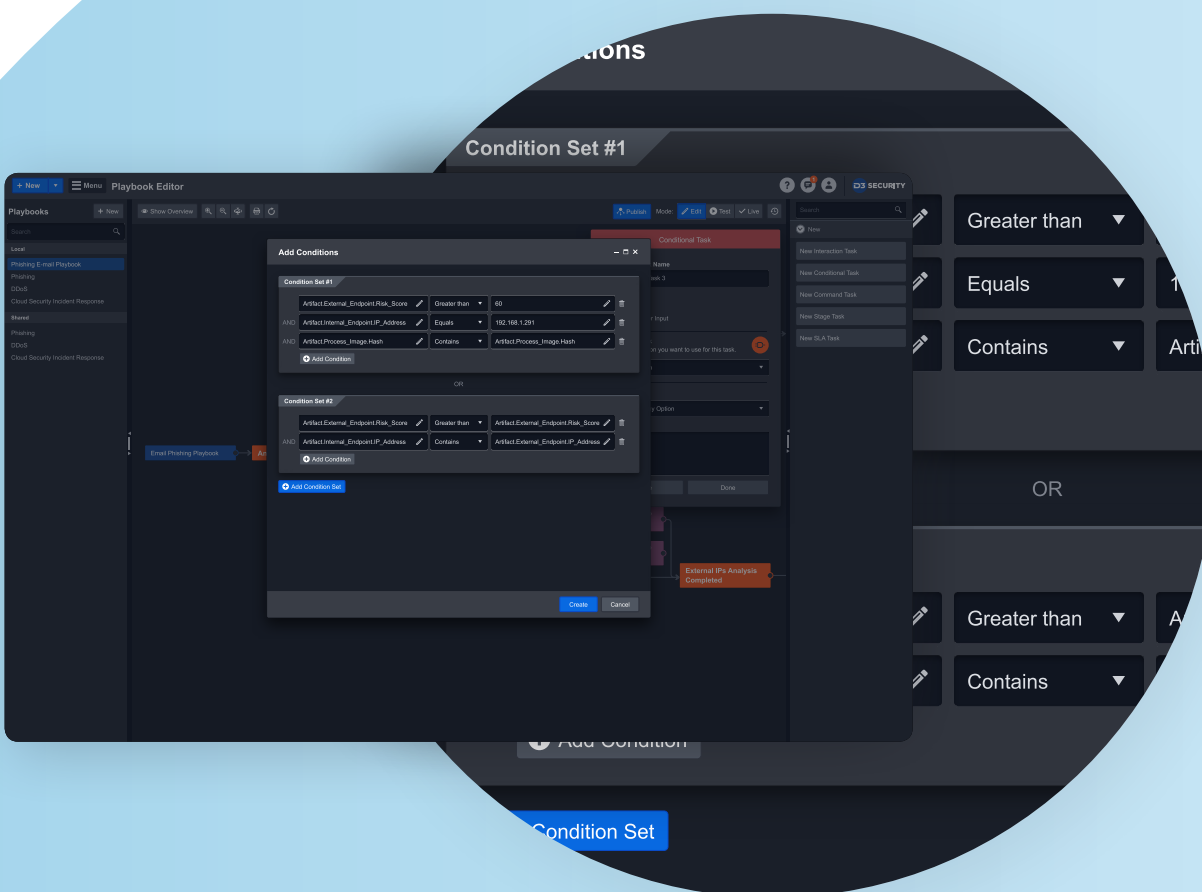
When an analyst triggers a response playbook, D3's playbook engine jumps into action by mapping all of the known information—including ATT&CK Intelligence—into the playbook and generating the steps needed for remediation. D3's playbook library provides a tailored action plan for each incident type that carries responders through all the phases of incident response.

5.2 VISUAL PLAYBOOK EDITOR

D3's playbook editor allows you to visualize and dynamically edit your workflows during preparation or response. Analysts can "drag and drop" automated actions at any point within the playbook, even on the fly.

5.3 PLAYBOOK LIBRARY

The foundation of a strong incident response program is the playbooks you use to guide your processes. Playbooks expedite response times by removing uncertainty, and ensure that your entire team is working together following proven steps. Strong playbooks can elevate the contributions of junior employees, by embedding industry best practices and the wisdom of senior personnel into the workflow. D3 has a library of industry-standard playbooks, primarily built to the NIST 800-61 standard, but also including other frameworks such as SANS. In addition to the playbook library, D3 allows for full or partial customization, so that you can adapt workflows to your precise needs.



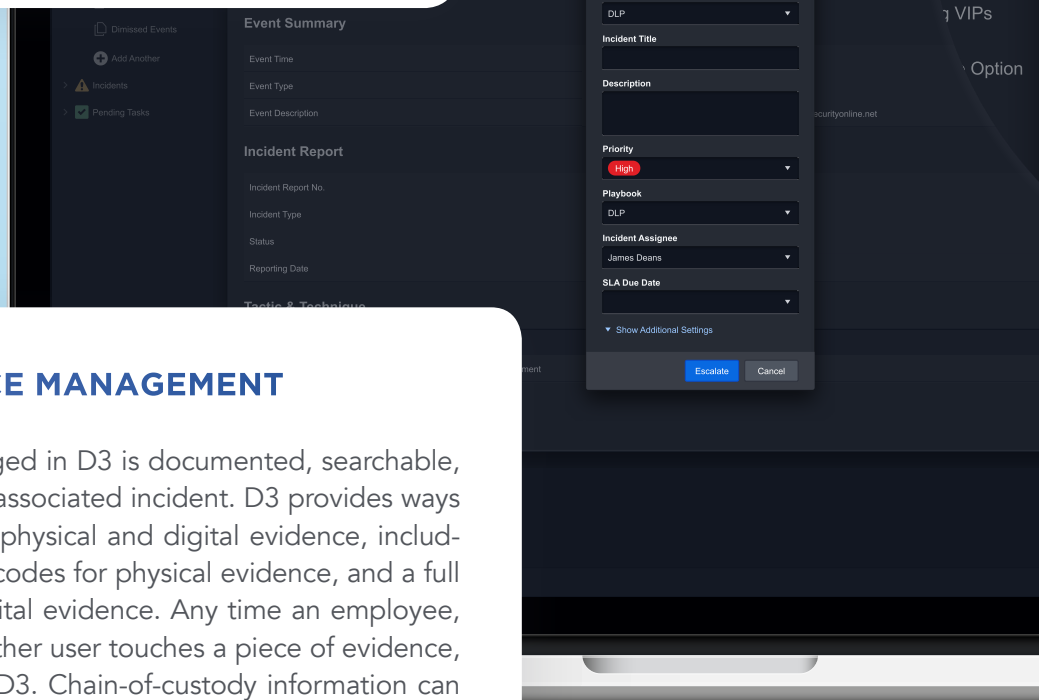
6. CASE MANAGEMENT

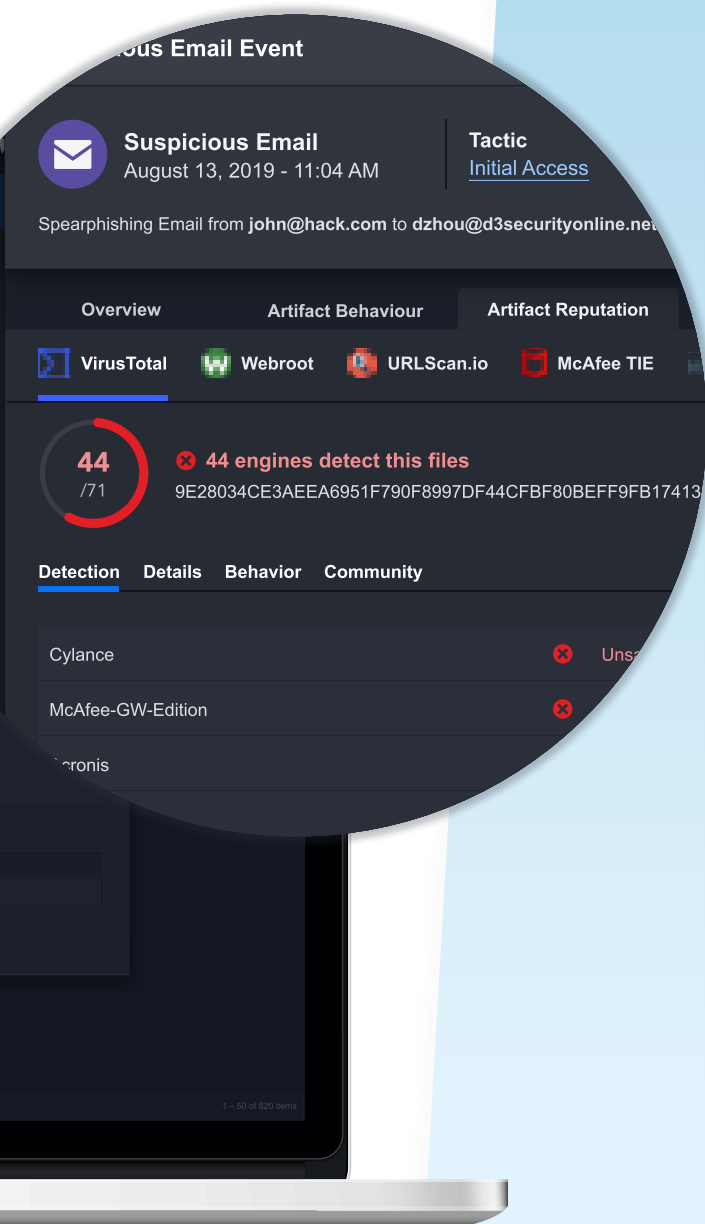
6.1 CASE MANAGEMENT WORKFLOW

Incidents are often linked through the method of attack, the source, the target, or the persons involved. For these instances, D3's case management module allows you to bring multiple incident reports together for deeper analysis and collaboration between multiple analysts within a single case. In order to standardize your procedures and get maximum value out of junior investigators, D3 guides you through the investigation process, with detailed steps, suggestions, interview scripts, email templates, and more.

6.2 EVIDENCE MANAGEMENT

All evidence logged in D3 is documented, searchable, and linked to its associated incident. D3 provides ways to manage both physical and digital evidence, including printable barcodes for physical evidence, and a full audit trail for digital evidence. Any time an employee, investigator, or other user touches a piece of evidence, it is recorded in D3. Chain-of-custody information can be viewed, reported on, and exported by users with the necessary privileges. This capability is useful for legal or regulatory issues that might require you to generate a granular list proving the complete chain of custody for a piece of evidence.





6.3 DATA PROFILING

Artifacts Database

D3 allows you to retain a centralized record of the artifacts that are implicated in incidents. This might include people, IP addresses, host names, infected machines, IOCs, malware variants, and nefarious URLs.

Link Analysis

D3's Link analysis is how you establish, visualize, and understand the connections between artifacts, incident records, external data sources, and other data points that your system records. Analysts can use a visually displayed web of connected artifacts to understand the timeline of a cyberattack, see its connections to previous incidents, and accelerate their response by retrieving additional information on any artifact with a single click.

Incident Timeline

D3 automatically generates a detailed timeline of each event. The system timestamps every correlated adversary action, incident creation, escalation, status change and security action, showing how the incident is unfolding and what is likely to happen next. Elements within the timeline can be clicked on to reveal more granular insights, such as threat intelligence or relevant approvals.

7. REPORTING & DASHBOARDS

7.1 MITRE ATT&CK DASHBOARD

D3's Monitor module features a dashboard that displays the detection of MITRE ATT&CK tactics and techniques in real time. This dashboard provides at-a-glance trend analysis to show what the most relevant threats are in your environment. D3 tracks the events, indicators, and artifacts related to each technique, giving you the ability to drill down on any of them for investigation. The default dashboard is based on ATT&CK, but the format can be fitted to any TTP criteria you use in your SOC.

See Section 4 for more about how D3 has embedded MITRE to enable intelligent SOAR.

7.2 METRICS, BENCHMARKS AND KPI'S

As the saying goes, "what gets measured, gets managed." So for your incident response processes to improve over time, team leaders need to have access to relevant metrics. D3 can track a wide range of metrics that will help you assess performance and compare against predetermined benchmarks, including:



Number of incidents within a timeframe, broken down by incident type.

Response times: average time to detect, remediate, and close.

Time spent on each phase of response, in order to identify procedural bottlenecks.

Employee performance, such as number of open and closed tickets.

7.3 ANALYSIS REPORTS

Every field in D3 is reportable, making it easy to visualize data in dashboards, link analysis, charts, trend reports, or summaries for senior management. D3's reporting features also support the important process of post-incident reviews, with information like root cause, time to detection, response playbook used, and lessons learned.

7.4 REPORT MANAGEMENT

D3 makes it easier to create, share, and collaborate on reports, saving analysts time so they can stay focused on protecting your organization. With D3, you can:


Save custom report templates to be reused, cloned, modified, or shared.

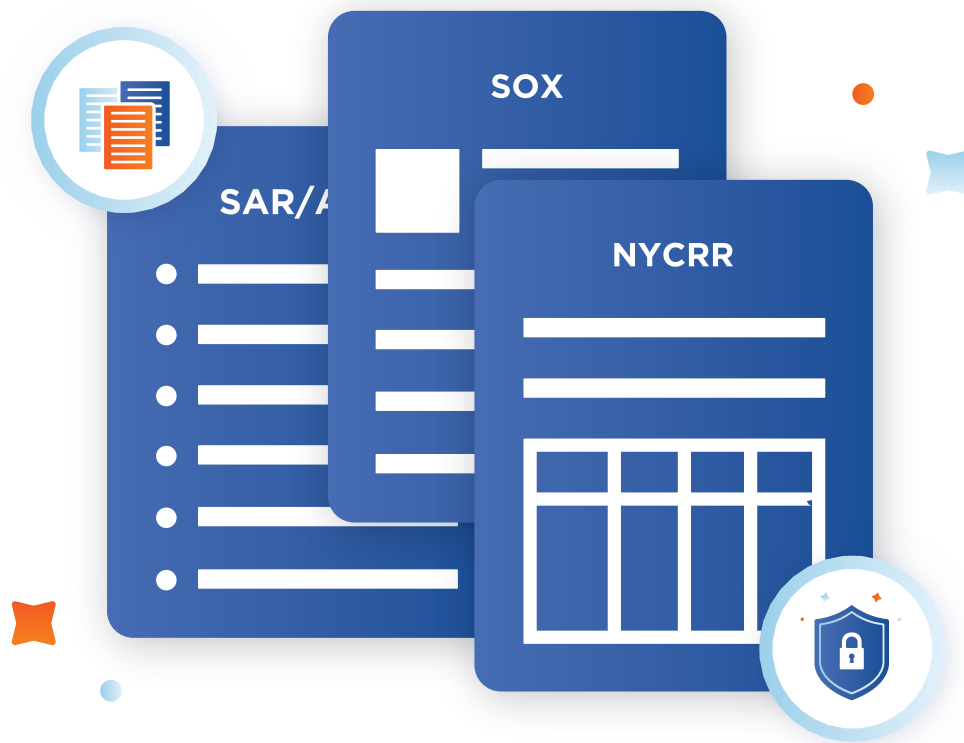
Share reports, even with "non-D3 users", without any data leaving the system.

Pin important reports to your dashboard

Automate report building based on date, record volume, incident types, or special parameters.

Schedule automated report-sharing.

Incident Report No.	20190829-172 
Incident Type	Suspicious Email (McAfee)
Status	Open IR
Reporting Date	August 29, 2019 11:40 AM



7.5 COMPLIANCE REPORTING

No one enjoys being audited or putting together compliance reports, and they're often made even worse by the fact that the information you need is distributed across many silos, each with its own data points and file formats. D3 gives you a centralized source and common taxonomy for all data, with a complete record of all entities (people, places, and things) and incidents of all types stored side-by-side. D3 also makes common compliance reports easier to assemble with built-in templates.

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

