D3 SECURITY ☎ 1-800-608-0081 www.d3security.com ✉ sales@d3security.com

D3 SOAR

ENTERPRISE INCIDENT & CASE MANAGEMENT SOLUTION FOR SECURITY ORCHESTRATION, AUTOMATION, & RESPONSE

CENTRALIZE AND STREAMLINE YOUR ENTERPRISE SYSTEMS – FOR SECURITY AND BEYOND

The growing volume and sophistication of cyber attacks, the emergence of new attack types, and a seemingly endless marketplace of security tools have resulted in an increasingly complex world of cybersecurity. Businesses need a more effective way to manage that complexity, reduce risk, and protect business assets.

Multiple vendors have emerged to address the challenges of resource shortages, the cybersecurity skills gap, analyst fatigue, and ever more sophisticated attackers.

Despite these benefits, Gartner has identified three issues with the offerings of many of today's SOAR vendors:

- No good way to sort through the "noise" created by the influx of data
- Speed is important, but automation is not the answer to everything
- Too narrow a focus on the Containment and Remediation phases of response, with little support for post-incident analysis

The D3 SOAR platform, unlike most SOAR offerings, is a powerful data management engine at its core. Strategically designed to ingest, manipulate, and process data in a highly flexible fashion, D3 eliminates these common SOAR challenges and gives CSIRTs ultimate control.

D3 SOAR filters out the "noise," allows highly flexible automation options, and encourages your CSIRT to treat incident response throughout the full lifecycle as standard operating procedure.

Data works better together, not in isolation.
D3's SOAR platform empowers you to centralize and streamline your suite of enterprise systems for better visibility into total business operations, closer multi-team collaboration, and better-informed decisions based on actionable insights gathered from nearly any system in your environment.

Powered by D3's proprietary Data Hub, Dynamic Data Structure, and Decision Tree, D3 is characterized by highly configurable Entities and Playbooks, and enhanced by an industry-leading Case Management Module.

Invest in a uniquely people-centric solution.
Your security protocols only work if they are followed consistently by everyone in your organization. In a People-Process-Technology framework, D3 SOAR gives you a powerful *technology* platform that helps your *people* implement your *processes*.

ORCHESTRATION

Orchestrate your suite of enterprise systems and applications to operate as a cohesive unit.

INTEGRATIONS

Integrate your security stack—NIDS, EDRs, SIEMs, etc.—with your Business Intelligence, ITSM, Data Management, HR Systems, and more.

D3 integrates via both RESTful API integrations and Python applets, giving you access to thousands of Playbook options throughout your environment, all from within the D3 SOAR platform.

Ingest data from multiple data sources to give your team the most flexibility in analyzing and acting on third-party events to enhance your cybersecurity team and threat response strategy. For example, you can:

- Reduce Time to Detect or prevent attacks by leveraging bi-directional integrations with your NIDs and EDRs.
- Gain a more accurate, global view of your security posture by centralizing information and prioritizing actions.
- Conveniently tap into your SIEM's event history and perform event searches without leaving the D3 system.
- Capture and feed raw data from events directly into Incident Reports.
- Create and update corresponding records in D3 from a displayed SIEM event.
- Enrich D3 with data from external intelligence sources to maintain an updated database of the latest threats and characteristics.
- Report on data from third-party systems with D3's Reporting Dashboards.

D3 PROPRIETARY DATA HUB & DYNAMIC DATA STRUCTURE

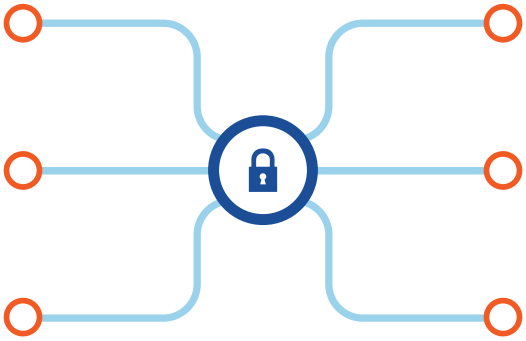
The core of D3's SOAR and Case Management platform, D3's proprietary Data Hub and Dynamic Data Structure guarantee that D3 will be able to grow with your business needs.

Data is collected, automatically normalized, and re-indexed in a data table where you can configure how to re-purpose the data to enrich external systems and provide the enterprise with a fuller view. Data-movement activities can be performed in batches. For example, you may run multiple activities in sequence or in parallel to extract data from multiple data sources in a single call, then automatically categorize the raw data into separate items as appropriate.

GRANULAR ACCESS CONTROL

Break down silos to enable closer collaboration between individuals and teams with granular permission levels.

- Use a combination of Role-Based Access Controls and Predefined Access Controls.
- Restrict permissions by any combination of individual Users, Groups of Users, Job Functions, Titles, and Geography.



AUTOMATION

Shorten response time. Streamline repetitive, manual tasks. Ensure compliance and traceability. By automating low-level tasks, you can shorten response time and allow your analysts to focus on more strategic and meaningful tasks, such as investigating advanced threats and making complex decisions that require their expertise.

AUTOMATE ACTIONS & DATA ENRICHMENT

Automatically query any number of third-party systems to collect event details and populate an Incident Report, or trigger D3's Playbooks to automatically create an Incident Report with auto-populated fields based on SIEM alerts.

Execute SQL or Python scripts to trigger downstream actions based on activity conditions, or enrich data values from third-party systems to provide analysts with additional context in an easy-to-understand format, eliminating wasted time on repetitive manual labor, such as copying and pasting from multiple windows.

PLAYBOOK CONFIGURATION

Powerful configuration options give you the flexibility of custom development, without the time required to write your own code.

- Extensive Python Library and hundreds of third-party integrations out-of-the-box to automatically execute actions such as blocking IP addresses or re-routing server traffic.

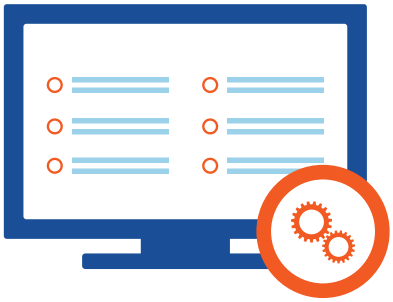
- Highly flexible configuration via a Visual Playbook Editor, with drag-and-drop automation and command line scripting (SQL & Python), to easily create new Playbooks from scratch or modify out-of-the-box Playbooks for your business requirements.

EXAMPLES OF COMMON AUTOMATION ACTIONS

- Trigger EPPs to contain malware
- Escalate alert tickets
- Adjust User Permissions in D3 or in your third-party directory service
- Record Incident details
- Collect data from workflows for analysis and trend identification
- Create, assign, and close Tasks.
- Check reputation scores from Threat Intelligence Platforms.

EXAMPLES OF FLEXIBLE CONFIGURATION OPTIONS

- Incorporate advanced criteria weighting to calculate risk severity as a threshold for downstream actions.
- Use Loop and Wait Activities with conditional logic to take actions such as modifying data in IR forms.



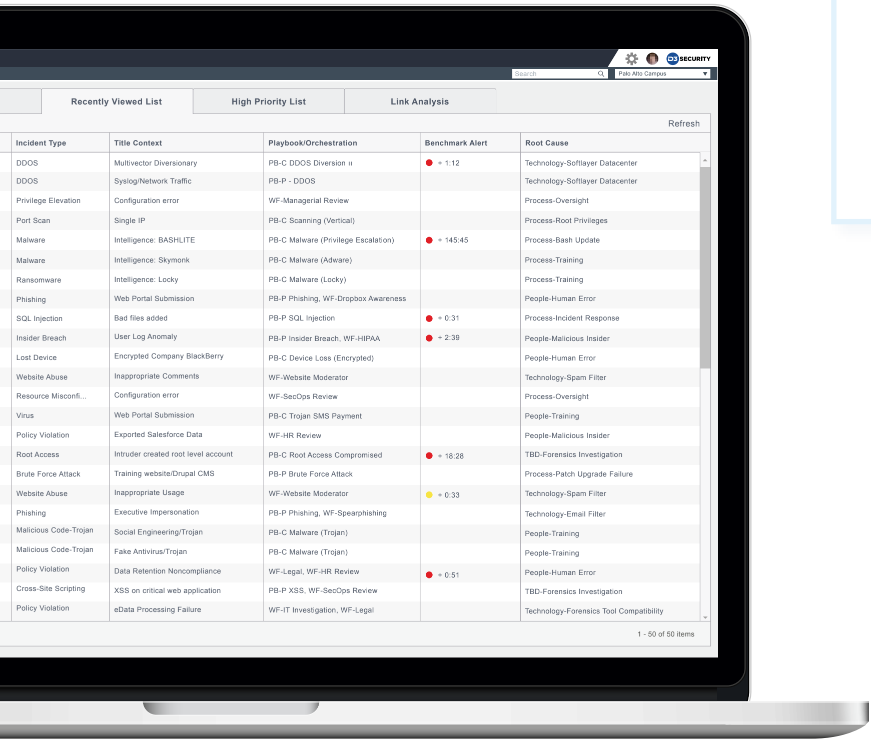
INCIDENT RESPONSE

Mitigate attack effects by giving your CSIRT the right information at the right time to make the best decisions at every step.

INTELLIGENT INCIDENT REPORTS

The quality of the data collected directly affects the quality of the information you get. Collect quality data from the start with intelligent Incident Reports built on conditional logic to reduce undue cognitive load on your analysts and responders.

- Data enrichment for identified IPs, URLs, and malware to add context to raw data.
- Use form field values to trigger Playbook operations, such as sending e-mails or terminating third-party processes.
- Create IR types for reporting or for fully automated workflows.
- Easily modify IR forms at any time with the D3 Admin Tool.



Incident Type	Title Context	Playbook/Orchestration	Benchmark Alert	Root Cause
DDOS	Multivector Diversionary	PB-C DDOS Diversion II	● + 1:12	Technology-Softlayer Datacenter
DDOS	Syslog/Network Traffic	PB-P - DDOS		Technology-Softlayer Datacenter
Privilege Elevation	Configuration error	WF-Managerial Review		Process-Oversight
Port Scan	Single IP	PB-C Scanning (Vertical)		Process-Root Privileges
Malware	Intelligence: BASHLITE	PB-C Malware (Privilege Escalation)	● + 145:45	Process-Bash Update
Malware	Intelligence: Skymonk	PB-C Malware (Adware)		Process-Training
Ransomware	Intelligence: Locky	PB-C Malware (Locky)		Process-Training
Phishing	Web Portal Submission	PB-P Phishing, WF-Dropbox Awareness		People-Human Error
SQL Injection	Bad files added	PB-P SQL Injection	● + 0:31	Process-Incident Response
Insider Breach	User Log Anomaly	PB-P Insider Breach, WF-HIPAA	● + 2:39	People-Malicious Insider
Lost Device	Encrypted Company BlackBerry	PB-C Device Loss (Encrypted)		People-Human Error
Website Abuse	Inappropriate Comments	WF-Website Moderator		Technology-Spam Filter
Resource Misconfi...	Configuration error	WF-SecOps Review		Process-Oversight
Virus	Web Portal Submission	PB-C Trojan SMS Payment		People-Training
Policy Violation	Exported Salesforce Data	WF-HR Review		People-Malicious Insider
Root Access	Intruder created root level account	PB-C Root Access Compromised	● + 18:28	TBD-Forensics Investigation
Brute Force Attack	Training website/Drupal CMS	PB-P Brute Force Attack		Process-Patch Upgrade Failure
Website Abuse	Inappropriate Usage	WF-Website Moderator	● + 0:33	Technology-Spam Filter
Phishing	Executive Impersonation	PB-P Phishing, WF-Spearphishing		Technology-Email Filter
Malicious Code-Trojan	Social Engineering/Trojan	PB-C Malware (Trojan)		People-Training
Malicious Code-Trojan	Fake Antivirus/Trojan	PB-C Malware (Trojan)		People-Training
Policy Violation	Data Retention Noncompliance	WF-Legal, WF-HR Review	● + 0:51	People-Human Error
Cross-Site Scripting	XSS on critical web application	PB-P XSS, WF-SecOps Review		TBD-Forensics Investigation
Policy Violation	eData Processing Failure	WF-IT Investigation, WF-Legal		Technology-Forensics Tool Compatibility

1 - 50 of 50 items

GUIDED INCIDENT RESPONSE WORKFLOWS

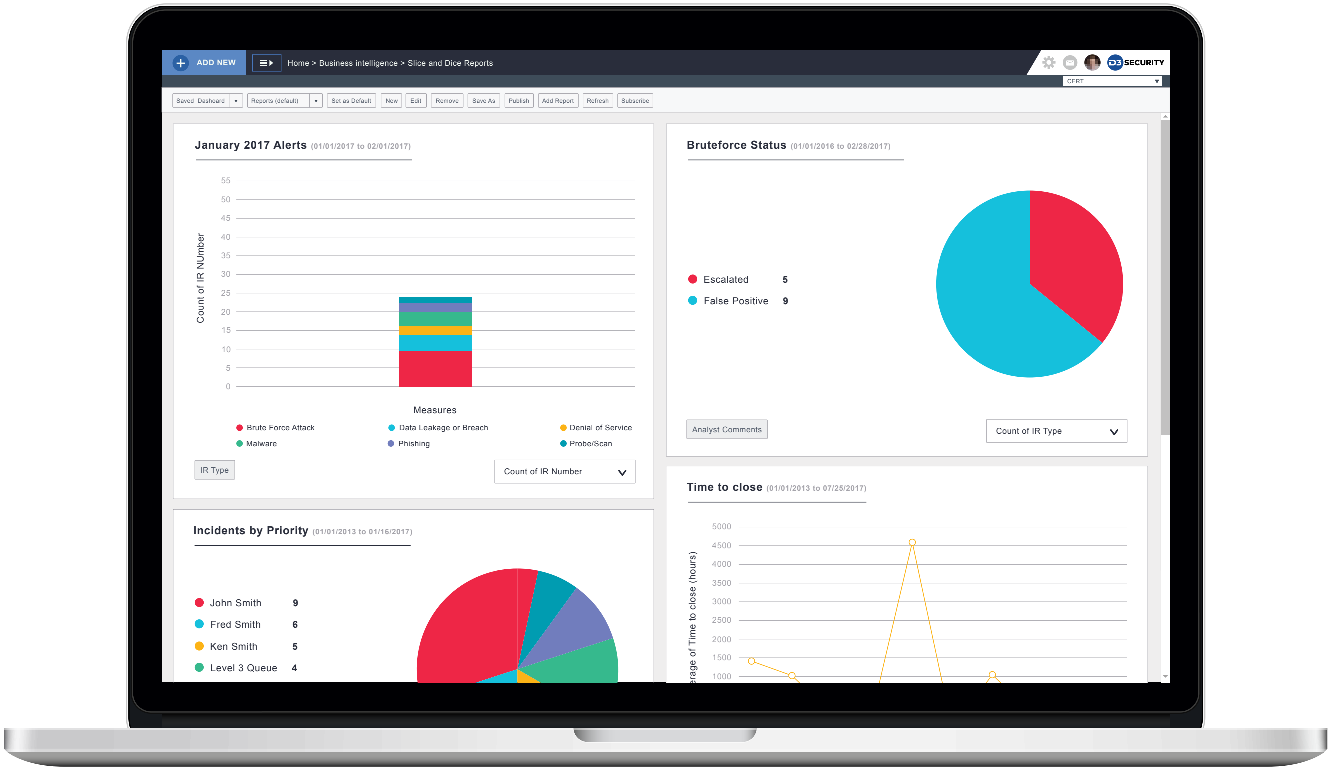
Ensure consistent response, training, and on-boarding with step-by-step guidance to ensure nothing is missed in the procedures designed by your experienced cybersecurity professionals.

- Out-of-the-box Playbooks guide your analysts through industry-standard NIST frameworks from day one.
- Modify existing Playbooks or create your own to ensure all analysts consistently follow company protocol.

EXAMPLES OF COMMON IR PLAYBOOKS

- Malware
- Hacking
- Denial of Service
- Data Leakage or Breach
- Social Engineering Attack

POST-INCIDENT ANALYSIS & REPORTING



Senior leadership and management can oversee security operations with summary reports and actionable metrics.

With D3's proprietary Dynamic Database Structure, you can configure D3 SOAR to collect and report on any field appropriate for your business. Conduct Root Cause Analysis to apply lessons learned and feed information back into the D3 Data Hub to power integrated systems, create new workflows, and improve your defenses.

INSTANT & LIST REPORTS

Gain clear visibility of SOC team performance. Build and visualize Case data by selecting multiple Case-related data tables used in D3 to track KPIs to identify areas of improvement and take corrective actions identified by Reporting, Link Analysis, and the Case Management Module.

SLICE & DICE REPORTING

"Slice & dice" multiple sources of data in a single instance with detailed charting options to visualize your CSIRT performance with richer and broader perspective.

- Compare multiple reports and segment your data until you get the right level of detail.
- Generate Reports, Dashboards, and Pivot Tables, either manually or automatically.
- Save, Schedule, and Export or Email Reports to internal or external users in multiple formats.

CASE MANAGEMENT MODULE

Few SOAR systems are designed with evidentiary value in mind. Add D3 Security's industry leading Case Management Module to SOAR for enhanced Case investigation and collaboration.

Corporate forensic investigations can be challenging because there are often unknown, duplicate, or siloed data that impede multi-team collaboration and hinder security teams from effectively responding to and preventing recurring incidents.

D3 Security's Case Management Module enables closer cross-functional collaboration. Link Cases with Incidents from D3 SOAR to expedite incident resolution and investigations, build legal defenses, and demonstrate compliance.

LINK ANALYSIS

How do you identify repeat offenders? Are they targeting specific assets? Are they repeatedly exploiting the same vulnerability? Is there enough evidence to warrant a Case? Has a Case already been created for related Incidents?

Answer these questions and more by visualizing relationships via associations and dependencies to identify subtle clues and early indicators.

- Cut out noise with flexible Filter and Scope options, such as defining combinations of Date Ranges, Fields, Link Types, and highlighting important information.
- Start from a Root Node and add or delete nodes and Custom Links as you investigate.
- Build, visualize, and manipulate multi-tier relationships between Cases, Incident Reports, Entities, Persons, Tasks, and Items, depending on your configuration.

IT FORENSICS

Build your Investigation Team with subject matter experts from multiple job functions (e.g. Forensics, Human Resources, etc.), and substantiate your findings in any investigation.

- Track seized data, custodians, threat actors, physical artifacts, and logical artifacts in any format.
- Search and access all evidence records within the Evidence Library.
- Document interviews, interviewers, interviewees, and narratives.
- Enable secure and seamless collaboration with granular Access Control Levels.
- Record seizure, custody, control, transfer analysis, and disposition of evidence with chain of custody for each evidence record to maintain compliance.
- Create, track, and secure Case Review requests to allow Case Review while preventing unauthorized editing.

ABOUT D3 SECURITY

D3 Security is a full-spectrum Enterprise Incident Response & Management platform that unifies teams across borders and job functions—IT, Corporate Security (Physical & Cyber), Legal, HR. Your teams can easily manage all incident types, collaborate on cases and investigations, conduct post-incident analyses, derive actionable analytics, and automatically report on progress to continually improve your security program.