D3 SECURITY

SOAR

BENEFITS AND FAQS

WHITEPAPER

CONTENTS

WHAT IS SOAR?

SECURITY ORCHESTRATION

AUTOMATION

RESPONSE

Security orchestration, automation, and response (SOAR) is an important technology for IT security, security operations center (SOC), and incident response (IR) teams who want to improve the speed, quality, and efficiency of their operations. SOAR helps companies collect security alerts and threat intelligence, streamline analysis and triage, and orchestrate actions across disparate tools and personnel. Together, these capabilities increase the speed of decision-making and remediation, significantly reducing risk to the organization.

GARTNER DEFINES SOAR AS A COMBINATION OF THREE DISTINCT TECHNOLOGIES

Security Incident Response

Includes incident documentation, task assignment, and investigation/case management.

Orchestration and Automation

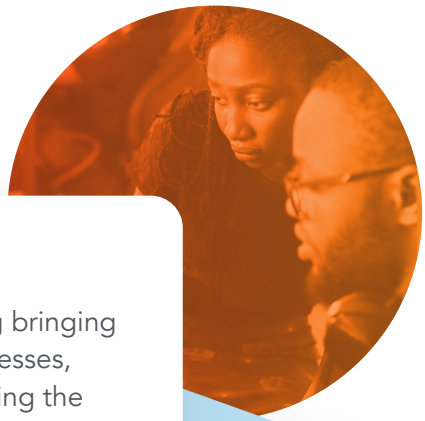
Provides tool-to-tool workflow automation, primarily for triage and simple remedial actions, but lacks case management, reporting and other executive-level features.

Threat Intelligence

Brings together multiple sources of external threat intelligence in a single place, with some correlation capabilities. Requires additional solutions to act on the intelligence.

WHO SHOULD BE INTERESTED?

Anyone involved in IT security should want SOAR because of its wide-ranging benefits. People with the following roles and responsibilities will be particularly interested:



CISOs and IT Security Executives

SOAR aligns closely with key CISO responsibilities, including bringing maturity to security strategy and incident management processes, protecting the company from security breaches, and improving the efficiency of security personnel.

SOC Leaders and Analysts

A constant barrage of security events and a shortage of skilled employees mean day-to-day efficiency and execution are pressing needs in every SOC. SOAR helps by transforming security events into actionable information and ensuring every alert is contextualized and managed according to the right playbook. SOC leaders and senior analysts are often tasked by their CISO to evaluate SOAR solutions.

Privacy and Compliance Teams

Increasingly, organizations must maintain compliance with IT, security, privacy and financial regulations. A robust SOAR platform can track evidence, generate compliance reports, and extend workflows to privacy, forensics, and HR teams to enable collaboration on important cases.

WHICH ORGANIZATIONS PURCHASE SOAR?

Large-to-mega sized enterprises are all purchasing SOAR products. Any organization with a global presence, and internal SOC and IR teams, is a great candidate for SOAR. Even companies that rely on MSSPs are good candidates because SOAR can help prioritize and streamline work between internal and external security services.

Mid-sized enterprises often lack security skills and budgets, making SOAR a necessary solution to enhance internal capabilities and scale existing security expertise across the organization through playbooks and automation. SOAR also increases the impact and value of other SOC tools through integrations.

MSSPs are increasingly adopting SOAR to serve as a workbench for their SOC analysts, and as an integration hub that can plug into a multitude of tools used by clients. SOAR tools can also enable high-value services and reports that MSSP can sell to clients, such as custom playbooks or, in the case of D3, event mapping based on TTP frameworks like MITRE ATT&CK.

All industries are targeted by adversaries and malicious insiders, and therefore can all benefit from SOAR. Finance, healthcare, energy, government, technology and professional services are among the leaders in adoption of SOAR solutions.

Companies with technology gaps, such as those with SIEM, endpoint security, EDR, firewall and other prevention and detection technologies, but who are still managing incidents through email, spreadsheets, ticketing, and other generalized tools, are great candidates for SOAR.

WHAT ARE THE BENEFITS OF D3 SOAR?

D3 offers the first and only next-generation SOAR solution, combining security orchestration and automation with the predictive capabilities of the MITRE ATT&CK framework. Bringing together all three pillars of the Gartner SOAR model, D3 offers the most comprehensive SOAR solution on the market.

Integrations

D3 offers 260+ integrations and thousands of automated actions. Unlike many SOAR vendors, D3 provides an open and fully independent ecosystem of integrations, a benefit recognized by Gartner in their *2019 Market Guide for Security Orchestration, Automation and Response Solutions.*

McAfee Together is power.

LogRhythm The Security Intelligence Company

Chronicle

elastic

MICRO FOCUS

IBM

CROWDSTRIKE

Symantec

Carbon Black.

Check Point SOFTWARE TECHNOLOGIES LTD

FireEye

splunk>

Orchestration

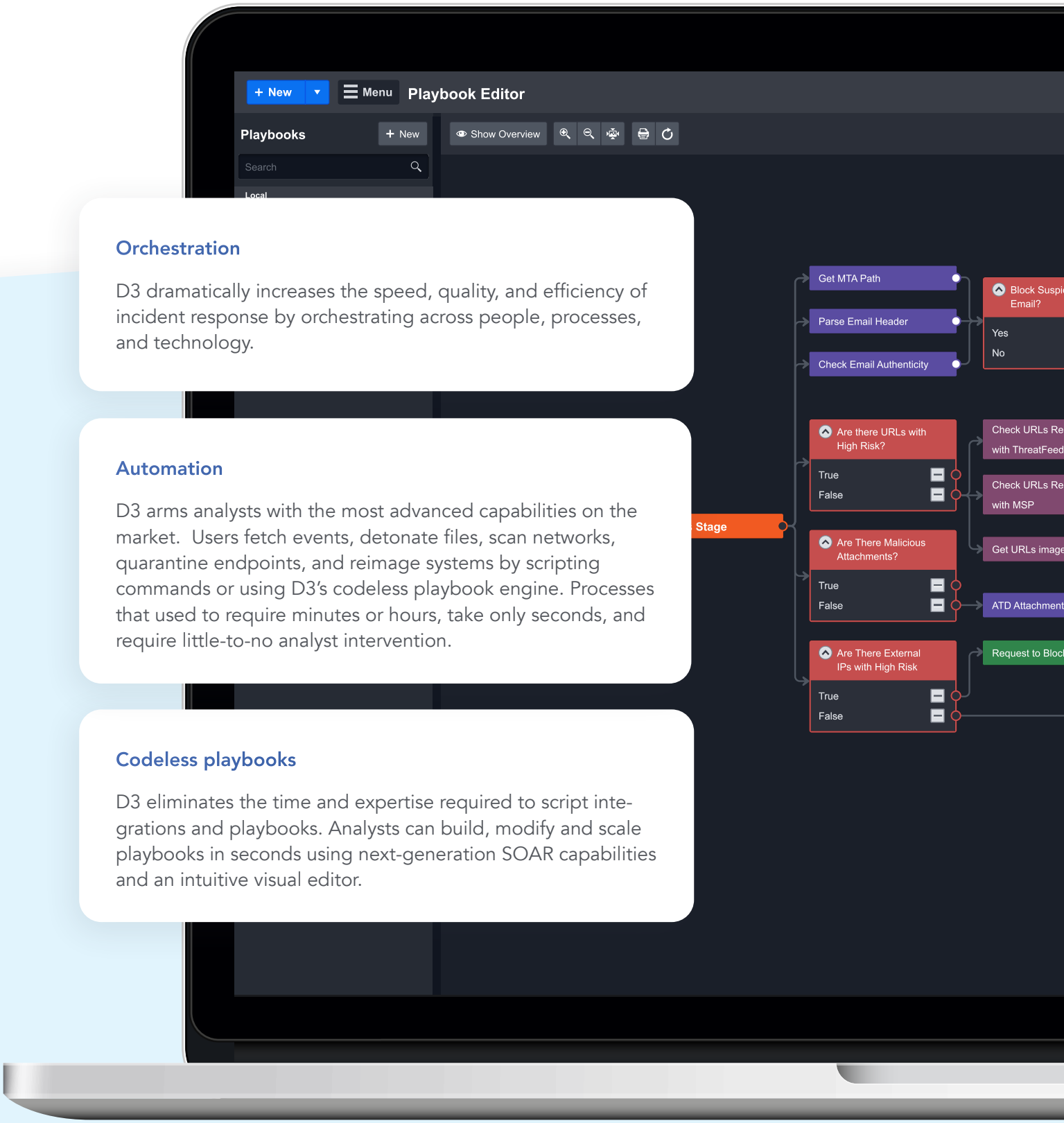
D3 dramatically increases the speed, quality, and efficiency of incident response by orchestrating across people, processes, and technology.

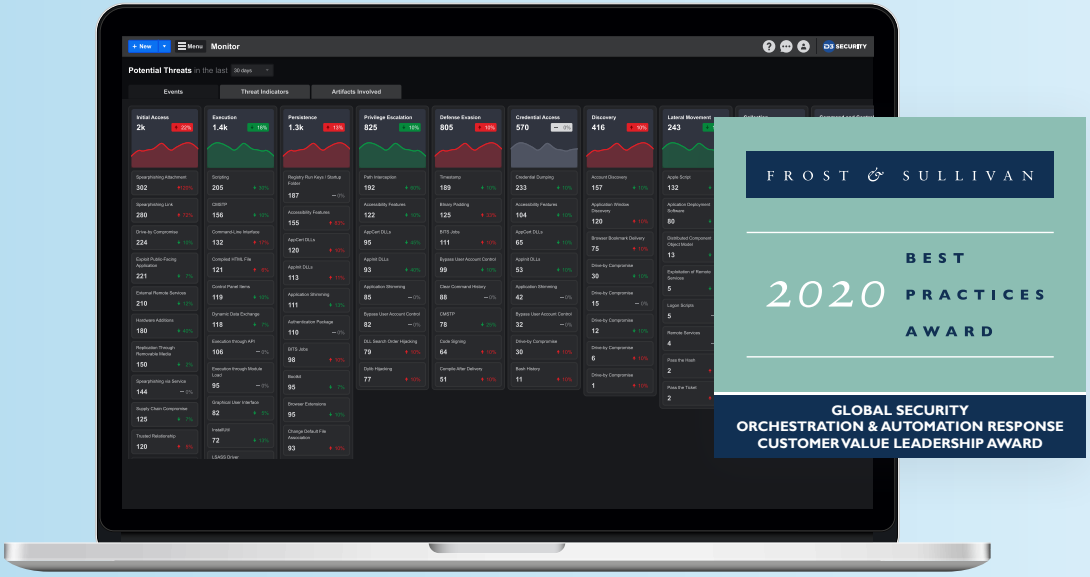
Automation

D3 arms analysts with the most advanced capabilities on the market. Users fetch events, detonate files, scan networks, quarantine endpoints, and reimage systems by scripting commands or using D3's codeless playbook engine. Processes that used to require minutes or hours, take only seconds, and require little-to-no analyst intervention.

Codeless playbooks

D3 eliminates the time and expertise required to script integrations and playbooks. Analysts can build, modify and scale playbooks in seconds using next-generation SOAR capabilities and an intuitive visual editor.





Independent consulting firm Frost & Sullivan named D3 the top SOAR solution for customer value in 2019 and 2020.

MITRE ATT&CK

D3 surfaces ultra-rich context by correlating and mapping events against the MITRE ATT&CK matrix, focusing SOC analysts on suspicious behavior and critical threats. Dashboards and playbooks based on ATT&CK enhance the SOC's visibility into adversary actions.

Case Management

D3's robust case management system centralizes the management of tasks, reporting, chains-of-custody, and digital and physical evidence. Investigation workflows extend from the SOC to privacy, compliance, corporate security, HR and other departments, ensuring all case-related data is entered and tracked in D3.

Dynamic Link Analysis

Built-in link analysis allows D3 users to reveal connections and establish relationships faster, offering unrivalled analysis functionality. Users can combine events, incidents, IOCs, adversaries, and timelines in a drag-and-drop visual dashboard.

Digital Forensics

D3 provides specialized workflows and case management features for digital forensics teams and eDiscovery. The system triages case requests and assignments, making it easy to manage custodian lists, data processing and collaboration.

SOC Reporting

D3 provides an incredible array of SOC reports, including top source/destination IPs, ports, domains, blocked domains, services, incident types, percentage of recurring incidents, percentage of incidents with compliance issue, MTTD, MTTR, and many others. Custom reports can also be generated.

Compliance

D3 automatically documents every incident, escalation, playbook, piece of evidence, and decision, ensuring comprehensive audit and compliance reporting. Turnkey reports are available for FinCEN, HIPAA, NERC CIP, and other state-level or international standards.

SOAR SUCCESS STORIES

A major US health system implemented D3 SOAR for its SOC and IR team. Triage and remdiation time was significantly reduced through integration with Splunk, ServiceNow, VirusTotal and DomainTools. Playbooks for key use cases like phishing included cross-departmental workflows for privacy and forensics collaboration.

The client's average remediation time went from 48 hr. to 28 min., a 99% reduction directly attributed to D3 SOAR.

An international MSSP implemented D3 SOAR for its SOC and CSIRT team. Integration with 10+ solutions, including RSA, Palo Alto, Checkpoint, Sophos and Darktrace, enabled a high level of automation across 40 playbooks. Enhanced data-retention capabilities ensured new regulations were met.

In just the first year, the MSSP enabled a high-value service using D3's MITRE ATT&CK features, generating significant net-new revenue.

ABOUT D3 SECURITY

D3 Security's Next-Generation 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