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

HOW D3 MEASURES UP TO GARTNER'S SOAR REQUIREMENTS

Gartner recently published the 2020 Market Guide for Security Orchestration, Automation and Response Solutions in which D3 was named a representative vendor. In the report, Gartner describes D3 SOAR as having "powerful" incident response, case management, and threat intelligence features, and more than 300 connectors to date for orchestration and automation.

In this document, find out how D3 maps successfully to all of Gartner's SOAR recommendations, offering a comprehensive end-to-end solution for SOCs and security leaders around the world.

MAPPING D3 WITH GARTNER'S RECOMMENDATIONS

Gartner defines SOAR as the convergence of Security Incident Response Platforms, Security Orchestration and Automation, and Threat Intelligence Platforms. Later in the report, Gartner also defines SOAR as being made up of four major engines:

WORKFLOW AND COLLABORATION

TICKET AND CASE MANAGEMENT

ORCHESTRATION AND AUTOMATION

TI MANAGEMENT

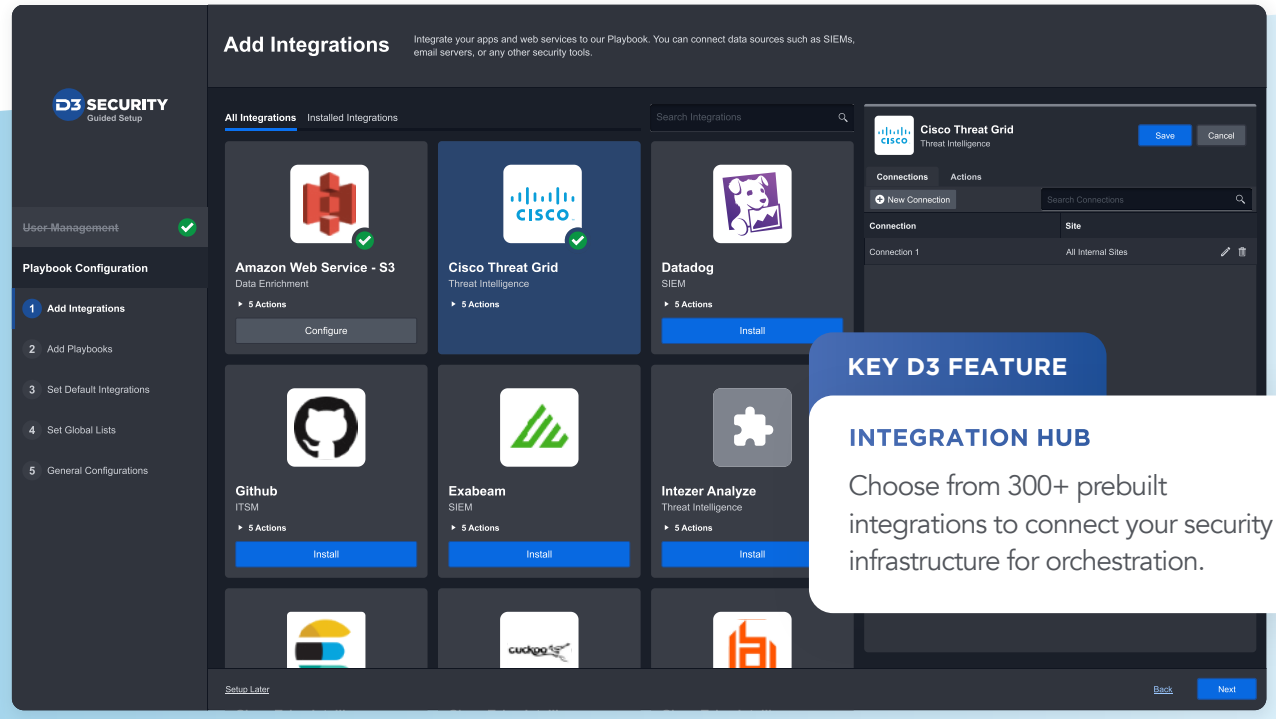
HIGH-LEVEL TECHNICAL ATTRIBUTES

Gartner recommends that organizations looking to evaluate SOAR on technical merits should start with capabilities at a high level, including:

	D3 SECURITY
Alert triage and prioritization	D3 automates rich alert enrichment and prioritization via integrated threat intelligence sources, historical data, and MITRE ATT&CK correlations.
Orchestration and automation	D3's codeless playbooks orchestrate and automate across more than 300 tools.
Case management and collaboration	D3 has some of the deepest case management features of any SOAR platform, with workflows that enable complex, multi-team investigations.
TI and investigation	D3's threat intelligence integrations put detailed data at analysts' fingertips, with integrated sandboxes to confirm suspected malicious files.
Dashboard and reporting	D3 can generate scheduled or ad hoc reports from virtually any data in the system. Customizable dashboards include the MITRE ATT&CK-based Monitor dashboard, which reveals the occurrence of each attacker technique in the environment.

RECOMMENDATIONS FOR SOAR BUYERS

INTEGRATIONS AND CONNECTIVITY



KEY D3 FEATURE

INTEGRATION HUB

Choose from 300+ prebuilt integrations to connect your security infrastructure for orchestration.

Gartner

Buyers should favor SOAR solutions that are compatible with the arsenal of products installed in the organization environment.

HOW D3 NEXTGEN SOAR MEASURES UP

D3 integrates with 300+ tools, including SIEM, TIP, firewall, endpoint protection, email protection, ticketing, and cloud security products. These integrations enable D3 clients to not just benefit from D3's capabilities, but also to enhance the impact of their existing tools.

Gartner

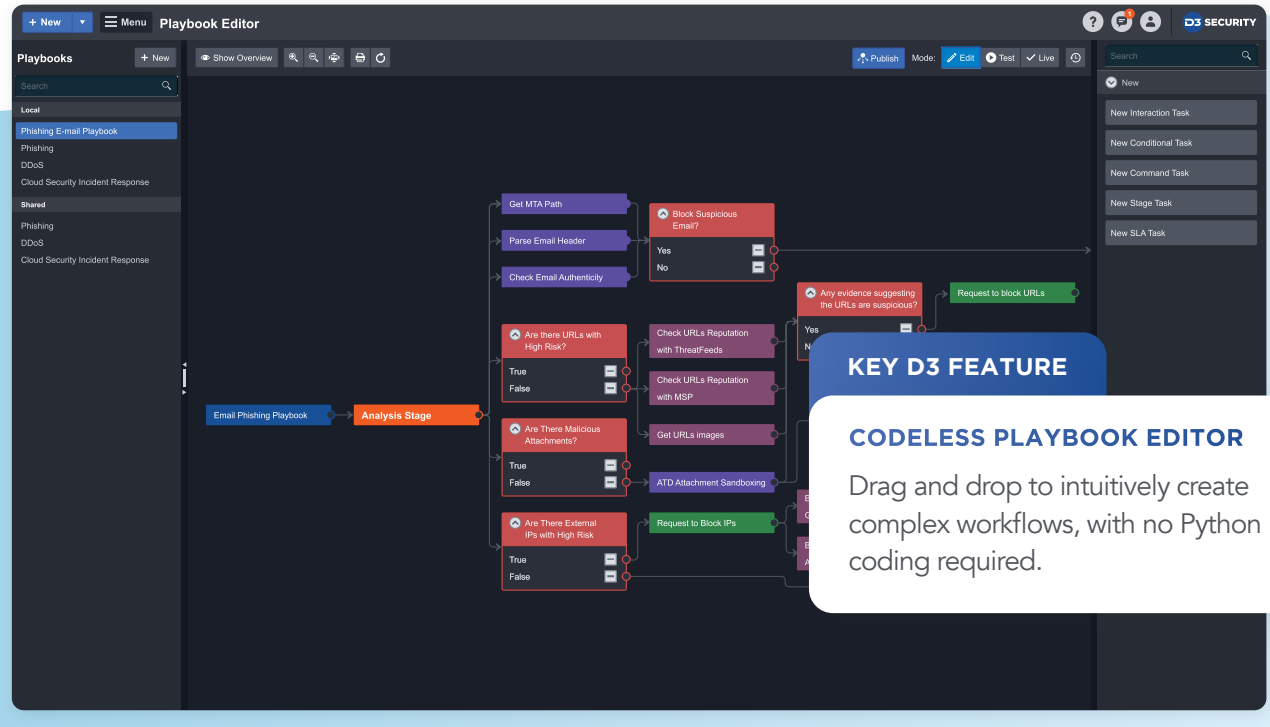
Buyers should favor SOAR solutions that deliver the use cases needed to complement your set of security products to manage the SOC and security operations functions.

HOW D3 NEXTGEN SOAR MEASURES UP

D3's versatility allows it to complement the way almost any SOC functions. D3 can act as the central security operations hub for the SOC, but many clients also use it in more specialized ways to take advantage of its case management features, MITRE ATT&CK correlation, or playbook orchestration, just to name a few examples.

RECOMMENDATIONS FOR SOAR BUYERS

WORKFLOWS



KEY D3 FEATURE

CODELESS PLAYBOOK EDITOR

Drag and drop to intuitively create complex workflows, with no Python coding required.

Gartner

Buyers should favor SOAR solutions that offer the capability to easily code an organization's existing playbooks (using a low- or no-code model) that the tool can then automate, via an intuitive UI.

HOW D3 NEXTGEN SOAR MEASURES UP

D3 offers a codeless playbook editor that enables drag-and-drop creation and editing of playbooks. Automated steps can be added in seamlessly, including complex sequences of actions that can be nested within other playbooks.

Gartner

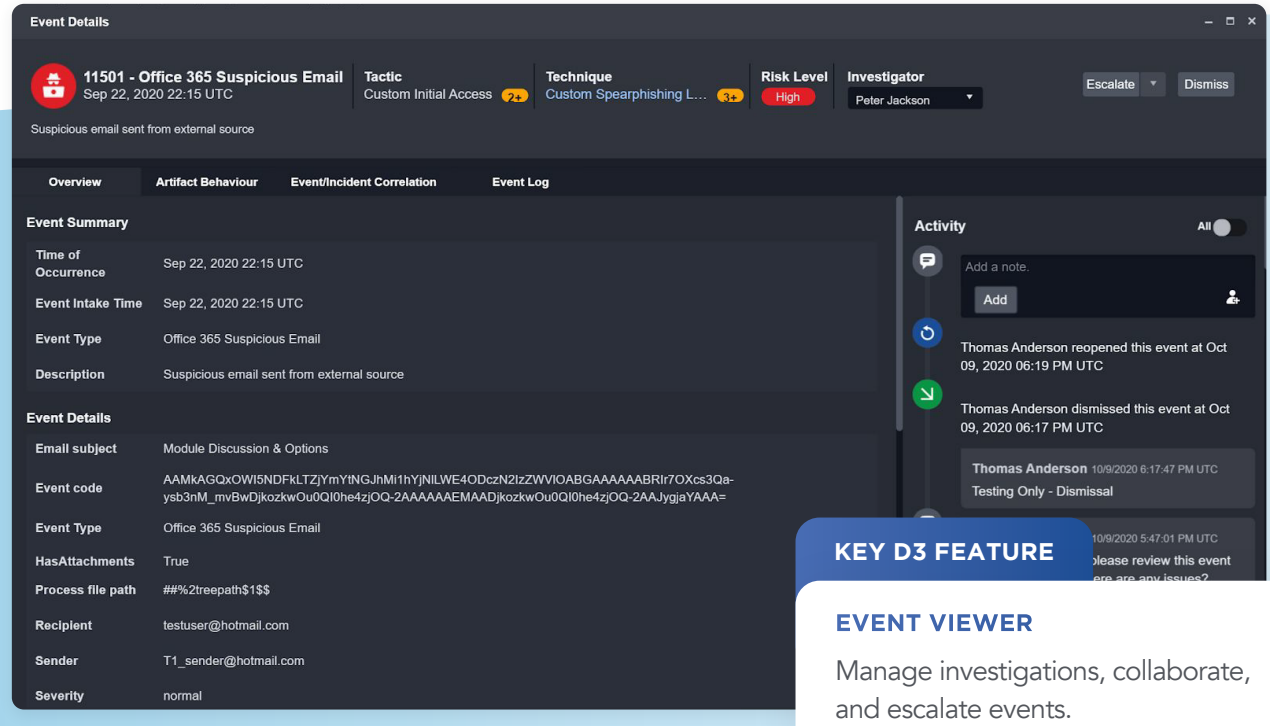
Buying a SOAR solution must be driven by your existing processes.

HOW D3 NEXTGEN SOAR MEASURES UP

Here, Gartner's authors are repeating a familiar refrain that adding a SOAR solution to immature processes won't magically make those processes better. This is why in PoCs and new implementations, D3 always recommends starting with a few well-developed use-cases, such as phishing response, and then expanding the scope from there.

RECOMMENDATIONS FOR SOAR BUYERS

INVESTIGATION AND CASE MANAGEMENT



KEY D3 FEATURE

EVENT VIEWER

Manage investigations, collaborate, and escalate events.

Gartner

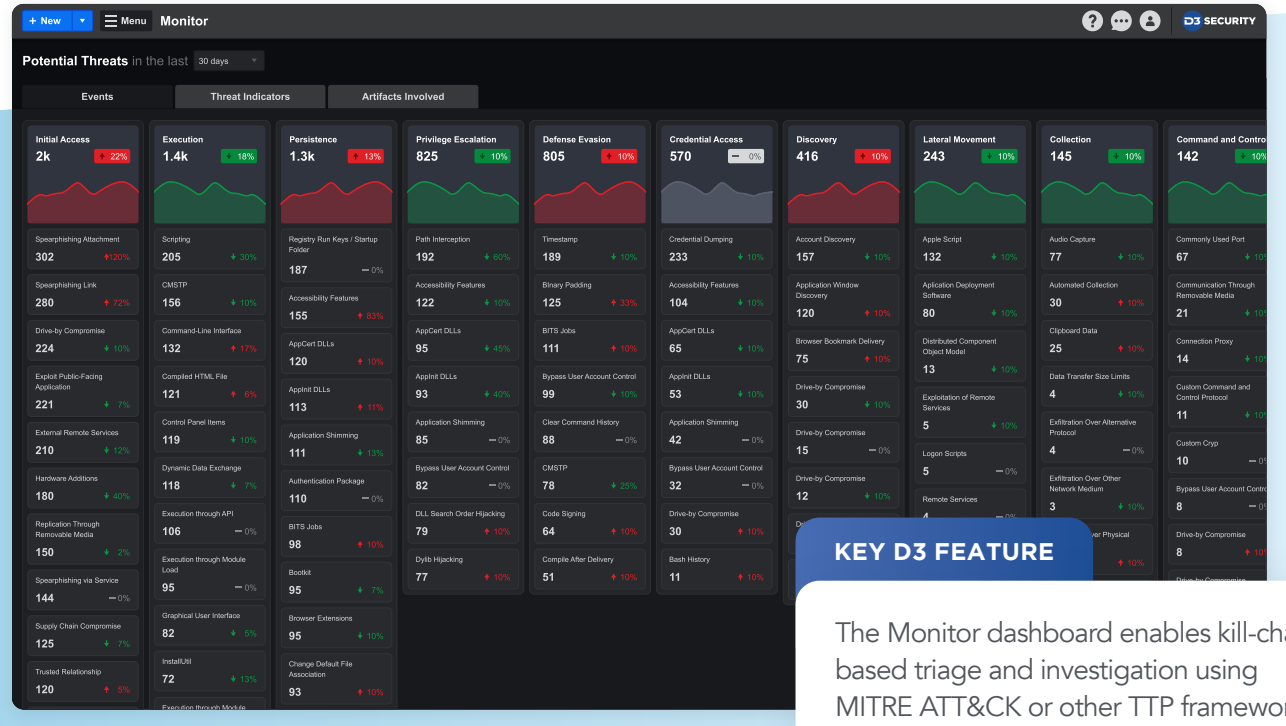
Buyers should favor SOAR solutions that optimize the collaboration of analysts, for example, with a chat or IM framework that makes analysts' communication more efficient, or with the ability to work together on complex cases.

HOW D3 NEXTGEN SOAR MEASURES UP

Multiple investigators can collaborate on D3 incidents, including via a chat feature where users can add and review notes in the timeline. There are also features to assign tasks and securely loop in others, even if they're outside the SOC. Related incidents can be easily grouped together into cases for deeper investigation.

RECOMMENDATIONS FOR SOAR BUYERS

THREAT MONITORING, INVESTIGATION AND RESPONSE



KEY D3 FEATURE

The Monitor dashboard enables kill-chain-based triage and investigation using MITRE ATT&CK or other TTP frameworks.

Gartner

Buyers evaluating SOAR should consider capabilities including TI and investigation—defined as evidence-based knowledge, including context, mechanisms, indicators, implications, and action-oriented advice about threats—as well as alert triage and prioritization, which has the goal of producing highly accurate incidents that deserve genuine attention from analysts.

HOW D3 NEXTGEN SOAR MEASURES UP

Uniquely among SOAR platforms, D3 correlates attacker techniques and generates a cyber kill-chain-based view of threats against your environment. This vastly improved contextualization and mapping allows analysts to quickly identify serious threats and better recognize the attacks and campaigns that comprise individual security events.

RECOMMENDATIONS FOR SOAR BUYERS

HOSTING AND PRICING

Gartner

Buyers should favor SOAR solutions that have a pricing model that is aligned with the needs of the organization and is predictable. Avoid pricing structures based on the volume of data managed by the tool or based on the number of playbooks run per month. These metrics carry an automatic penalty for more frequent use of the solution.

HOW D3 NEXTGEN SOAR MEASURES UP

D3 charges a simple and predictable per-user license fee. We never charged based on data volume or playbook usage, since these penalize clients when they need D3 most.

Gartner

Buyers should favor SOAR solutions that offer flexibility in the deployment and hosting of the solution.

HOW D3 NEXTGEN SOAR MEASURES UP

D3 offers cloud or on-premise hosting, and supports hybrid environments through integrations with cloud and on-premise security stacks.

THE NEXT GENERATION OF SOAR

The qualities that make D3 NextGen SOAR a perfect fit with Gartner's recommendations are the same qualities that make it the industry's #1 vendor-agnostic security orchestration, automation, and response (SOAR) platform. D3's 300+ integrations, low-code/no-code playbooks, and automated correlation of attacker techniques enable a fast and conclusive model of security operations that reduces clients' MTTR by as much as 96%.

To learn more about D3 NextGen SOAR, visit D3Security.com