A Comprehensive Guide to Smart SOAR

D3 Smart SOAR

An operating system for autonomous triage and cross-platform response.

With D3 Security's Smart SOAR, teams have a single pane of glass for managing automated incident response across their security stack. The technology transforms thousands of low-fidelity alerts into few high-fidelity, high-confidence incidents, giving responders more time to investigate real threats.

Each layer of the Smart SOAR platform serves to increase the fidelity and actionability of the security information. Alerts are ingested from across the security stack, de-duplicated, and normalized into a common data structure. Users can define workflows to classify and prioritize alerts on ingestion based on risk-based triage. False positives and validated threats can be handled through automation, while uncertain or complex incidents can be escalated for investigation.

Problem Statement

We are now several years into the era of security orchestration, automation, and response (SOAR), and it has become clear that most SOAR tools are not capable of helping security teams overcome the challenges they face. In polls of security professionals, there seems to be no improvement in morale or confidence that negative trends can be reversed, despite the influx of new technology.

At D3 Security two or three years ago, almost all of our new customers did not yet have SOAR in their organization. Now, the majority of new customers are organizations that are giving up on their previous SOAR tool to look for something better. This underscores the failure of what we call "Legacy SOAR" to meet users' needs.

Industry Trends

Alert Overwhelm

With so many tools generating alerts, the average SOC simply cannot investigate every alert. Alert fatigue means that security teams waste huge amounts of time confirming false positives, while genuine threats slip by undetected.

Cybersecurity Skills Gap

For many years, industry analysts have been warning of a worsening gap between the number of qualified cybersecurity professionals and the number of security jobs that companies need to fill. The skills gap has put security talent at a premium, making it imperative that security teams be extremely efficient with the resources they have, and that they do not lose employees due to burnout or dissatisfaction.

Too Many Tools

The number of tools in the average enterprise SOC has exploded, necessitating huge amounts of manual work to navigate myriad interfaces, hunt for important information across data silos, and coordinate the work done in different tools.

Vendor Acquisitions

In recent years, many SOAR vendors have been acquired by larger companies. These vendors' SOAR platforms are now being offered as part of a suite of tools, with in-house integrations prioritized, instead of as standalone, vendor-agnostic solutions. SOAR innovation in these companies is slowing to a crawl, as talent leaves in mass and corporate priorities divert attention away from SOAR.

Why Smart SOAR?

At D3 Security, we named our SOAR product Smart SOAR because there needs to be differentiation between the basic automation offered by some of the newer SOAR vendors, the suite-based SOAR tools sold by tech giants, and truly end-to-end SOAR platforms like ours. All these things are called SOAR, but the similarities are only superficial.

Throughout this document, we will describe in detail how Smart SOAR works, and how it stacks up against Legacy SOAR. As an overview, some of the capabilities that make Smart SOAR different are:

Unlimited, vendor-maintained integrations.

Enables Smart SOAR to connect to any number of products and data sources, from homegrown or bespoke solutions to industry leaders like Microsoft, SentinelOne and CrowdStrike. All via feature-rich integrations that are fully built and maintained by D3's dedicated integration team. New integrations can be built by request in approximately seven days.

The Event Pipeline.

Normalizes, deduplicates, enriches, and correlates your security alert data, bringing much needed structure to data and providing a foundation for analyzing behaviors and stitching together incidents based on their shared indicators and techniques. Crucially, the Event Pipeline can turn an unmanageable alert queue into a small number of high-fidelity incidents.

Intelligence beyond IOCs.

Smart SOAR incorporates identity (e.g. user IDs, devices, and accounts) and behavior (e.g. MITRE ATT&CK techniques) data to create a truer picture of threats.

Memory.

Legacy SOAR doesn't retain alert information, so it is blind to obvious patterns. Smart SOAR retains alerts and artifacts for 90 days to enable correlation across time.

Cross-stack correlation and orchestration.

No matter where an alert originated, Smart SOAR enables users to conduct against all relevant datasets, and orchestrate a cross-stack response.

Incident response and case management.

Playbooks and incident workspaces that support investigations of complex incidents.

These capabilities enable security teams to make lasting progress against major challenges, instead of just treading water.

Functional Components of Smart SOAR

The rest of this guide will be dedicated to the major components of Smart SOAR. These are not the technical components of the software, but rather the functional stages that alerts and incidents pass through, from ingestion to resolution. Even this level of attention will not fully encapsulate what can be achieved with Smart SOAR, so we recommend that any interested reader schedule a one-on-one demo at D3Security.com

1. Integration & Ingestion

To enable intelligent security across your entire environment, you need rich data flowing into your SOAR tool, and effective commands to other tools flowing out. If your incoming data is limited, you aren't seeing enough of the picture to make accurate decisions. If your orchestration is limited, you aren't able to quickly take action against threats.

Unfortunately, Legacy SOAR integrations are often limited in depth and quality, requiring additional manual threat analysis and incident response tasks. Legacy SOAR's integration design is flawed because:

They rely on community-built or customer-maintained integrations, which require work from users.
Their out-of-the-box connectors are limited, often because the vendor has a preferred product suite.
Their internal expertise on other tools is limited, which puts the responsibility on the customer to manage the integrations and fix issues.

Many Legacy SOAR vendors were independent vendors before being acquired. Following acquisition, the vendors' priorities become narrowed to those of their parent company, taking focus away from integration maintenance and development, especially for integrations with competitors' tools.

Smart SOAR needs to be vendor-agnostic, so that it can offer the broadest and deepest set of integrations, while enabling its users to keep their preferred, best of breed tools. As the leading independent SOAR provider, D3 Security is able to work closely with all of our technology partners to build and maintain feature-rich integrations with every leading tool. Even when integrating with SOC platforms with built-in SOAR, Smart SOAR outperforms those capabilities.

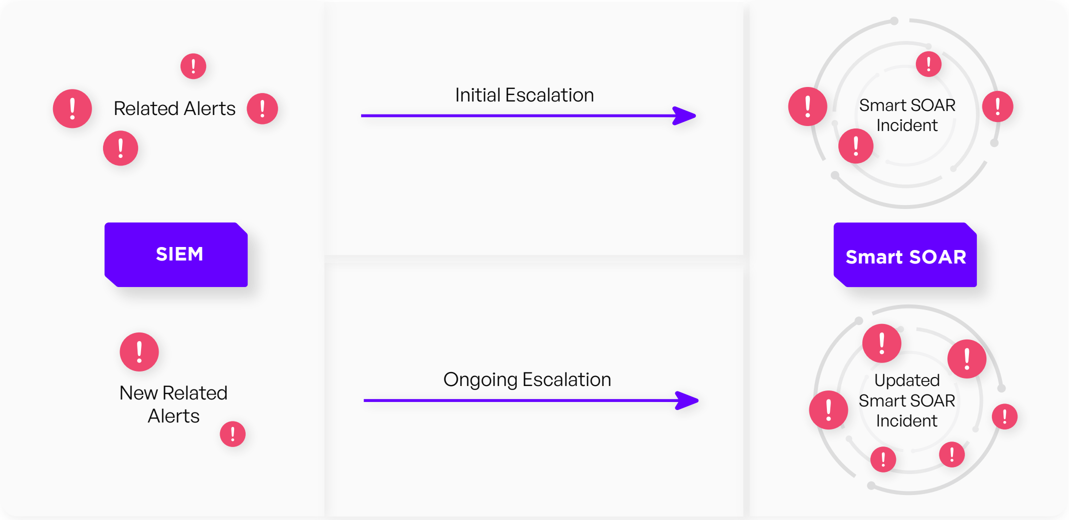
Smart SOAR

1. Add Notes to Threats
2. Add Threat to Blacklist
3. Block Hash
4. Connect Agent to Network
5. Create Group
6. Create White List Item
7. Disconnect Agent from Network
8. Fetch Event
9. Fetch Files
10. Get Activities
11. Get Agent
12. Get Agent Applications
13. Get Agent Info
14. Get Agent Process
Get Blacklist
15. Get Events by Query ID and Type
16. Get Groups
17. Get Hash
18. Get Hash Reputations
19. Get Query Status
20. Get Script Results
21. Get Script Task Status
22. Get Site
23. Get Sites
24. Get Threat
25. Get Threat Analysis
26. Get Theat Events
27. Get White List
28. Initiate Scan
29. List Accounts
30. List Agents
31. Mark as Threat
32. Mitigate Threats
33. Quarantine Host
34. Query
35. Reactivate Site
36. Remove Items in Blacklist
37. Resolve Threat
38. Response Parameters
39. Set Customer ID
40. Test Connection
41. Threat Summary
42 Update Alert Verdict
43. Update Threat Incident

Legacy SOAR

1. Mitigate threat
2. Create White List Item
3. Get Activities
4. Get Agent
5. Get Hash
6. Get Site
7. Get Sites
8. Get Threats
9. Get White List
10. List Agent
11. Mark as Threat
12. Reactivate Site
13. Resolve Threat
14. Threat Summary
15. Response Parameters

The commands enabled by a typical Smart SOAR integration compared to the commands enabled by the same tool's integration with a leading Legacy SOAR platform.



Smart SOAR integrations ensure that nothing important is lost during ingestion. Imagine a scenario where your SIEM has grouped alerts together to create a higher-level incident and escalated it to your SOAR tool. What happens when the SIEM detects new related alerts and adds them to the incident? Legacy SOAR doesn't ingest the new alerts and correlate them to the existing incident. Smart SOAR can.

D3 has a team that is dedicated to deep understanding of the products with which we integrate. That knowledge ensures our customers can effortlessly integrate with their other tools and stitch together data from different platforms into a single, normalized stream. Other SOAR vendors operate a self-service model, expecting the customer to understand the API capabilities of all of their tools and do the heavy lifting of aggregating all the important data through playbooks and Python scripts. This limits customers' ability to effectively implement use-cases that they need, because they lack the internal resources to build integrations. D3's Smart SOAR handles everything through expertly designed integrations that enable the inflow of data and outflow of automated actions that support the rest of Smart SOAR's differentiators.

Legacy SOAR	Smart SOAR
Mix of pre-built and community-built integrations.	**Professionally built and maintained integrations.**
Integrations are limited by vendors' corporate agendas, resulting in pressure on customers to use specific toolsets.	**Unlimited number and scope of integrations. Connect to the best of breed tools you want to use, with no compromises.**
Mix of Partner APIs and Public APIs, which have limited functionality.	**Maximized functionality through Partner APIs and Internal APIs.**
Basic integrations that rely on the customer's resources for maintenance and troubleshooting.	**Expert understanding of integrations throughout the tech stack. Removes burden from SOC team to build and maintain integrations using their own resources and expertise.**
Unidirectional integrations. Can't synchronize incident statuses and other data between tools.	**Bidirectional integrations that enable synchronization of Smart SOAR incidents with changes in other tools, via remote execution of commands.**

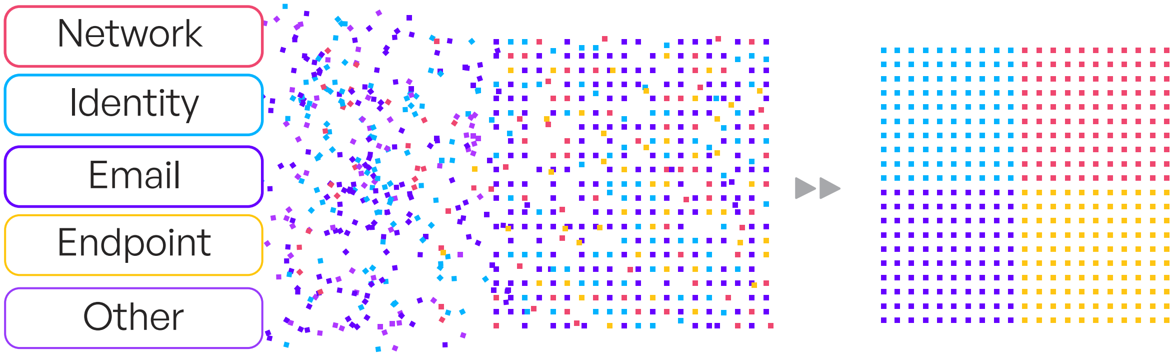
Key Outcome: Legacy SOAR burdens security teams with "self-serve" integration building, maintenance, and troubleshooting, leading to wasted time and incomplete data. Smart SOAR means that you spend zero time working with integrations, because it's all handled by the vendor's expert team.

2. Normalization

An important requirement for effective automation is to normalize the security alert data from across numerous systems. This involves collecting all relevant data from disparate sources, and, regardless of its formatting, field titles, and conventions, transforming it into a standardized format. By doing so, it becomes much easier to automate processes and perform analysis on the data.

Legacy SOAR cannot normalize data, so alerts and artifacts from different sources cannot be automatically compared. It's apples and oranges. So, users lose time, make mistakes, and get burnt out jumping from tool to tool to dig for the data they need to reveal the relationships between alerts and artifacts. This slows down their response times and closes the door to many of the major benefits that SOAR can bring.

D3's Smart SOAR normalizes all data in its Event Pipeline, which gives it the ability to conduct effective automated triage. For example, a normalized database allows for correlation across different telemetries and technology stacks. Data from various sources can be combined and analyzed to provide a more complete picture of an event.



Additionally, Smart SOAR can label tactics, techniques, and procedures (TTPs) associated with specific alerts. This information can be correlated with frameworks like MITRE ATT&CK and D3FEND. This information can be used to identify patterns and trends in the data and develop dismissal rules that can automatically dismiss alerts that are unlikely to be genuine threats.

Legacy SOAR	Smart SOAR
Ingest and process fewer than 50 alerts per minute. Ingestion failures cause alert backlogs to accumulate.	**Ingest and process up to 2000 alerts per minute.**
Alert data across tools can't be compared because of different formats and require manual coordination for analysis	**Normalize all alerts for standardized and actionable data**
All alerts are treated separately	**Automatically extract artifacts and correlate across the stack to find and consolidate related alerts**
TTPs cannot be applied consistently across alerts from different systems.	**Enable application of TTPs to alerts**

Key Outcome: A standardized database of all important security alert data—the foundation for risk-based alert triage, correlation, TTP analysis, automated dismissal rules, and incident response orchestration.

Without normalization, security teams must manually assemble and correlate security alert data, leading to longer dwell times, missed incidents, and lower confidence in decisions.

3. Triage

Faced with endless streams of alerts, security teams struggle to locate the signal in the noise because Legacy SOAR:

- Does not fully leverage available external threat intelligence and internal data, such as the company's CMDB.
- Does not incorporate identity data into analysis.
- Does not operationalize TTPs and IOBs to identify suspicious patterns of activity.
- Cannot correlate against past incident data to reveal trends.
- Does not correlate across data siloes. EDR alerts are triaged with EDR data, etc.

In D3’s Smart SOAR, security teams are given the clarity they need to make sense of real threats and spend much less time on false positives. Instead of a single tier of automation for enriching and responding to incidents, D3 has two separate tiers: one for triage that is applied to every incoming alert as part of the Event Pipeline, and one for investigating and remediating validated incidents.

In the Event Pipeline, alert data can be correlated against, and enriched with, data from threat intelligence sources, the company’s CMDB, and access policies, asset inventories, and other sources. Nested playbooks can be triggered by enrichment to conduct further investigation. At this stage, alerts are deduplicated and related alerts are grouped together for efficient analysis. This stage ensures that alerts are high-fidelity with accurate risk scoring.

Identity & Memory

Smart SOAR also uses two key elements during triage that Legacy SOAR often ignores: identity and memory.

Identity

Capturing important data like user roles, user IDs, device IDs, and cloud accounts, so that the triage process can incorporate the significance of who is involved in the alert. If the same person’s device and accounts are both involved in alerts, that suggests something serious is going on.

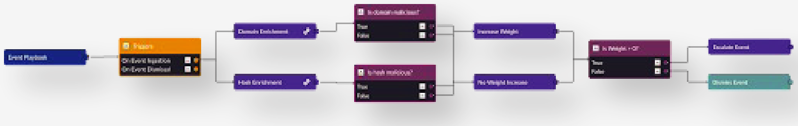
Memory

Retaining alert data for 90 days so it can be queried to find recurring IOCs, techniques, and targets.

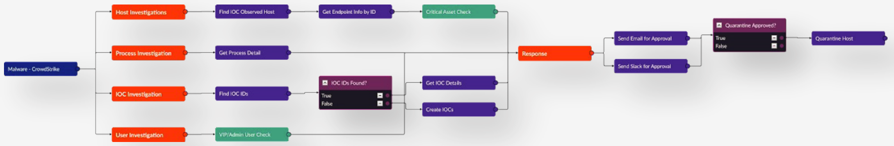
Using memory, identity, and indicators of behavior, cross-stack correlation is extremely powerful. Take for example, a pre-built event playbook for MITRE technique T1566, a phishing attempt. The playbook normalizes, parses, enriches, and correlates the artifacts from a phishing email detected from an email system, such as Office 365. The artifacts, such as a phishing email link and a malware attachment, are enriched against third-party intelligence for reputation checks. The data is then correlated against the email server to identify all the users who have received the same email or similar emails from the same sender.

By checking an integrated identity system such as Azure AD, hosts logged into by the phishing email recipients can be retrieved. Another cross-stack correlation against the network systems will search the users’ hosts’ outbound network traffic on the firewall. Likewise, a cross-stack correlation against the endpoint systems will look for evidence on whether the phishing attachment has been opened and spawned malicious processes. All of these correlations are incorporated into a severity score and escalated as an incident.

Example of Alert-Level Playbook



Example of Incident-Level Playbook



Legacy SOAR	Smart SOAR
Single tier of automation for enriching and responding to incidents.	**Dedicated automation tier for alert-level triage before escalating to the incident level.**
Threat intelligence integrations are likely to be skewed towards the vendor's in-house threat intelligence.	**Comprehensive threat intelligence integrations.**
Does not incorporate identity into analysis of risk without user coding or third-party solutions.	**Identity data for alerts, enabling triage based on users, accounts, and devices.**
Strictly IOC-based triage.	**Behavior-based triage, leveraging frameworks like MITRE ATT&CK.**

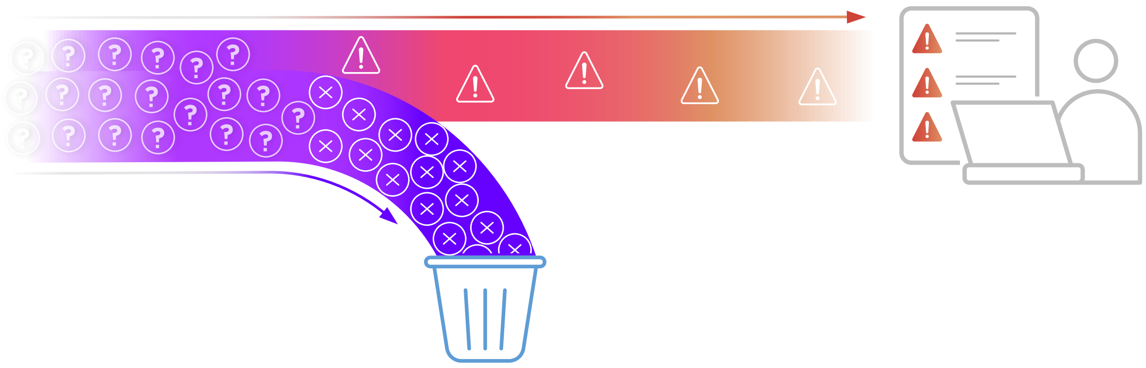
Key Outcome: Smart SOAR provides a fully contextualized view of every alert, systematically building confidence so you can always make the right decisions. Without this, analysts don't have the information they need, so they waste even more time assembling the data they need to be confident in their decisions.

4. Dismissal & Escalation

A universal concern for security teams is how sensitive they want their detection tools to be. The worst possible outcome is for a genuine threat to slip by undetected, so an easy choice is to make sure your tools escalate every alert that has any uncertainty around it. But this inundates your security analysts with high volumes of low-fidelity alerts, leading to an unacceptable amount of time spent investigating false positives. However, the information does exist to make confident dismissals and escalations—even automatically—but users of Legacy SOAR cannot achieve this, because Legacy SOAR:

- Does not operationalize behavior and identity information
- Does not effectively prioritize high-risk alerts
- Requires context-switching to get a complete picture of an alert
- Presents too many false positives to analysts

D3's Smart SOAR unlocks confident and safe dismissal of most alerts, escalating only a small number of high-fidelity, high-confidence incidents for human investigation. This is because all alerts pass through the Event Pipeline, which automates sophisticated triage, including correlation against identity data and memory of past incidents. Simple alerts can be resolved with an automated playbook, and benign alerts can be dismissed based on the user's rules. For example, if the threat intelligence scores for the artifacts are below a certain level.



Legacy SOAR	Smart SOAR
Not enough enrichment and correlation to safely dismiss false positives.	**Sophisticated rules for safe dismissal of false positive alerts.**
Does not have the internally stored information required to automatically resolve simple alerts.	**Automatic resolution of simple alerts based on triage rules and global list.**
Lacks the identity, memory and TTP correlation capabilities for risk-based alert triage.	**Comprehensive risk-based triage to escalate high-risk incidents.**
Strictly IOC-based awareness, so suspicious patterns of activity based on behavior or identity cannot be detected.	**IOC, IOB, and identity awareness for identifying and escalating anomalous incidents.**

Key Outcome: 90% fewer incidents assigned to human responders. Because incident responders are not inundated with noise, they can focus on real threats, increasing retention and engagement while freeing them up for proactive tasks that improve security posture.

5. Incident Response

Adversaries of all kinds benefit from Legacy SOAR's incident response shortcomings. This is because Legacy SOAR:

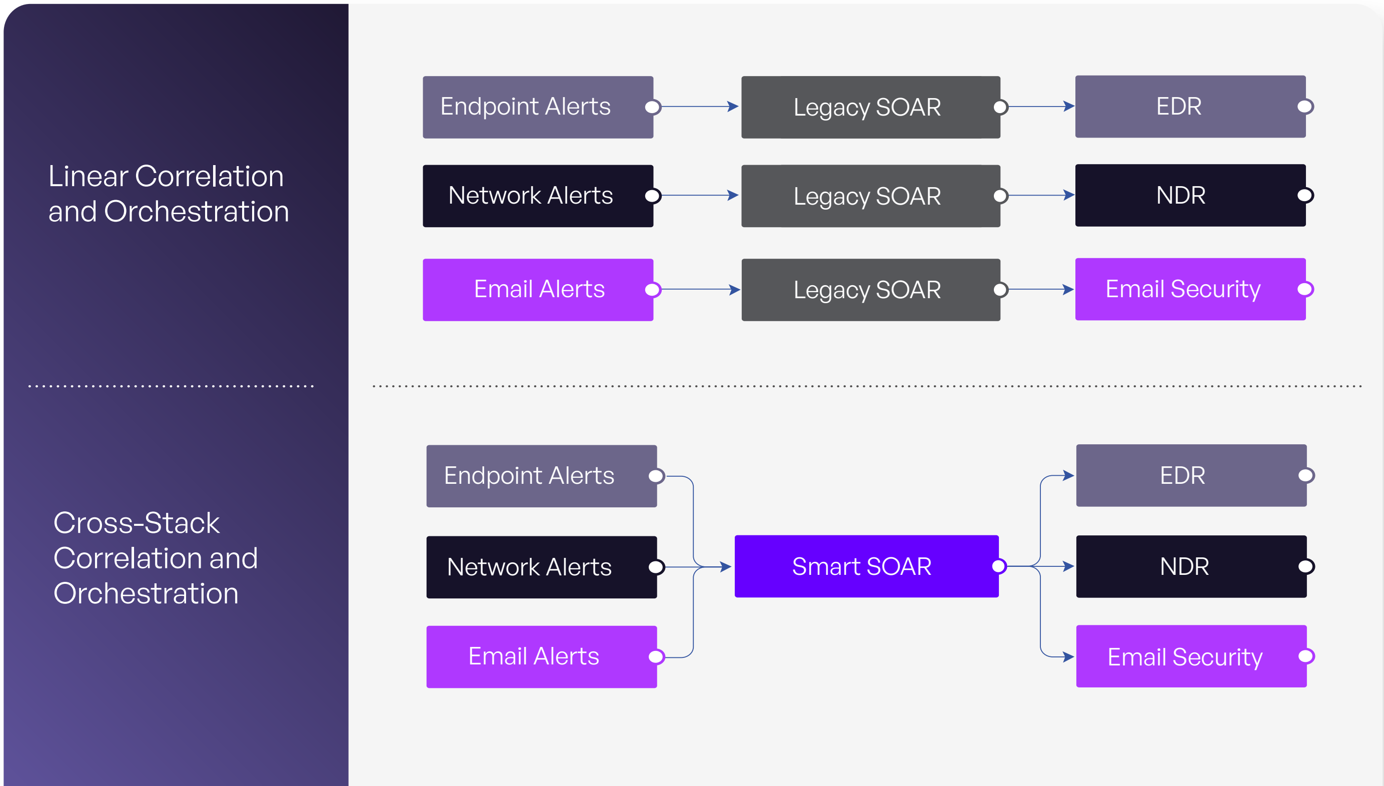
- Floods analysts with low-fidelity alerts that lack important information
- Orchestrates simple automated responses without taking into account situational awareness
- Cannot perform multi-dimensional correlation and orchestration across tools, time-frames, artifacts, and TTPs.
- Does not uncover behaviors and IOCs that could be part of the same incident

Whether you're shutting down basic phishing attempts or investigating a multi-pronged attack from a well-funded adversary, D3's Smart SOAR gives you the incident response capabilities to conclusively resolve threats at scale.

The deduplication, triage, and dismissal that is performed by the Event Pipeline means that human incident responders have far fewer incidents to investigate, and the incidents that are escalated to them are high-fidelity, complete with enriched information (e.g. OS versions, process lists, and malware families), artifact relationships (e.g. host machine A has been accessed by user B), risk scores, and correlated events. This means that incident responders are able to spend more time on real incidents, instead of wasting efforts on false positives.

Smart SOAR's playbooks enrich and orchestrate across the stack, meaning that no matter what the original alert source is, the incident can be holistically responded to. So, for example, an endpoint alert can be further contextualized with suspicious network traffic and the response can be orchestrated in the endpoints (deleting a file, quarantining an endpoint), the firewall (blocking a domain), the email system (searching inboxes for similar files, blacklisting a sender), and anywhere else that might be impacted by the incident.

Legacy SOAR provides quick and simple responses to incidents, normally in the form of simple automated actions. Smart SOAR, in contrast, is a mission control center for the SOC, with related alerts, artifacts, and TTPs dynamically brought into incidents for efficient investigations. Smart SOAR playbooks don't just act faster, with parallel tasks that reduce dwell time, they support the complexity required to eliminate risk, with looping tasks and ongoing surveillance of key assets and potential methods for further attacks.



Legacy SOAR	Smart SOAR
Low-fidelity alerts.	**An Event Pipeline that transforms alert noise into high-fidelity incidents.**
Linear, IOC-based enrichment.	**Cross-stack enrichment of IOC, IOB, and identity data to aid responders.**
Linear orchestration.	**Cross-stack orchestration playbooks for precise, multi-platform incident response.**
Incident responders won't get to every genuine threat because they are spending so much time on false positives and benign alerts.	**Lower of volume of incidents to investigate, allowing responders to spend more time on each genuine threat.**
No case management capabilities.	**Case management capabilities to track and audit incidents and evidence.**
Manual compiling of data for incident reports.	**Automatically generate incident reports.**

Key Outcome: Smart SOAR gives the visibility and capability to act in a unified way across the tech stack. Automated analysis in the triage stage ensures remediation actions are surgically precise, with no adverse effects due to lack of context or awareness.

D3

☎ 1-800-608-0081

D3Security.com

✉ sales@D3Security.com