D3 SECURITY

Supercharge Microsoft Security Tools with D3 Security Smart SOAR™

Microsoft Intelligent Security Association

Microsoft

Preferred solution

The Microsoft Security product portfolio is the core of many security operations centers (SOCs). To maximize the return on their investments in these tools, security teams can leverage third-party security orchestration, automation, and response (SOAR) solutions that increase efficiency, investigation quality, and interoperability within and beyond the Microsoft product suite.

Microsoft product-centric SOCs have several options regarding automation and orchestration:

Opt out of automation and manually triage alerts, perform enrichment tasks by hand, and respond to incidents across each system separately.

This is an inefficient use of precious security resources and leaves you open to risks because most alerts will go uninvestigated.

Purchase suite-based SOAR.

Many vendors sell a full suite of security tools, not just SOAR. While these SOAR tools will likely offer integrations with Microsoft products, the quality of the integration will be compromised by the vendor's conflicted interests. Why would they build the best possible integration with Microsoft Defender for Endpoint when they also have a competitive endpoint detection and response (EDR) product?

Purchase a "lightweight" SOAR tool.

Lots of the tools that vendors refer to as SOAR offer very basic capabilities. These tools are good for automating repetitive tasks, but not much else. In order to actually elevate your security operations, you need something more robust.

Considering the shortcomings of these options, the best way to integrate your Microsoft product-centric SOC to optimally leverage automation is D3 Security Smart SOAR. It's not enough to simply integrate your tools, you need deep integrations and expertly built playbooks that close the gaps in your detection tools.

D3 Security's close, collaborative relationship with Microsoft has resulted in dozens of professionally built and maintained integrations. And because no SOC uses exclusively Microsoft tools, Smart SOAR boasts unlimited integrations with third-party tools, bringing them seamlessly into your automated workflows.

Key Integrations

Among Smart SOAR's 36 (and counting) integrations with Microsoft products are Azure cloud services, collaboration tools like Microsoft Teams, and many security tools. Some of the most important integrations for security workflows are:

Microsoft Defender for Endpoint

Microsoft Defender users can orchestrate 26 different actions from Smart SOAR, including fetching events, enriching incidents with endpoint data, and quarantining infected hosts. This creates an automation-powered process for any endpoint security incident that acts quickly and conclusively before threats get out of control.

Microsoft 365

Phishing is still the entry point for most cyberattacks, which makes email a critical part of cybersecurity incident response. When a potential phishing email is detected, Smart SOAR can retrieve the email and attachments, parse out the artifacts, check the reputations of the artifacts against threat intelligence and past incidents, and determine if the email is a genuine threat. If it is, Smart SOAR can then find other instances of the email across the company's inboxes and delete them.

Azure Active Directory

Some experts say that "identity is the new perimeter," which underscores the importance of being able to act quickly in Azure Active Directory (Azure AD) during a security incident. Companies using Azure AD (and on-premises AD) can enrich Smart SOAR incidents with user and group information, manage users and groups from Smart SOAR, and quickly orchestrate remediation actions like forcing a password reset or revoking a sign-in session.

Microsoft Sentinel

Smart SOAR can centralize all information related to Microsoft Sentinel events and incidents. Whether they are from your EDR, email, identity, or network tools, using Smart SOAR and Sentinel will create a comprehensive picture of security alerts. At the same time, Microsoft Sentinel and Smart SOAR have bidirectional synchronization to keep all incident statuses, severities, notes, and updates aligned.

D3 Security's Partnership with Microsoft

Of all SOAR vendors, it is safe to say that D3 Security has the closest relationship with Microsoft. D3 Security has been a member of the Microsoft Intelligent Security Association (MISA) since 2020 and was named a finalist for the 2023 Microsoft Security Excellence Award for Security Trailblazer. The award recognizes a Microsoft partner that provides excellent security products and services to joint customers.

As a member of MISA, D3 Security has collaborated extensively with Microsoft, including presenting together on webinars and at conferences. Most importantly, D3 Security works closely with the Microsoft team on our dozens of integrations with Microsoft products. This has provided the opportunity to deliver integrations that offer advanced functionality and are always kept up to date with the latest version of each Microsoft product.

What Makes D3 Security Integrations Different

Not all SOAR integrations are created equal. Integrations that solely rely on public APIs and are not maintained or regularly updated by experts can end up wasting more of your time than they save. Unfortunately, these are the integrations that you get from most lightweight or suite-based SOAR platforms.

Take, for example, a SOAR tool made by a vendor that also sells security information and event management (SIEM) and EDR products. Will that vendor work closely with Microsoft to build the best integrations between their SOAR tool and Microsoft Sentinel and Defender for Endpoint? Of course not! They are in direct competition with those tools and would much prefer to steer their users toward the rest of the products that they sell.

As an independent vendor, D3 Security can work with Microsoft to expertly build integrations across dozens of products, while still offering great integrations with any third-party tools you might use as well. The result is deep, bidirectional integrations that leverage partner APIs for maximum functionality. Microsoft product-specific playbooks built by D3 Security are based on expert knowledge of the tools involved, enabling them to target correlations to fill any gaps in the information provided by those tools.

Best of all, the D3 Security team is always working on integrations and sharing the benefits with its clients. No "self-serve" integrations here. The setup, troubleshooting, maintenance, and upgrades all happen with expert support.

Features and Benefits of Smart SOAR

Smart SOAR isn't simply a way to connect your Microsoft Security tools; it's an enterprise-grade security operations platform that enables massive steps forward for your detection and response capabilities, including:

Autonomous risk-based alert triage.

24/7 TTP-driven incident response.

Proactive threat hunting.

100% automated risk assessments and recommendations.

SOC performance monitoring.

Intelligence Beyond IOCs

One of the important ways in which Smart SOAR exceeds the limitations of conventional SOAR products is by incorporating different types of information into its correlation and analysis. First, Smart SOAR has **memory**, retaining all alert data for 90 days. This enables historical data to be used in analysis to identify patterns over time.

Second, Smart SOAR uses **identity** data, such as 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.

Finally, Smart SOAR uses the MITRE ATT&CK framework to track attacker **tactics**, **techniques**, **and procedures** (TTPs) across alerts. This behavior-based analysis makes it easier to interrupt multistage attacks and hunt for undetected threats.

Smart Playbooks

Smart SOAR playbooks are more than simple automated sequences. The out-of-the-box playbooks are cross-dimensional (orchestrating across tools, artifacts, TTPs, and timeframes), MITRE-compliant, end-to-end workflows. Because of D3 Security's expertise with integrated tools from Microsoft and other vendors, the playbooks are not generic use cases (such as malware analysis and remediation); they are specifically designed to fill the detection and remediation gaps of the tools involved.

The codeless playbook editor empowers security teams to easily build, test, and modify their own workflows, with no vendor support or internal coding resources necessary.

The Event Pipeline

The heart of Smart SOAR is the Event Pipeline. This unique feature provides a dedicated tier of automation at the alert level before alerts even enter an analyst's queue. Upon ingestion, every alert goes through three stages of processing. Security teams that use the Smart SOAR Event Pipeline can see a reduction of alert volume of 90–98%, replacing endless false positives and low-fidelity alerts with few, high-confidence incidents to investigate.

Ingestion

As a vendor-agnostic SOAR provider, D3 Security provides feature-rich, professionally maintained integrations that leverage partner APIs and internal APIs for optimal capture of telemetry at the ingestion stage.

Stage 1: Normalization

In the Event Pipeline, embedded normalization logic extracts all the important data from alerts and standardizes it for easy correlation. This saves huge amounts of time and enables better analysis of alerts.

Stage 2: Triage

In the triage phase, alert data is correlated against – and enriched with – data from threat intelligence sources, the company's CMDB, 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.

Stage 3: Dismissal and Escalation

After the severity of an alert is determined through the triage stage, the Event Pipeline then dismisses the alert as a false positive/low-risk event, or it escalates the alert to incident status where it enters an analyst's queue. The dismissal and escalation criteria can be completely customized by the user.

Microsoft Security and Smart SOAR for MSSPs

In addition to all the features already described, MSSP partners of D3 Security that have Microsoft product-centric security stacks also benefit from:

- Full multitenancy for secure segregation of clients' data and workflows.
- Streamlined onboarding of new clients.
- A client portal that streamlines secure communication.
- The ability to offer new and high-value services based on SOAR.

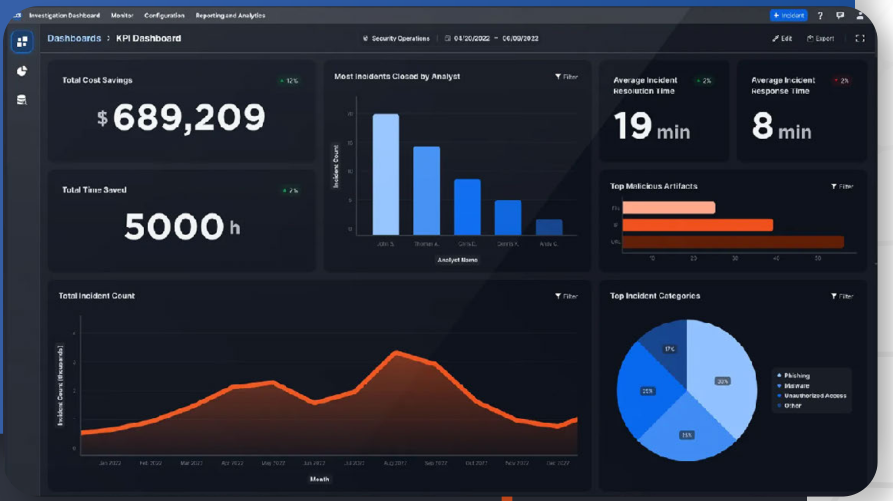
Case Study

A prominent MSSP in the United Kingdom recently signed on with D3 Security to overcome the challenges they were having with repetitive work, overly manual tasks, and lack of integration between their Microsoft tools. They needed a way to automate enrichment and triage tasks for Microsoft Sentinel events so that their analysts wouldn't have to look up the same IPs, URLs, and other entities every time they were involved in an incident. The MSSP's tools did not allow them to investigate larger incidents holistically, collaborate on cases, or effectively handle end-to-end incident response workflows with ITIL escalation.

They needed the ability to design automated workflows and to integrate their security stack, which included Microsoft Sentinel as well as Defender for Endpoint, Defender for Cloud, and Defender for Cloud Apps.

By adding D3 Smart SOAR, the MSSP was able to:

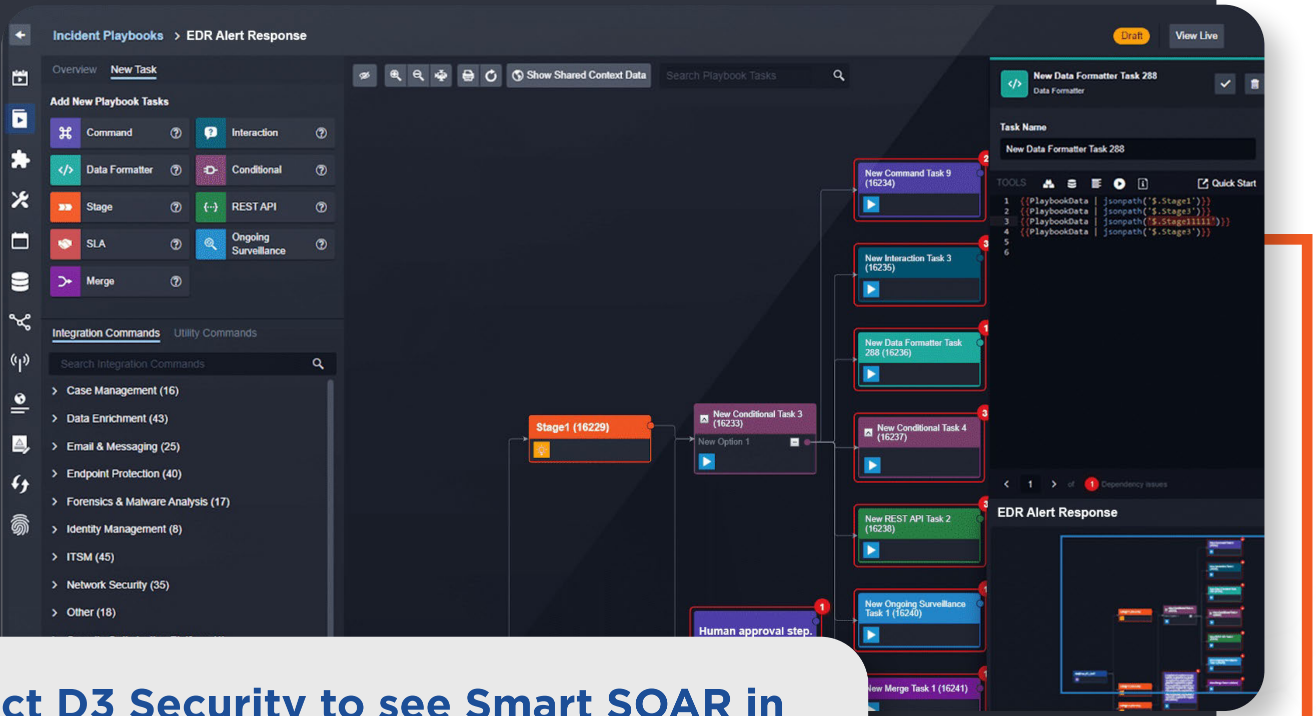
- Leverage feature-rich, bidirectional integrations between Smart SOAR, Microsoft Sentinel, and Microsoft Defender products.
- Turn alerts from across the Microsoft suite into unified, high-fidelity incidents.
- Establish a single pane of glass for all incidents, along with automated incident response playbooks and support for collaborative investigations.



Smart SOAR Playbook Examples

Use Case	Remediating phishing attacks	Failed login attempts
Microsoft integrations	• **Microsoft Sentinel** • **Azure Active Directory** • **Microsoft Defender for Endpoint** • **Microsoft Defender for Office** • **Microsoft Intune** • **Microsoft 365 Defender**	• **Microsoft Sentinel** • **Azure Active Directory** • **Microsoft Defender for Endpoint** • **Microsoft 365 Defender**
Scenario	1. A suspicious email is forwarded to the SOC by an employee, triggering the playbook. 2. The Smart SOAR playbook first leverages Microsoft Sentinel to search for other suspicious emails from the same sender, determining if it's a broad campaign or a targeted attack. 3. If Microsoft Sentinel confirms it's a wider campaign, Smart SOAR uses Azure Active Directory to gather information about the affected users, helping to identify potential targets. 4. Defender for Endpoint is then employed to search for devices where the file hash is found, identifying who has downloaded the file. 5. Next, the playbook uses Defender for Office to analyze email activity and attachments, ensuring no further malicious content is circulated. 6. Microsoft Intune checks the compliance and management state of the affected devices, evaluating whether the machines need to be quarantined or not, and reports the findings back to Smart SOAR. 7. Microsoft 365 Defender is then utilized to block the malicious file and monitor the environment for additional threats. 8. Finally, the playbook resets user credentials using Azure Active Directory and initiates a scan on affected devices with Defender for Endpoint.	1. Smart SOAR receives a "multiple failed login attempt" alert from Microsoft Sentinel, triggering the playbook. 2. Smart SOAR uses Azure Active Directory to collect user information and recent activity logs, including login attempts and their outcomes. This data helps identify unusual patterns and potentially compromised accounts. 3. Next, Smart SOAR uses Microsoft 365 Defender to analyze email activity for the affected user, checking for phishing attempts or suspicious messages that may have led to the failed login attempts. 4. Smart SOAR then uses Defender for Endpoint to check the user's device for signs of malware or unauthorized access. 5. If the investigation suggests a compromised account, Defender for Endpoint is used to enforce remote quarantine and prevent further unauthorized access. 6. Finally, the playbook uses Azure Active Directory to reset the user's password, ensuring account security.

Ready to get started with D3 Security Smart SOAR?



Task Name: New Data Formatter Task 288

```
{{PlaybookData | jsonpath('$.Stage1')}}
{{PlaybookData | jsonpath('$.Stage3')}}
{{PlaybookData | jsonpath('$.Stage11111')}}
{{PlaybookData | jsonpath('$.Stage3')}}
```

Contact D3 Security to see Smart SOAR in action and discuss how we can best help you reach your security operations goals.

LEARN MORE