The SecOps Handbook to TDIR

splunk>
a CISCO company

There's a lot of buzz about the latest cyber threats — and world-weary security analysts are keenly aware. Malware has mutated to great new heights; AI has introduced a slew of attack vectors; and cybercrime syndicates are coming up with crazier tactics. (And even crazier names — who had Peach Sandstorm on their cybercrime bingo card?) Bottom line: It's tough out there if you're a security analyst. Believe us, we know.

In the 2024 State of Security report, 46% of security pros said they were struggling to keep up with cybersecurity requirements. To make matters worse, security teams are overwhelmed by an endless sea of data — spending too much time analyzing logs across multiple tools in an attempt to identify and protect the right data at the right time.

More ~~money~~ security tools, more problems

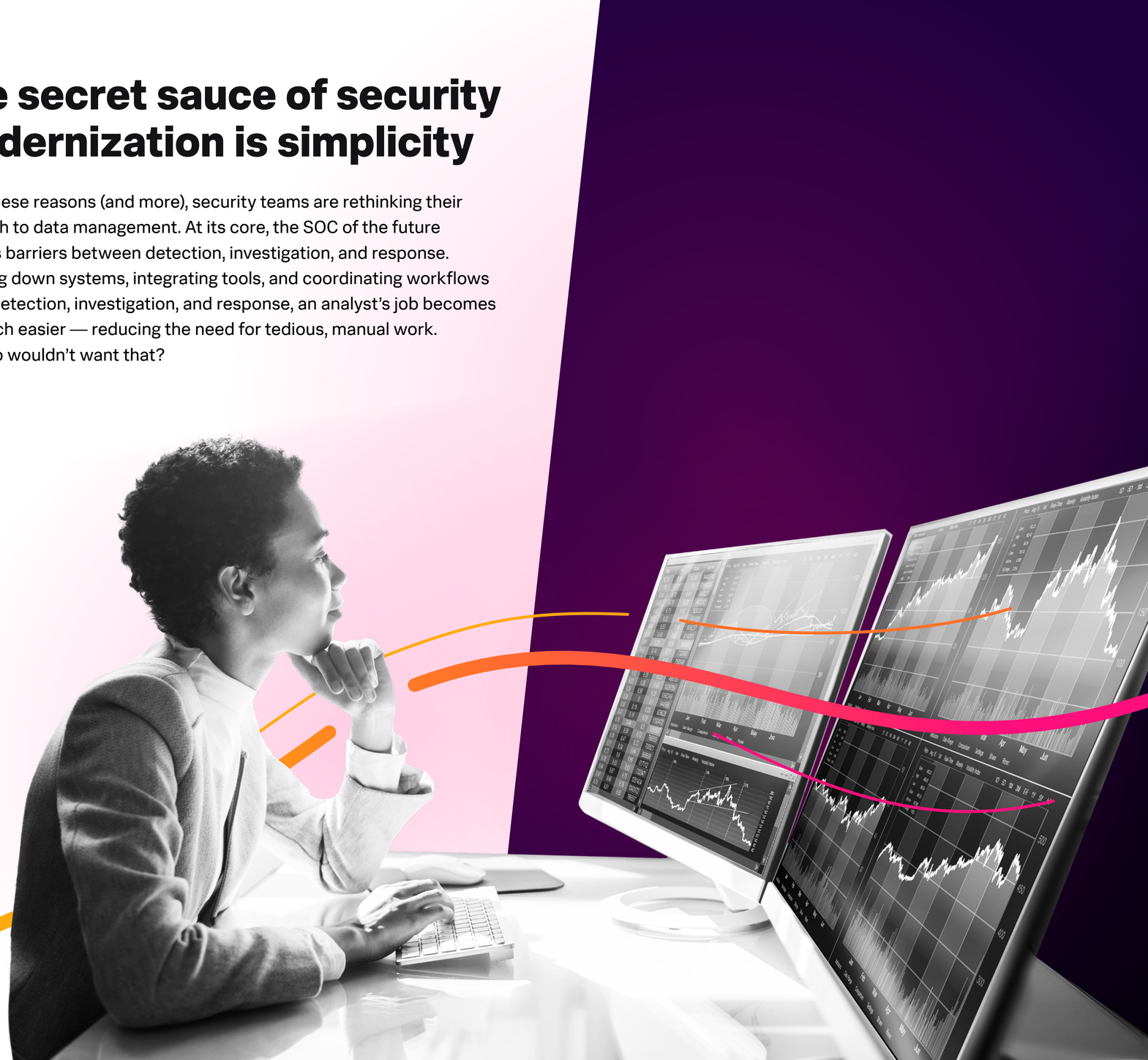
Organizations big and small often rely on "swivel-chair security," according to the latest ESG SOC Market Trends report. Analysts pivot from one tool to the next, extracting and analyzing security logs from a dizzying range of tools. Unsurprisingly, this is labor-intensive and bogs analysts down, making it much harder to glean key insights when the time is ripe.

Mid-sized to large organizations also expect to triple the data collected across on-premises, edge, and public cloud locations by 2028, according to Gartner. This means even more data to track and protect.

That's why to do their job (and to do it well), analysts need a unified view of their environment and all that it contains — allowing them to effectively filter, correlate, and contextualize events while reducing the volume of low-fidelity alerts. SecOps teams can then spend less time sifting through excess data, allowing them to focus on what matters the most.

The secret sauce of security modernization is simplicity

For all these reasons (and more), security teams are rethinking their approach to data management. At its core, the SOC of the future removes barriers between detection, investigation, and response. By paring down systems, integrating tools, and coordinating workflows across detection, investigation, and response, an analyst's job becomes that much easier — reducing the need for tedious, manual work. And who wouldn't want that?



The name of the game: TDIR

Enter TDIR: a common set of practices that brings everything together into a neat little package — including all of your workflows, security tools, and data.

In essence, TDIR is a platform approach to security that unifies threat detection, investigation, and automated response. TDIR isn't a one-and-done approach to security, of course — it's an ongoing process comprised of three key stages:

- **Threat detection:** Your security team discovers unusual behavior on the network — like an employee accessing a large amount of sensitive data. This triggers an alert for an insider threat or data exfiltration.
- **Investigation:** An analyst investigates the event, looking into the employee's recent activities, network logs, and other data sources. They might find that the employee's account was compromised in a phishing attack, and the abnormal behavior is part of an ongoing attack. The team prioritizes this incident as high risk due to the sensitive data involved.
- **Response:** The security team acts immediately to isolate the compromised account, change passwords, and block the attacker's IP address. They also work with IT to patch any known vulnerabilities.

Central to a TDIR platform is a modern security information and event management (SIEM) solution, which helps you:

- **Create a comprehensive view.**
  Aggregate logs from different devices, endpoints, and applications for a centralized view of your security posture.
- **Step up threat detection.**
  Analyze network traffic and endpoint behavior to detect anomalies that potentially indicate a breach.
- **Accelerate threat investigation and hunting.**
  Home in on signs of malicious activity to get ahead of new and emerging threats.
- **Orchestrate and automate response.**
  Automate repetitive tasks so you can focus on deeper analysis and high-priority tasks.

Each stage of the workflow is connected. The investigation depends on data from the initial detection, and the response stage is informed by the lessons learned and insights gleaned during the previous stage, creating its own special security daisy chain.

TDIR alleviates SOC headaches like:

- Manual investigation
- Digital complexity
- Lack of visibility
- Insufficient context
- Skilled personnel shortage

The SOC of the Future

A platform that unifies the TDIR process is central to creating a SOC that is resilient in the face of emerging threats. According to the Cisco Cybersecurity Readiness Index, nearly 75% of organizations expect to be impacted by a cyber incident within the next two years, with 84% of executives claiming efficacy and efficiency as a top five priority. In light of this, organizations are modernizing SecOps — namely, how they can manage data volume and complexity in the face of digital transformation.

The secret sauce of security modernization is simplicity. At its core, the SOC of the future removes barriers between detection, investigation, and response. By integrating disparate tools and coordinating workflows, an analyst's job becomes that much easier, reducing the need for tedious, manual work.

A SOC of the future can help you:

- Handle and secure large volumes of data while maintaining compliance and governance.
- Reduce risk exposure and minimize vulnerabilities through specific measures like security audits, patching, and strong access controls.
- Enhance operations with AI and machine learning to enhance threat detection, analysis, and response, allowing for faster and more accurate security operations.
- Detect threats and leverage advanced technologies like behavioral analytics and threat intelligence to identify sophisticated or unknown security threats.
- Automate repetitive security tasks (e.g., triage, alerting, patching) to improve efficiency, reduce human error, and free up analysts for higher-priority work.

Tools that play together, stay together

Let's dive into how a unified TDIR solution stacks up next to different tools on the market:

SIEM + TDIR

SIEM technology is foundational to a unified TDIR solution and helps organizations see the interplay of data from different systems and domains. By integrating various tools and views into one system, a SIEM solution is a much more proactive (and holistic) approach to cybersecurity, especially when combined with machine-learning capabilities. A SIEM solution can help SecOps teams:

- Detect and deliver key insights.
- Prioritize incidents based on integrated intelligence.
- Conduct flexible investigations for effective threat-hunting.

SIEMs are ideal for continuous monitoring, real-time detection, investigation, and automated response, and can help security teams turn the chaos of meaningless alerts into relevant, actionable intelligence — shifting their focus to what matters the most.

XDR/EDR/NDR + TDIR

Other tools can also support TDIR, including extended detection and response (XDR), endpoint detection and response (EDR), and network detection and response (NDR). These tools support TDIR to a degree, but their scope is limited with little-to-no visibility outside their given domain.

It's difficult to capture the full breadth of a threat across network, server, cloud, and other environments — as a result, XDR, EDR, and NDR tools can't correlate endpoint data with activity across the broader infrastructure — like network traffic, cloud interactions, or application behavior.

The lack of visibility across tools also makes it hard to detect sophisticated, persistent threats that require advanced forensic investigation throughout long periods. TDIR platforms, with their broader investigative scope and historical data analysis, are more adept at tracing advanced persistent threats (APTs) and uncovering subtle signs of compromise over extended timeframes.

AI + TDIR

Perceptions of AI are changing fast. Just eight months ago, only 17% of respondents in the 2023 CISO report — Splunk's annual findings on how CISOs are addressing the latest threats — said AI would give an advantage to defenders. Now, almost half (43%) feel the same way, according to the State of Security.

AI technology is primed to revolutionize the SOC, particularly when it comes to automating threat hunting and threat detection. Traditionally, threat detection relied on signatures and correlation rules that looked at explicit attack conditions (like known knowns) — but this method falls short when conditions change.

With the power of AI, security teams can identify attacks that would otherwise be missed by standard correlation searches and can better assess what qualifies as anomalous behavior, pinpointing activities that might reveal a high-risk incident.

Without Splunk, we wouldn't have a successful student-powered SOC program.

— Sumit Jain, CISO, LSU

Louisiana State University students have the eye of the tiger when it comes to cybersecurity.

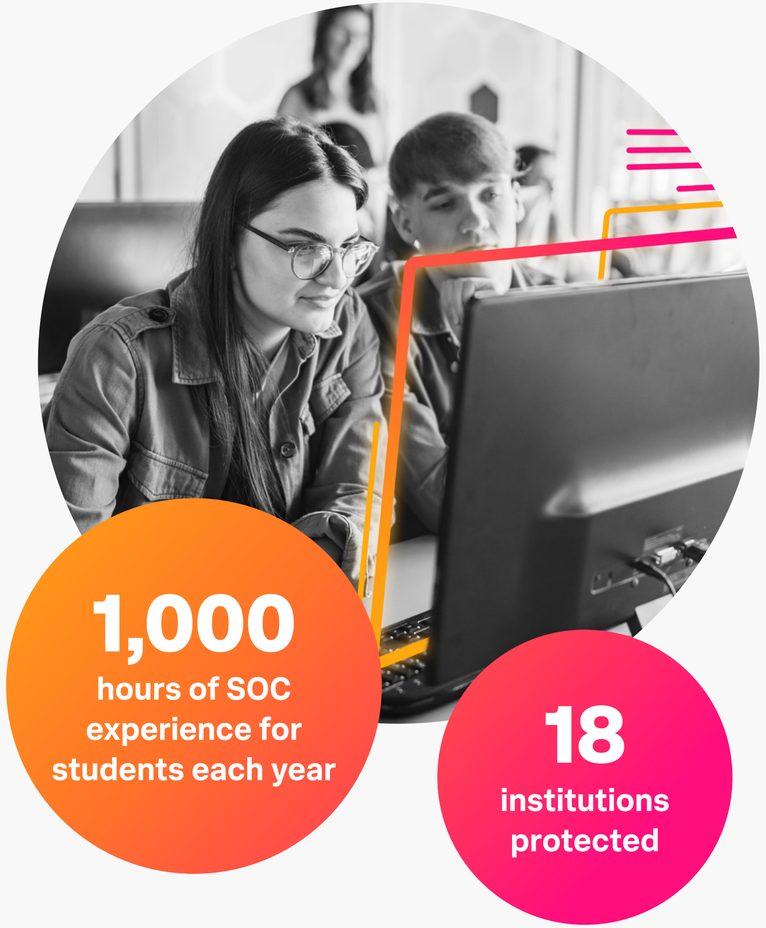
Key Challenges

As a leading cybersecurity institution, LSU wanted to offer students hands-on experience in security operations centers (SOCs) and increase the cyber posture of all higher education in Louisiana.

Enter Splunk and managed security provider TekStream. Now, LSU's student-powered SOC program is live at 18 Louisiana institutions and counting. And adoption is accelerating fast, expected to reach as many as 38 institutions by 2025. LSU is swiftly improving the cybersecurity of academic institutions across the state, positively contributing to workforce development, and laying the groundwork for a nationally leading cybersecurity curriculum.

Key Results

To the CISO at LSU, the main benefit of leveraging Splunk in its student-powered SOC program is its ability to identify and report notable security events in a more consumable fashion. "Being able to bring all incidents into a single environment has had the biggest impact on the efficiency of our program and the safety of participating institutions," says Jain. Otherwise, each institution would have to check its own environments to see what notables came up. "Instead," he continues, "we work through a single pane of glass on top of an institution-level single pane of glass. Without Splunk, we wouldn't have a successful student-powered SOC program."



What truly sets this program apart is its inclusivity of the entire campus community. Student-powered SOCs typically gear toward IT, cybersecurity, and computer science majors. "Our leadership team and Board of Regents want this to be an opportunity for everyone," says CIO Craig Woolley. "Therefore, the program is open to students of all disciplines. The only criteria we look for is the ability to think critically. If they can do that, everything else can be taught.

Breaking down the TDIR workflow

From threat detection to investigation to response

By coordinating efforts across detection, investigation, and response, SecOps teams can speed up mean time to resolution (MTTR) across operations; eliminate analyst grunt work; and thwart advanced attacks. Below, we break down what this workflow looks like, and how organizations can leverage their data and workflows accordingly.

1. Gather data

Aggregate and triage data

Data collection is the proverbial bread and butter of security monitoring. To develop foundational, end-to-end visibility, security teams need to be able to ingest, normalize, and index log data from across their infrastructure to perform search and analysis. By filtering, redacting, and routing data, security teams can focus on what matters the most while controlling for cost and complexity.

Ideally, a TDIR solution will collect and compile data from a range of tools, systems, and applications, routing and filtering out event data based on the relevant use case(s). Once the correct data sources are validated, log entries are consolidated and distilled into a handful of actionable security alerts. Teams can also enrich and correlate alerts with context from additional data sources, empowering practitioners to spend less time on non-actionable alerts and false positives.

Data sources to ingest include:

- **Endpoint:** Application and process execution, file integrity monitoring, network connections using extended endpoint detection and response (EDR) capabilities.
- **Application:** Business-critical applications like financial systems, systems processing sensitive data, customer data, and logs that record user activities.
- **Database:** Audit and transaction logs to identify unusual patterns of behavior, modification or deletion of records, and potential unauthorized access to sensitive or restricted records.
- **Cloud:** Software as a service (SaaS) business applications for user monitoring, infrastructure as a service (IaaS), and platform as a service (PaaS) environments (e.g., AWS and Azure).

Data management

Searching and accessing data across multi-cloud services and data stores can be a challenge, but a comprehensive TDIR solution can easily sift through swathes of data with data federation. This allows organizations to access relevant, high-quality data from any environment across the enterprise, whether it's stored in a data lake, cloud provider, or other location. Teams can then bring in select data on demand to accelerate detections or perform intensive drill-down searches. This not only preserves data integrity and reduces latency, but also ensures comprehensive visibility by allowing access to and the analysis of data across all storage locations.

Asset management

Per ESG research, 69% of respondents experienced at least one cyberattack that started by exploiting an unknown or unmanaged asset.

As organizations grow their business and expand their digital footprint to the cloud, security teams struggle with asset discovery and inventory (ie., identifying all devices, users, and applications across the network), exposing them to the risk of cyberattacks, data breaches, insider threats, and compliance issues.

Ideally, the SOC of the future should prioritize continuous asset discovery to better contextualize investigations. By integrating detailed asset and identity context as part of a unified TDIR solution, SOC analysts can quickly piece together the relationships and activities associated with potential threats, providing a clearer picture for faster incident investigations and helping identify compliance gaps in security controls.

Analysts need to figure out their most critical assets and what to protect and monitor in order of priority. By identifying and defining their most critical assets across their security stack, SOC teams can create the foundation for incident alerts, risk profiles, and threat models. But first, they need to know what data to monitor before they can fully protect and prioritize it.

This means having a clear understanding of the crown jewels of the organization — which could be anything from a customer database to personally identifiable information (PII) to cloud-based financial systems. By taking stock of what matters the most, you can prioritize the assets in your SOC to make sure alerts related to those assets are investigated first and foremost.

2. Identify and investigate threat(s)

Use threat detection models and frameworks

Analysts look at the big picture to identify a threat — not just a fragment of it. To achieve this, a TDIR approach looks at industry best practices, including detection frameworks like the MITRE ATT&CK framework and the Splunk Enterprise Security Threat Intelligence framework to help security teams home in on attacks based on well-known tactics, techniques, and procedures (TTPs).

Threat detection models and frameworks (like MITRE ATT&CK) can help you map assets to risk, and define the subsequent process, policy and indicators of compromise (IOCs) to look for (and what remediation looks like based on these details).

By focusing on detection frameworks like MITRE ATT&CK, security teams can reduce alert noise through a combination of static detections, ML detections, and risk-based detections. Automatic threat intelligence enrichment must also be applied to enhance alerts to surface additional indicators of compromise (IOCs).

The following MITRE ATT&CK tactics have been used to categorize some of the primary security detection use cases for TDIR:

- **New User Account Creation:** This detection identifies users/newly created accounts that have been added to your network in the past week.
- **Powershell Disable Security Monitoring:** This detection identifies attempts to disable various security features.

Threat intelligence

Threat intelligence frameworks — including MITRE ATT&CK, the NIST cybersecurity framework, and the Lockheed Martin Cyber Kill Chain — allow security teams to identify IOCs across different controls and protected systems. This helps organizations understand the threat landscape — particularly as it relates to the systems and users that they're protecting — as well as identify known IoCs that would otherwise go undetected by traditional or siloed security controls.

Examples of this include IP addresses, URLs or file hashes associated with phishing activity, or identifying information relating to an SSL certificate known to be used for malicious purposes.

Risk-based alerting

It's also important to incorporate the risk profile of relevant assets and systems. Risk scoring is a key part of security analytics and helps inform the basis/prioritization of security alerts and threat detections.

Examples of risk profiles include:

- **Asset risk profile:** What is the business impact of an incident affecting this asset? What is the likelihood of an incident affecting this asset? What is the security posture of this asset? What is the sensitivity or importance of the data processed or contained within this system? What types of users typically access or rely on this system?
- **Identity risk profile:** How important is this identity? Is it a service account, administrative account, executive-level user account or contractor account? Is it an account that is more likely to be targeted or is it inherently untrustworthy? What will the impact be if this identity is compromised? Is the user a flight risk?

3. Rapid response

Use automated orchestration and response

Security orchestration, automation, and response (SOAR) is an integral part of TDIR, as it helps harmonize discordant tools and ensure that from start to finish, all of the data comes together into a fine symphony of information that your security team can understand (and, most importantly, act on).

Gartner defines SOAR as "solutions [that] combine incident response, orchestration and automation, and threat intelligence management capabilities in a single platform." Without security automation and orchestration, security teams would be left to investigate every alert and threat manually. In today's world, this simply isn't feasible, and is practically a guarantee for disaster.

Let your SecOps SOAR

At the heart of SOAR are two major facets: orchestration and automation.

- **Security orchestration** connects all your tools and data, even when spread across distributed systems. The orchestration piece uses multiple automation tasks for a complete workflow, with a beginning and end.
- **Security automation** is all about simplifying and automating individual tasks: if this one thing happens, then this is the thing to respond with to fix it.

While just one of these can be a powerful tool in a SOC team's arsenal, automation and orchestration are best used in concert. These streamlined, automated workflows facilitate quicker investigation and response, reducing the risk of a successful breach. The coordinated effort across detection, investigation, and response not only speeds up the response process but also reduces complexity and manual efforts that are still all too common. Ultimately, this will allow to SecOps teams to move from being overwhelmed to being in control.

SOAR playbooks

Teams can orchestrate actions with playbooks that automatically triage and contain a malicious attachment from a phishing email. For developers, synthetic tests can highlight problems before the code is released, and user monitoring gives insight into the user experience along with any potential issues so that the code can be rolled back if and when needed.

These streamlined, automated workflows facilitate quicker investigation and response, reducing the risk of a successful breach. The coordinated effort across detection, investigation, and response not only speeds up the response process, but also reduces complexity and manual effort. With zettabytes of data to make sense of, automated workflows become all the more critical. This could look like basic automation — like enriching an IOC with external threat intelligence — all the way through advanced automation, like the complex multi-step automation of employee-reported phishing emails.

Similar to detections, the creation and management of these automation "playbooks" should support modern content management approaches, including full CI/CD pipeline support. And, like threat detections, the playbook content should map to common frameworks like MITRE D3FEND.

At a high level, SOAR can solve three major security challenges:

- Harmonize the data from other tools in the larger security stack
- Reduce noise while providing the ability to prioritize alerts
- Respond to threats via automation with speed and accuracy

A unified approach to security operations

With Splunk, security teams can get help across this entire TDIR workflow, gaining comprehensive visibility across the hybrid and edge technology landscape, including powerful tools for investigation and response, at scale. Teams gain a shared view of data with a common search language and tooling, simplifying cross-team collaboration to drive greater digital resilience across your organization.

How Splunk can help with TDIR

With an enterprise-grade platform, SOC teams have data and tools unified within a common work surface, helping them align within and across teams and technology.

- **Get out of fire-fighting mode:** Splunk security solutions are powered by an AI-enhanced platform, extended with industry-defining products (like Splunk Enterprise Security, Splunk SOAR, Splunk User Behavior Analytics, and Splunk Attack Analyzer), transforming your SOC from reactive chaos to a modern, unified TDIR experience.
- **Empower teams with one unified work surface:** Simplify security workflows by codifying processes into response templates to build repeatable processes. Empower security operations with the speed of automation right from single, modern work surfaces, and any stakeholder can have a real-time view of what they care about on Glass Tables.
- **Use automation to respond faster:** By automating manual, repetitive security processes across your integrated security stack, you can make a team of three feel like a team of 10. Splunk SOAR provides security orchestration, automation, and response capabilities that empower your SOC, allowing security analysts to work smarter, not harder, by automating repetitive tasks and triaging security incidents faster.

Search, analysis and visualization for actionable insights from all of your data, from edge to cloud.

Start Your Free Trial.

Keep the conversation going with Splunk.

splunk> a CISCO company

25_CMP_ebook_the-SecOps-handbook-to-TDIR_v5