How SOAR Is Transforming Threat Intelligence

The benefits of digital transformation for any enterprise are clear, but the transformation also comes with security implications as new technologies expand the attack surface, enabling attackers to come from anywhere. With cloud computing, automation, and artificial intelligence now mainstream, attackers can carry out their campaigns at unprecedented levels of sophistication and scale with minimal human intervention. Today, threat actors attack computers every 39 seconds.[1] A report by Cybersecurity Ventures projects that by 2021, a business will fall victim to ransomware every 11 seconds.[2] This is only possible because attackers are taking advantage of machine speed.

1. "Hackers Attack Every 39 Seconds," Security Magazine, February 10, 2017, https://www.securitymagazine.com/articles/87787-hackers-attack-every-39-seconds.
2. "Global Cybercrime Damages Predicted To Reach $6 Trillion Annually By 2021," *Cybercrime Magazine*, Cybersecurity Ventures, December 7, 2018, https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021.

How can enterprises keep up? It is increasingly arduous to implement and maintain a healthy security posture throughout an entire enterprise without disrupting business. This is where the security operations center (SOC) plays a vital role. SOC teams are responsible for addressing this challenge of keeping pace, using a combination of integrated security technologies, streamlined processes, and human power to detect, investigate, and respond to advanced cyberthreats.

Unfortunately, security teams of all sizes are overwhelmed and unable to function at full capacity due to a shortage of cybersecurity skills, high volumes of low-fidelity alerts, a plethora of disconnected security tools, and lack of external threat context. To address these challenges, we first need to break down the inner workings of a SOC and get a sense of what happens. Only then will we be able to appreciate the enormity of what SOC teams are up against and begin to apply solutions that work.

In larger organizations, mature security operations teams have a lot of moving parts. Three main functions make up effective security operations: SOC analysts, incident responders, and threat analysts.

SOC Analysts

SOC analysts look at thousands of internal alerts daily, sourced by security information and event management (SIEM) technologies, endpoint detection and response (EDR) systems, and sometimes hundreds of other internal security tools. Their job is to be the eyes of the enterprise: to detect, investigate, determine root cause of, and respond quickly to security incidents. SOC analysts continuously monitor the network using detection tools, identifying and investigating potential threats. Once they identify a potential risk, analysts also need to document their findings and share recommended actions with other stakeholders.

All this means SOC analysts often struggle with:

- **Alert fatigue:** The average enterprise receives more than 11,000 security alerts per day,[3] and doesn't have enough people to handle them.
- **Lack of time:** Repetitive, manual, and administrative tasks take too long. A lack of integration across the many tools analysts must use slows down every stage of the process.
- **Limited context:** It often takes days to investigate and respond to threats. Security tools don't provide adequate context on alerts or their relevance to the environment, forcing analysts to piece these things together manually.

To overcome these problems, analysts need:

- **Automation** to take care of daily tasks so they can focus on what really matters.
- **Real-time collaboration** with the rest of the team so they are always in sync and learning from one another.
- **Threat intelligence** that delivers context to help them understand the relevance and potential impact of a threat.

Figure 1: SOC analyst challenges

Incident Responders

Incident responders are worried about damage control. They look for possible breaches, and If they find evidence of one, their job is to investigate and prevent it from spreading. Due to the sensitive nature of breaches, all evidence needs to be well-documented and shared with all the stakeholders. Incident responders have access to tools that help them contain breaches, such as EDR tools to kill the end host. They engage firewall administrators to deploy policies that block propagation at the network level. They heavily rely on external threat intelligence to learn about the profiles and common techniques of attackers, allowing them to respond confidently and with precision.

Accordingly, incident responders are challenged when it comes to:

- **Knowledge transfer**, where a lack of collaboration between teams introduces gaps in security.
- **Case management**, because generic case management is not ideal for security use cases, resulting in inefficiency and poor documentation.
- **Lack of threat intelligence** as many incident responders are forced to use manual, flawed processes to gain context around external threats, causing delays and risks.

3. According to a commissioned study conducted by Forrester Consulting on behalf of Palo Alto Networks, February 2020. As of the publication of this document, the report has not yet been officially released.

Incident responders need:

- **Full security case management** to document their findings in detail and enable them to collaborate in real time with other stakeholders as well as provide preventive and quarantine measures across the enterprise.
- **Threat intelligence** to provide deeper context around attackers and their motivations.

Figure 2: Incident responders challenges

Threat Intelligence Analysts/ Programs

Threat analysts identify potential risks to organizations that have not been observed in the network. They provide context around potential threats by combining external threat intelligence feeds from multiple sources with human intelligence. According to a recent survey conducted by the SANS Institute, 49.5% of organizations have some type of a threat intelligence team or program with its own dedicated budget and staffing.[4] This is evidence of the growing importance of threat intelligence analysts, who help to identify attackers, uncovering their motivations, techniques, and processes. Threat intelligence teams pass their findings on specific attacks as well as broader threat landscape reports to SOC and incident response teams to build better preventive measures.

Threat intelligence analysts face:

- **Lack of control** over threat intelligence feeds, forcing the analysts to manually tune and score indicators of compromise (IOCs) to match their environment.
- **Siloed workflows** causing poor communication and integration between incident response and threat intelligence tools, teams, and processes.
- **Difficulty taking action** since putting threat intel into action is highly manual and relies on other teams.

Threat intelligence analysts need:

- **Full control** over threat intelligence feed indicators to build their own logic and reputation based on their environment and business needs.
- **Collaboration** with other teams to quickly arm them with rich context and up-to-date research.
- **Robust documentation** to capture their findings.

Figure 3: Difficulties facing threat analysts

4. "2020 SANS Cyber Threat Intelligence (CTI) Survey," SANS Institute, February 11, 2020, https://www.sans.org/reading-room/whitepapers/threats/paper/39395.

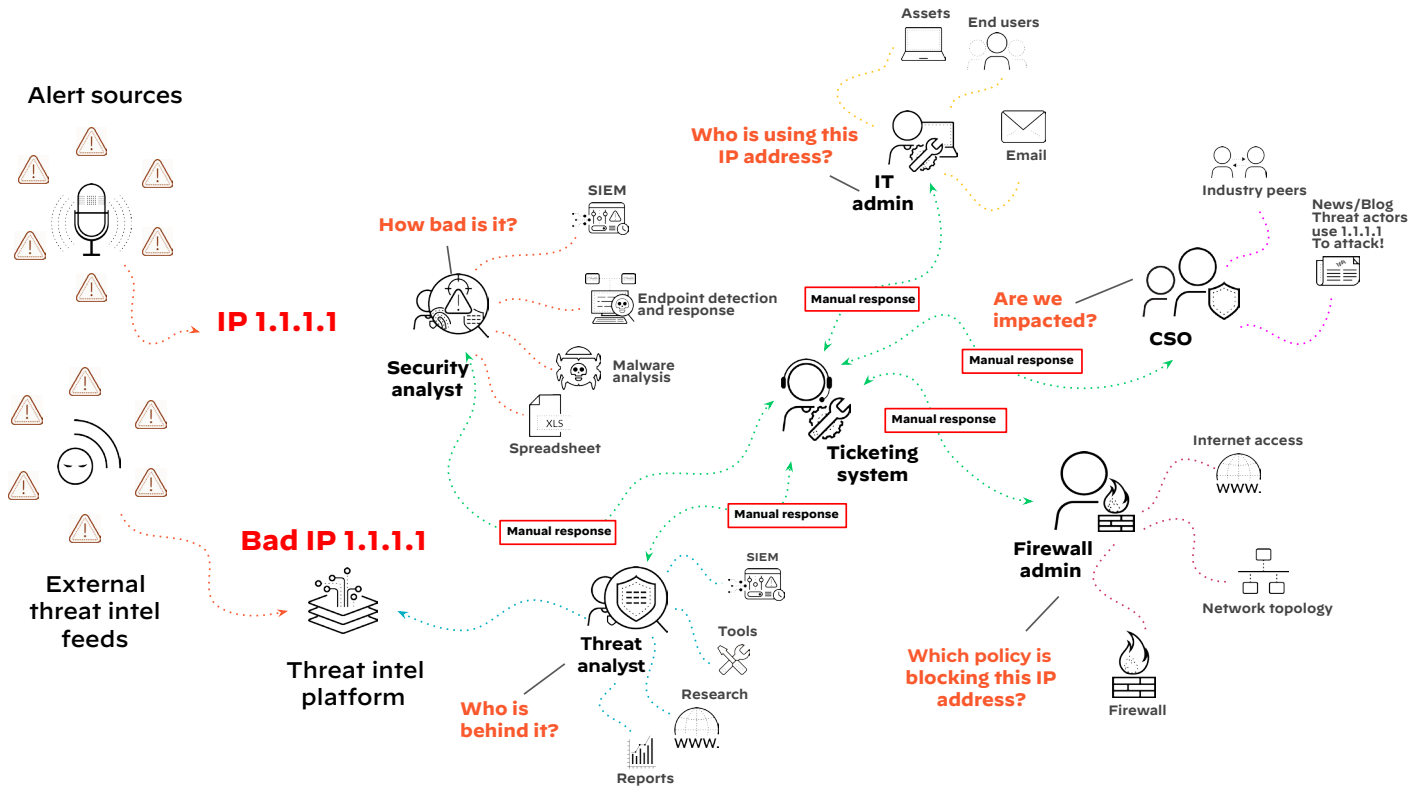

Figure 4: Holistic view of a typical day in a SOC

SOAR to the Rescue

There is an underlying theme across these teams: They all need automation, case management, real-time collaboration, and close tie-ins to threat intelligence. Many SOCs use security orchestration, automation, and response (SOAR) platforms to manage alerts across all sources, standardize processes with playbooks, and automate response for any security use case, but there is still a significant gap when it comes to threat intelligence management.

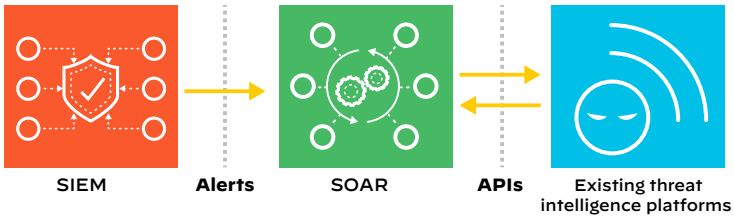

Figure 5: A typical SOAR + TIP siloed deployment

Security teams still rely on siloed threat intelligence platforms (TIPs) to provide visibility into external threats, but TIPs are failing to live up to their promises as teams struggle to take automated actions on relevant indicators across disjointed threat feeds. Industry analysts have recognized this as an issue, offering guidance that SOAR and TIPs need to converge. TIPs are merely adding complexity by aggregating intelligence sources without the real-world context or automation required to take quick, confident action. It's time for a different approach.

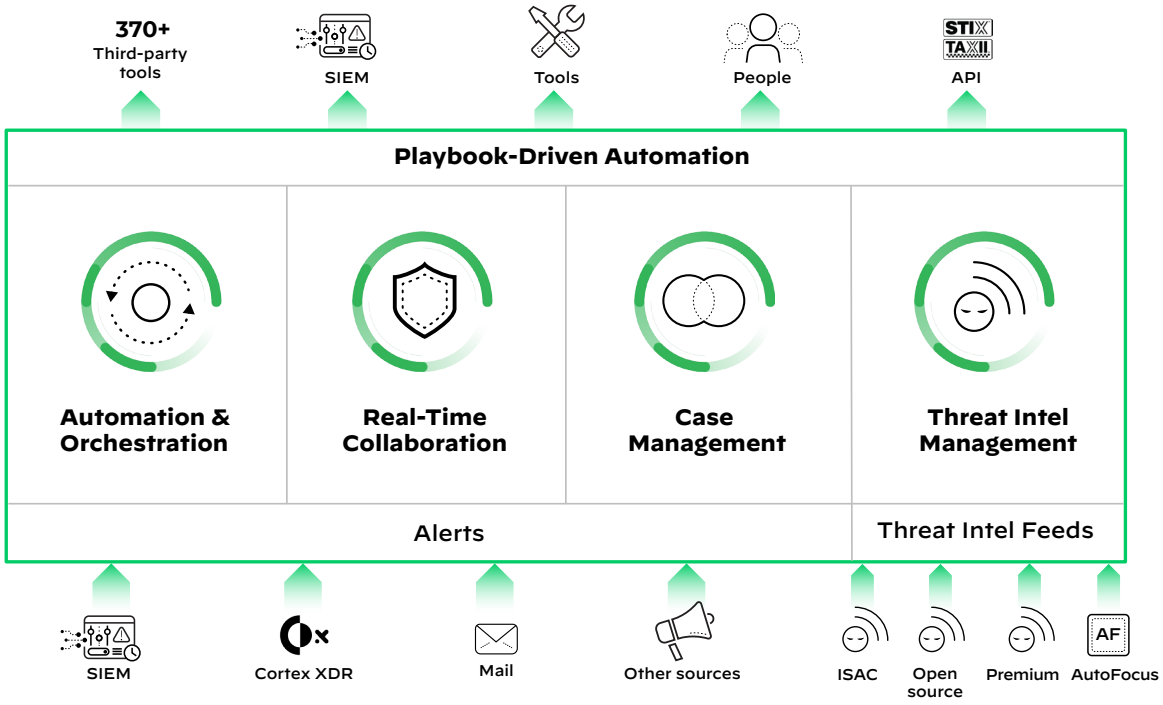

Figure 6: Cortex XSOAR playbook-driven automation

We Need an Extended SOAR Platform

Cortex® XSOAR™, with native Threat Intel Management, just makes sense. As part of the extensible Cortex XSOAR platform, Threat Intel Management defines a new approach by unifying threat intelligence aggregation, scoring, and sharing with playbook-driven automation. It empowers security leaders with instant clarity into high-priority threats to drive the right response, in the right way, across the entire enterprise.

Cortex XSOAR unifies case management, automation, real-time collaboration, and native Threat Intel Management in the industry's first extended security orchestration, automation, and response platform.

Figure 7: Benefits of Threat Intel Management

Cortex XSOAR allows you to:

- **Eliminate manual tasks** with automated playbooks to aggregate, parse, deduplicate, and manage millions of daily indicators across multiple feed sources. Extend and edit IOC scoring with ease. Find providers that have the most relevant indicators for your specific environment.
- **Reveal critical threats** by layering third-party threat intelligence with internal incidents to prioritize alerts and make smarter response decisions. Supercharge investigations with high-fidelity, built-in threat intelligence from Palo Alto Networks AutoFocus™ service. Enrich any detection, monitoring, or response tool with context from curated threat intelligence.
- **Take automated action** to immediately shut down threats across your enterprise. Expand the scope of your investigations by easily sharing threat intelligence across internal teams and trusted organizations.

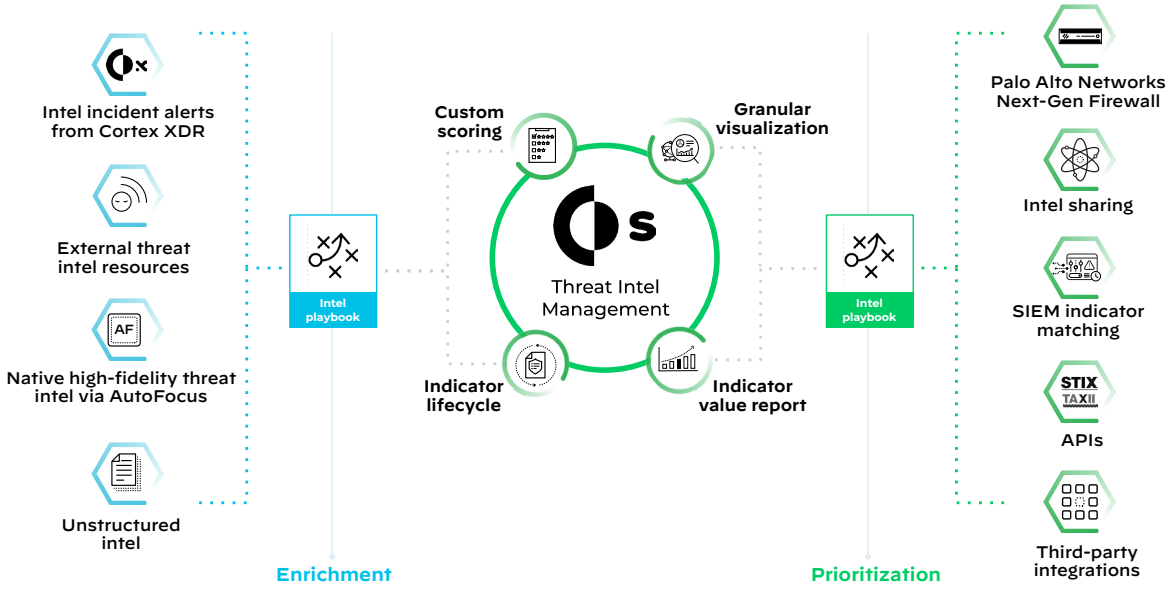

Figure 8: Threat intelligence enrichment and prioritization

Use-Case: Incident Prioritization

Security analysts deal with millions of indicators collected from hundreds of multi-sourced intelligence feeds. These indicators lack context required for analysts to make informed decisions, take action, and respond with confidence and precision. The tools at their disposal can't handle the sheer volume of indicators, and analysts end up re-prioritizing indicators to match their environment. Cortex XSOAR with native Threat Intel Management gives analysts complete control and flexibility to incorporate any business logic into their scoring. Built-in integration with more than 370 vendors allows analysts to react in real time as the indicators are consumed.

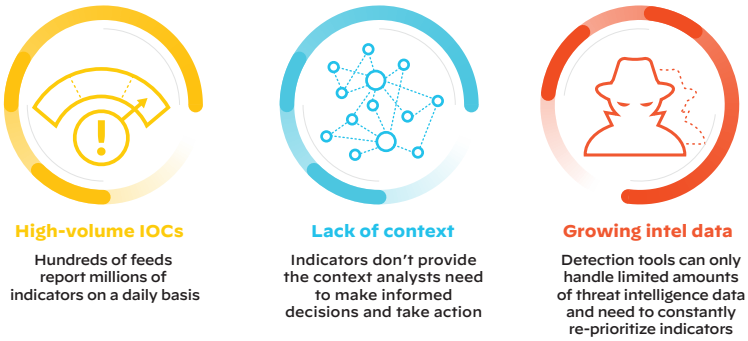

Figure 9: Challenges of disconnected intelligence tools

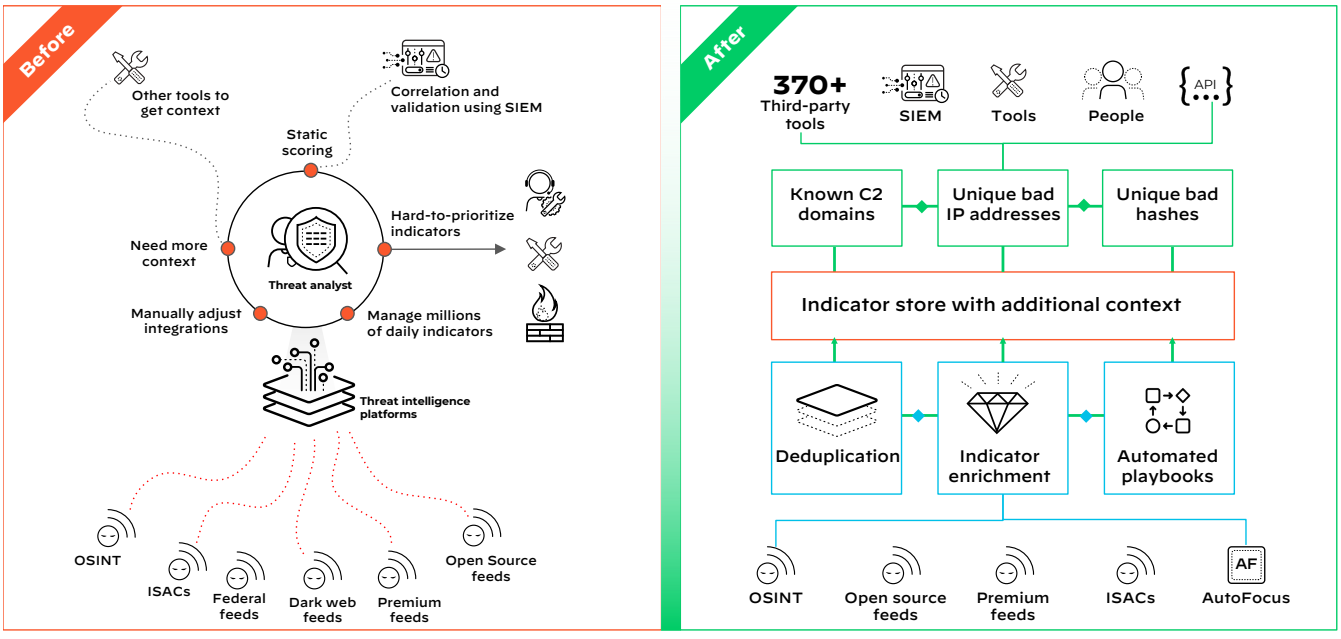

Figure 10: Intelligence management before and after Cortex XSOAR

Breadth of Cortex XSOAR Use Cases

The open and extensible Cortex XSOAR platform can be applied to a wide range of use cases—even to processes outside the purview of the SOC or security incident response team. Some of the most common use cases include phishing, security operations, incident alert handling, cloud security orchestration, vulnerability management, and threat hunting.

The future of SOAR includes native Threat Intel Management, enabling teams to break down silos between security operations and threat intelligence functions. When these are offered together in one platform, SOC analysts, incident responders, and threat intelligence teams can unify their efforts against advanced adversaries, optimizing their communication, efficiency, and access to insights.

Figure 11: Cortex XSOAR benefits across the SOC

Cortex XSOAR redefines orchestration, automation, and response with the industry's first extended SOAR platform that includes automation, orchestration, real-time collaboration, case management, and Threat Intel Management, enabling security teams to keep pace with attackers now and in the future.

Visit us online to learn more about Cortex XSOAR.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com