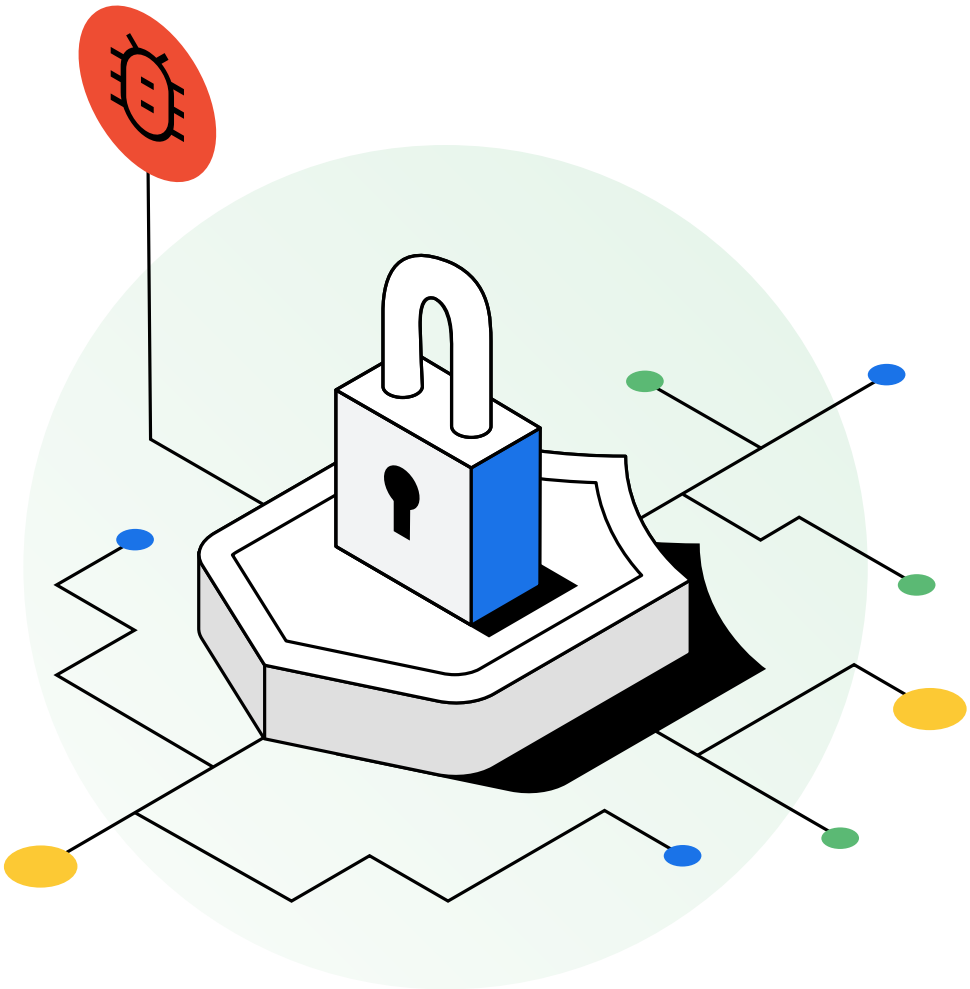
Google Cloud
Security

White paper

# Stay Ahead of the Latest Threats with Intelligence-driven Security Operations



## The Current SOC Landscape: Lots of Data, Lots of Noise, No Relief

Understanding the threat landscape and what it means for your organization is the cornerstone of establishing a modern approach to threat detection, investigation, and response (TDIR). However, achieving this dynamic, modern approach with traditional SIEMs has proven difficult. Why? Data overload—far too much information to make use of strategically within the organization—and lack of effectively applied threat intelligence.

Traditional SIEMs are also not typically thought of as outcome oriented products. They're very good at collecting data and providing a way to search that data, but ultimately require the SecOps team to connect the dots and apply what is needed in order to understand what is happening in the organization's environment.

As a result, many security teams struggle to understand which constitutes a real threat and find it difficult to determine which steps to take to respond more effectively to the ever-changing threat landscape. It also places SecOps teams in an awkward position when it's time to answer the tough questions from the C-suite and translate security risks into business risks.

This paper examines why SecOps teams struggle to effectively operationalize threat intelligence to deliver the security outcomes their organizations require. Readers will also learn how a modern, intel-driven SOC that leverages applied threat intelligence enables organizations to keep up with the changing threat landscape and reduce risk.

## Why SecOps Teams Struggle with Threat Intelligence

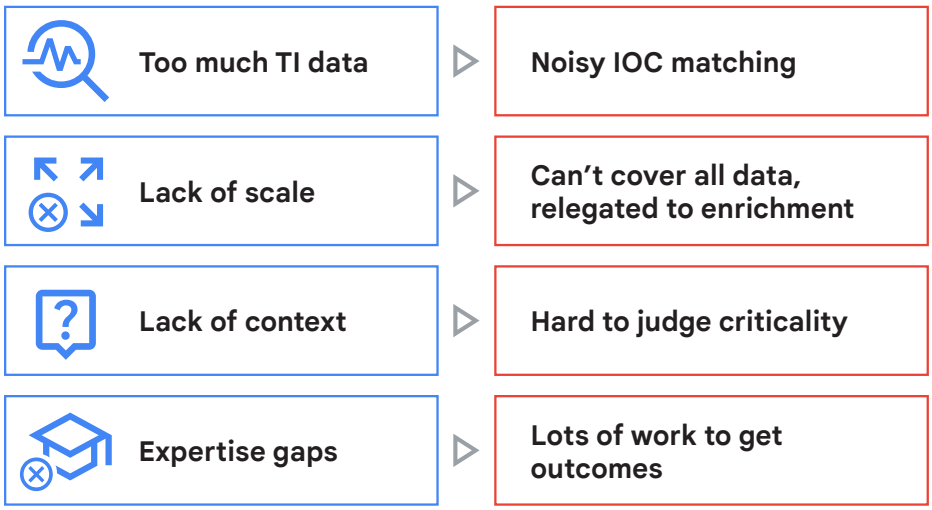
There are a few challenges when it comes to traditional threat intelligence. What most people do in practice today is try to stitch together the information that they're collecting or buying from third-party data sources with their existing SIEM. And the natural questions are "why isn't that good enough, why doesn't that work right"?  There are a few reasons why the current status quo of trying to connect the data between these two tools doesn't result in optimal outcomes.

- **Data overload.** On a regular basis teams are collecting lots of threat intelligence data and can quickly have data overload—too much information to really make any use of inside the organization. Organizations can also get high amounts of non-quality intelligence data and that tends to result in noisy IOC matches and ultimately people stop paying attention to them because they don't have the time or the expertise to be able to start sifting through it all. And unless there is a firm pulse on what's happening in the threat landscape and the know-how to apply it to the organization, this data can become stale very quickly.
- **Lack of context.** Data often lacks context, making it difficult to figure out whether it really matters inside of the organization and if it's indicative of something malicious or simply a false positive. IOCs are just a small piece of the picture and aren't able to show teams deeper information on behaviors.
- **Expertise gaps.** It's rare that an organization has its own threat intel arm, doing research and monitoring the threat landscape, particular to how it's impacting their organization. This is also hard work and it's difficult for people to do this, and at scale.
- **Lack of integration.** Threat intel is rarely integrated directly into other products, such as a SIEM, in a meaningful way.

But we can't really talk about the challenges with threat intelligence unless we talk about the SIEM as well.

**Not outcome oriented.** The SIEM is the place for aggregation and collection of event data, but traditional SIEMs are not outcome oriented products. They're really good at collecting data and providing a way to search that data, but ultimately SIEMs rely on people to connect the dots and apply context.

**Hard to scale.** SIEMs don't scale particularly well when applying intelligence data over large volumes of events—so when you have a large organization who may have trillions of events they're ingesting, there's no way that




Combining SIEM and threat intelligence—the worst of both worlds?

you can actually apply intelligence, even if it is good quality, across all the events themselves. There are also typically limits to how much data can be ingested and how quickly teams can normalize and analyze all their security telemetry.

**Manual processes.** SIEMs in general don't deliver enough turnkey value. The manual nature of processes, coupled with an ongoing talent shortage, leaves SecOps teams understaffed, overworked, and overwhelmed. And potentially missing critical threats.

## Enter Applied Threat Intelligence

The key to enabling a modern, intel-driven SOC is an end-to-end threat detection, investigation, and response workflow underpinned by threat intelligence every step of the way so that it can go beyond passively applying threat intelligence to delivering actionable outcomes based on that threat intelligence. But what do we really mean by applied threat intelligence and how does it serve as the backbone to intel-driven SecOps?

We identified the challenges with traditional threat intelligence in the previous section, now let’s take a look at what applied threat intelligence brings to the table and how it can help streamline the SOC and make TDIR more efficient.

- **Extensive understanding of the threat landscape.** If you're trying to apply threat intelligence, you first need to have the best threat intelligence in the world. As the old adage says, garbage in, garbage out. If you buy subpar intelligence you're not going to get very good results.
- **Continuous analysis of all data against the latest frontline intelligence.** You need to look at all the information that’s at your disposal. You can't take selective enrichment and have that be the way in which you're applying intelligence. Instead you need to look at all your event data, have unfiltered information, continuously apply intelligence, in real time, over those events, and you need to be able to keep that up to date. Because you don't want that intelligence to go stale or have outdated detections and indicators constantly popping up causing more work for the SecOps team down the line.
- **“Post-processing” using advanced techniques for higher fidelity.** You need to be able to have more of what we call post-processing or detection based activity on top of raw intelligence hits. This goes beyond surface indicators that will simply see malicious activity happening in the environment and let you figure out the rest. This post-processing provides prioritization detections around those indicators and that has to be part of the overall workflow.

- **New insights about threat actors are turned into behavioral detections and outcomes**. You need to stay as close as possible to the threat landscape. It's about having the quickest and most responsive intelligence and direct access to what's happening on the front lines that can be turned into behavioral detections and keeping information as fresh as possible.

By gathering and collecting intelligence through this wide angle lens and getting a deep understanding of it, it's possible to apply this intelligence in a ubiquitous and broad-based way over every single event that comes in. Think of it as "coloring in" your event data. Enriching it with intelligence, by default, for every single event that comes into the system and makes it possible to:

- Match intelligence data to real-time security telemetry data.
- Describe threat-actor motivations, tools, techniques, and tactics.
- Cover attacks relevant to the entire environment.
- Arrive early enough to detect and address threats.
- Provide immediate and clear action for triage and mitigation.

## The Payoff: Intel-Driven SOC Outcomes

Applied threat intelligence gives SecOps teams the ability to generate turnkey outcomes with little to no engineering of the system:

- Ensures every event is matched with the latest threat intel
- Aggregates all matches automatically in one single pane of glass.
- Prioritizes threats based on the unique aspects of the environment.
- Factors in the organization's internal intelligence.
- Maps to MITRE ATT&CK.

With applied threat intelligence, SecOps teams reduce the time spent on monitoring threat activities while uncovering high-level threats with more efficient threat-hunting and investigation workflows. They can also

## The 5 Pillars of the Intel-Driven SOC

**Proactive instead of reactive**—To embrace modern security realities such as rapidly changing business conditions and threats, a modern SOC needs to "look left" such as at the automated asset inventories from attack surface management tools.

**AI-augmented instead of people-dependent**—A modern SOC still relies on people but enables them to build and tune automations to scale their cybersecurity capabilities faster than the growth of the business and the evolution of threats.

**Applied threat intelligence instead of threat intel feeds**—Threat intelligence must go beyond flowing in at high speeds and be actionable to immediately integrate with detection and response tools to reduce workflow steps to the minimum.

**Threat outcomes instead of alerts and plumbing**—Threat-centric, enriched views with full context about threats and assets allow the security operations team to handle alerts faster and prevent attackers from gaining access to the environment.

**Operationally scalable instead of capacity-constrained**—By combining quality threat intelligence with AI, organizations can practically apply threat intelligence to their security operations. This includes summarizing reports, guidance, workflows, and converting natural language into query searches.

leverage high-quality insights to prioritize actionable outcomes that help piece together the story between events, alerts, assets, and users to stay ahead of the latest threats and deliver several key benefits for the organization:

> "It's about using both the humans and the machines to do the job that they're good at to assess the threat, make sure we've got the intelligence around it, and make sure that we've not been hit by it previously and we can respond going forward."

**– CISO, EMEA Insurance Company, The Business Value of Google Security Operations**

- Eliminates security blind spots.
- Ingests, analyzes, and searches security telemetry at cloud scale and speed.
- Turns applied threat intelligence into action to detect and defend against novel attacks.
- Elevates productivity as intelligence helps the SecOps team understand threat details.
- Automates detection, investigation, and response workflows.

SecOps teams also gain an extensive understanding of the threat landscape by seeing threat-actor associations related to any indicators of compromise. As they analyze data continuously against the latest frontline intelligence to quickly identify high-impact threats and leverage the full context of intelligence across threat-mitigation workflows to prioritize tasks, SecOps teams can accelerate the process of turning threat insights into behavioral detections and outcomes.

**Learn more about how Google approaches security operations or schedule a demo of Google Security Operations today to see applied threat intelligence in action.**