THREATQUOTIENT™

THREAT INTELLIGENCE PLATFORM, SIEM OR TICKETING SYSTEM: What's the Difference?

by Ryan W. Trost, Co-Founder & CTO

One of the most iconic scenes in TV history is the *I Love Lucy* skit in the chocolate factory. Lucy and Ethel can't keep up – the faster the conveyor belt, the more chocolates to wrap. This is very similar to a challenge many security professionals face – the more logs in a security information and event management (SIEM) system, the more alerts to triage. Ticketing systems have the opposite shortcoming as they are not meant to be a repository for disparate data sources to help support an intelligence-driven investigation. Given the volume of indicators published daily and the volume of log data available, funneling threat intelligence directly into your existing SIEM or ticketing system and getting the results you want is not realistic. In fact, doing so can create more noise and false positives. For more accurate and relevant insights into threats against your organization, you need to consider a threat intelligence platform (TIP).

As a relatively new technology in the cybersecurity space, it is only natural that organizations are wondering how a TIP fits into their overall security strategy and respective budget planning. Here is some helpful insight into the varying roles of SIEMs, ticketing systems and TIPs within the security infrastructure. By using each technology for its intended purpose, you'll get more value from your threat intelligence, and your SIEM and ticketing system will work more effectively and efficiently as well.

THE ROLE OF THE SIEM

SIEMs have been around for decades. They were designed to replace manual log correlation and to identify suspicious network activity by normalizing alerts across multiple technology vendors. SIEMs correlate massive amounts of data from your sensor grid (your internal security solutions, mission critical applications and IT infrastructure). Today that can exceed several terabytes per day (or even petabytes for far-reaching global enterprises), creating scalability and performance challenges when intersected with intelligence. As with every traditional technology riding the coattails of the threat intelligence buzz, SIEMs can do some limited monitoring for indicators of compromise (IOCs), but fall short as they are purely a tactical correlation engine. SIEMs also lack the necessary data retention to effectively utilize threat intelligence.

Most SIEMs only analyze and correlate one month's worth of recent activity; anything older is archived. But as we all know, attacks can slowly evolve over months. For an analyst, having that historical data is a critical component of a successful hunting mission to identify adversarial patterns and trends.

Another often overlooked shortcoming is that because SIEMs are priced by throughput (whether by number of log sources or the volume of logs), most organizations economize by only funneling "budget friendly" or critical alert logs into the SIEM. Budget friendly logs are logs that *do not* produce superfluous volumes, i.e., firewall logs (not in debug mode) or reasonable endpoint logs. This fairly common practice means threat intelligence that is funneled exclusively into the SIEM will only serve to validate or nullify an attack that has already been "detected" in alert logs.

Malicious activity occurring below the alert radar will remain undetected. Years of high-profile intrusions have proven that commercial rules and signatures don't work as well as intended, particularly when it comes to stopping advanced and emerging threats.

Finally, SIEMs are primarily a one-way consumer of information – taking logs in but not distributing critical information to the "worker bee" sensor grid. SIEMs can push data to ticketing systems to pre-populate fields, but there's no automated refining of detections based on SIEM alerts – an effort left to analysts to do manually.

SIEMs do play an important role in security beyond compliance and regulatory checkboxes, but they also have serious limitations when organizations are forcing a round peg into a square hole by trying to leverage them for threat intelligence reporting. Funneling threat intelligence directly into a SIEM isn't a viable option if you want to get the most from your external data feeds and your analysts' time and talent. Now let's take a closer look at ticketing systems and their limitations in handling threat intelligence.

THE ROLE OF THE TICKETING SYSTEM

Ticketing systems allow teams to organize, describe and archive event investigations and incidents. They focus on fact or fiction during incident response activities as analysts reverse the trail of breadcrumbs of an intrusion. There are two sizable gaps that ticketing systems have with respect to successfully supporting a threat intelligence program. First, most ticketing systems were built to support system administration efforts including password resets, request access to a certain website, even moving offices across the hall, etc. Whereas complex cyber-driven investigations require certain data fields and workflows for capturing, learning and sharing of knowledge as investigations unfold.

Second, ticketing systems are currently unable to communicate "out-of-the-box" with numerous sensor grid blocking or detection technologies to deploy intelligence to strengthen defenses. This limitation is due to the fact that ticketing systems historically rely on either manual entry or pulling information from the SIEM, where the alerts are being correlated and triaged. They aren't designed to relay policy changes out to the firewalls, web-proxies, endpoints, etc. This is a core capability as teams weed through the noise of blacklists and "aged" sharing efforts to find the most relevant threats against their organization.

THE ROLE OF THE THREAT INTELLIGENCE PLATFORM

In contrast to SIEMs and ticketing systems, TIPs are purpose-built for threat intelligence. There are several TIP offerings on the market with various differences, but they share some common baseline capabilities.

At the bare minimum, a TIP aggregates, structures and allows companies to better utilize threat intelligence with the ability to handle millions of IOCs, conduct both cyber and non-cyber event analysis and engage in adversary profiling.

Some TIPs also allow organizations to engage in the level of teamwork and collaboration required to identify which IOCs are relevant to the organization and hone in on advanced threats. For example, IT security and incident response (IR) professionals may have the capability to comment on indicators; build adversary tactics, techniques and procedures (TTP) profiles; and overlay selected "events" over a longer period of time to look for and identify patterns.

Streamlining how your analysts and tools work together, TIPs are ideally suited to trigger the team's internal intelligence workflow and finish that workflow with a feedback loop. By funneling threat intelligence into a TIP and then allowing the TIP to distribute the information to multiple systems within your environment, you can enhance your threat intelligence as well as proactively and automatically improve security posture.

WORKING TOGETHER THROUGH BIDIRECTIONAL INTERCONNECTIVITY

TIPs that support bidirectional integration with SIEMs and ticketing systems empower organizations to derive more value from their existing security investments.

For example, TIPs complement SIEMs, allowing security teams to overcome the limitations of a SIEM by enhancing a tactical strategy with a more strategic adversary focus. When intelligence is first aggregated within the TIP, it can be augmented

with context and prioritized for relevance *before* being fed into the SIEM. Enriching the alerts inside the SIEM with additional context (e.g., malware family, kill chain stage, IR ticket number, score, etc.) allows teams to write more mature SIEM rules to filter out noise and focus on higher priority events. A TIP also enables faster blocking and detection by automatically updating the sensor grid hourly based on the latest threat intelligence.

TIPs can also query ticketing systems with newly created indicators to enrich threat data with greater context. For example, understanding whether or not that indicator has been seen before and, if so, the steps taken by the previous analyst to triage the alert can help jumpstart an investigation.

Both SIEMs and ticketing systems can play a key role in the threat intelligence lifecycle by feeding data and indicator-rich tickets back into the TIP, thus making valuable contributions to the threat intelligence lifecycle. Organizations can understand which sources of intelligence provide higher fidelity alerts for detecting and preventing future incidents.

Just like Lucy and Ethel couldn't keep up with the volume of chocolates coming down the conveyor belt, your SIEM and ticketing system can't keep up with the volume of intelligence available today while staying true to their intended roles. By pushing intelligence into a TIP and then working in concert with your SIEM and ticketing system, you can maximize the value of external feeds, enhance your overall threat intelligence and increase the effectiveness of your detection systems and teams to stop threats faster.

QUICK REFERENCE

THE SIEM

WHAT IT DOES

SIEMs correlate massive amounts of data daily with limited IOC monitoring.

SHORTCOMINGS

- Lacks the data retention necessary to show threat patterns over an extensive amount of time
- Imports only "budget-friendly" logs
- Lacks the bidirectional data flow (re-ingestion of investigation outcome) to maximize future correlation effectiveness to the sensor grid

THE TICKETING SYSTEM

WHAT IT DOES

Ticketing systems allow teams to organize, describe and archive event investigations and incidents.

SHORTCOMINGS

- Inability for out-of-the-box communication with numerous sensor grid technologies to re-deploy valid intelligence to strengthen defenses
- Lacks the "bigger picture" capability to incorporate data feeds, industry/community collaboration and tool orchestration

THE TIP

WHAT IT DOES

A TIP allows companies to better utilize threat intelligence with the ability to handle millions of IOCs, timeline and trend analysis for both cyber and non-cyber event analysis, and adversary profiling.

BENEFITS

- Streamlines workflows to ensure your analysts and tools work uniformly
- Allows you to write more mature SIEM correlation rules to filter out commodity noise
- Enables faster detection and blocking by automatically updating the sensor grid based on the latest and more relevant threat intelligence

ABOUT THE AUTHOR

As CTO and co-founder of ThreatQuotient, Ryan Trost utilizes his 15+ years of security experience focusing on intrusion detection and cyber intelligence to help drive thought leadership as well as innovative product discussion. As a recognized leader in the cyber industry, Ryan frequently speaks at industry conferences, including BlackHat, DEFCON, SANS, HTCIA (High Technology Crime Investigation Association) and FIRST. Ryan is the author of Practical Intrusion Analysis and has also developed one of the first geospatial intrusion detection algorithms used to identify geolocation attack patterns. Prior to ThreatQuotient, Ryan managed several USG and Commercial Security Operations Centers (SOCs) and was the Sr. Director of Security and Privacy Officer for a medium-size healthcare company in Northern Virginia. Ryan also serves as Chairman of the Advisory Board for the Northern Virginia Community College cyber degree program.

ABOUT THREATQUOTIENT™

ThreatQuotient™ understands that the foundation of intelligence-driven security is people. The company's open and extensible threat intelligence platform, ThreatQ™, and cybersecurity situation room solution, ThreatQ Investigations, empower security teams with the context, customization and prioritization needed to make better decisions, accelerate detection and response, and advance team collaboration. Leading global companies use ThreatQuotient solutions as the cornerstone of their security operations and threat management system.

For additional information, please visit threatq.com.

TQ_TIP-vs-SIEM-vs-Ticketing-US_Rev1