DARKREADING

NOVEMBER 2023

Sponsored by

Google Cloud

Key Elements Enterprises Need to Include in Modern SecOps

Security teams are overwhelmed in the operations center. What will it take to unlock effective threat detection and master data collection and response for modern defense?

INSIDE:

Key Elements Enterprises Need to Include in Modern SecOps »

Most Enterprise SEIMS Blind to MITRE ATT&CK Tactics »

How AI-Augmented Threat Intelligence Solves Security Shortfalls »

Don't Overlook Social Media's Threat Intel for Enterprise Cybersecurity »

Google Cloud Perspectives: AI Is Moving the Needle in Addressing Top Security Challenges »

Brought to you by

informa tech

Next

FEATURE

Key Elements Enterprises Need to Include in Modern SecOps

Security teams are overwhelmed in the operations center. What will it take to unlock effective threat detection and master data collection and response for modern defense?

By Evan Schuman, Contributing Writer, Dark Reading

The security operations center (SOC) is the enterprise's first line of defense against an active attack. It is the brain of all security operations, with a team that sifts through threat intelligence, events data, logs, and activity reports from throughout the enterprise and key partners around the world. And, yet, the SOC is as underfunded and understaffed as any other area in security. SOC staff members typically work with antiquated tools, wrangle outdated data, and grapple with massive blockages to the information and systems they need to do their jobs.

Today's enterprise SOC environments are both massively distributed and highly localized. An enterprise often has more than a dozen authorized global cloud providers — on top of an untold number of shadow IT cloud deployments. Some of these clouds are designed to work with others, but many are not. Then there are the issues related to IoT, remote offices, and third-party systems.

How can CISOs realistically give SOCs the tools needed to effectively manage all of that?

Overwhelmed by Data and Noise

It all starts — or doesn't — with access. Many enterprise SOCs have insufficient access to their own employer's NAT IP addresses and — critically — its many cloud environments. Visibility requires not only credentials and internal URLs, but also the names of all relevant personnel on file with the cloud provider, which would need to be notified in the event of an active attack.

"The oceans of data have become a tidal wave leaving SOCs drowning in mostly useless data and noise. For some reason, we as a security community continue to enable the notion that collecting 'all the data' will prevent attacks, but that has proven to be false time and time again," says Tyler Young, CISO at security data vendor BigID. "The assumption that we can simply plug data into our SIEM to overlay known threat data and our internal telemetry and magically find threat actors in our environment is just wrong." Indeed, much of the data currently gathered by SOCs is useless by the time it reaches stakeholders, Young says. One reason is that private sector organizations often hesitate to share details about incidents. Another challenge is that a dearth of context and details around incidents makes it more difficult for SOC staffers to make use of the information they do have.

Threat Intel Must Be Actionable

Brian Bell, the global head of cybersecurity and risk services at consulting firm Wipro, says that what many vendors — and quite a few enterprise SOC teams — consider to be threat intelligence actually is not. What people sometimes forget, he says, is that threat intelligence needs to be actionable and usable.

"Threat intelligence is a term that sees a lot of abuse in the industry," Bell says. "The threat feeds you receive, whether paid or open source, are not intelligence; they are information at best and usually just data — never intelligence." Bell notes that a threat feed that consists of a list of bad IPs or domains with no context is simply data. Without proper curation, such a list is difficult to use effectively. "Information is much more useful than data but is still not intelligence," he says.

A threat feed that provides a minimum of context — as in, "This IP is associated with Dridex" — is on the border between data and information, Bell says. A threat feed that gives a list of bad IPs, along with the exact observed activity — as in "Dridex C2 communication on port 8043" — and the time the activity was observed has applied sufficient context to the data to produce information.

"Threat intelligence will be produced internally — not by reading blogs and repackaging the information but by applying a critical eye to what the security operations center and the incident response team are seeing in the wild," Bell adds. "What is currently actively targeting my organization? What context can I apply to this data? What intention can I direct it with?"

> **"Threat intelligence will be produced internally — not by reading blogs and repackaging the information but by applying a critical eye to what the security operations center and the incident response team are seeing in the wild." —Brian Bell, Wipro**

What Is the SOC's Material Business Impact?

Connected assets are the lifeblood of businesses, but it's often unclear how each asset is being used, says Curtis Simpson, CISO of asset intelligence platform vendor Armis. "The individual tools in the security stack are unclear of how each asset registering malicious or suspicious activity relates to the business. This limits the ability to effectively establish severity based on business impact and, in turn, leads to the prioritization of alerts based on only very limited technical context," he says.

When each tool has been configured to over-alert so that nothing is missed, and prioritization is based on limited technical context, the SOC is faced with an overwhelming list of conflicting priorities. The recommended approach to modernizing and optimizing the SOC focuses on asset intelligence. The first and most foundational step is to adopt a modern continuous asset discovery, identification,

and intelligence platform that augments or replaces existing asset discovery and inventory software. This enables organizations to move from static, incomplete configuration management database (CMDB) data with limited contextual value to continuously consumable asset intelligence that guides prioritization.

Simpson suggests that this approach not only benefits the enterprise more effectively but also positions the SOC as essential and strategic.

“At the highest level, SOCs should position the intelligence platform between the rest of the security stack and the SIEM/SOAR [security information and event management/security orchestration, automation, and response] to validate and triage every incident for suppression or response,” Simpson says. At the same time, he acknowledges, many teams face resource constraints. “The team is already overwhelmed and undertaking optimization projects to address long-term challenges and position the SOC for the future when simply attempting to keep their head above water can make it challenging to even get started, let alone continuously optimize.”

Making Complexity Simple

There are some who argue that the very nature of the SOC, along with how most enterprises leverage SOCs, is flawed and needs to be significantly reworked. Complexity is one of the biggest challenges facing the SOC, says Steve Winterfeld, the advisory CISO at Akamai.

“When I became a CISO, I didn’t realize how much time would be consumed with vendor management,” Winterfeld says. “But having a large number of security capabilities can lead to multiple issues. You have one engineer trying to maintain and optimize multiple systems, so none of them are up to date. Next, you have one analyst trying to respond to feeds from multiple systems and, in some cases, multiple dashboards. This leads to missed alerts that could have prevented an incident from becoming a major crisis.”

> **“When that orphan tool comes up for renewal, you need to ask yourself, ‘Is there a chance here for me to move to a single vendor that is perhaps an improvement for integration?’ Treat every renewal as an opportunity to reduce the complexity.” —Steve Winterfeld, Akamai**

The global attack surface has gotten exponentially more complex in the last few years. The attack surface is compounded by remote workers, customer access capabilities, growth of apps and APIs, the move to hybrid cloud infrastructure, BYOD, and SaaS, leaving security teams with multiple environments to protect, Winterfeld says. The clouds themselves are so large and numerous that they thwart efficient and cost-effective management. “Today, I am paying more to monitor my cloud infrastructure than I am paying for the cloud infrastructure,” says Ken Westin, field CISO at Panther Labs, pointing to the need to have salaried specialists for each cloud platform. “When the cloud platforms make a change to their APIs or their log format, all of the data pipelines and detections break as a result.”

Take a Zero-Budget Approach

Winterfeld suggests that CISOs take a zero-budget approach to SOC security tools. For example, consider whether SOC operations will be affected if the vendor of a tool is acquired.

“It’s all part of our third-party risk analysis,” he says. “When that orphan tool comes up for renewal, you need to ask yourself, ‘Is there a chance here for me to move to a single vendor that is perhaps an improvement for integration?’ Treat every renewal as an opportunity to reduce the complexity.”

As with other enterprise technology tools, SOC tools originate from many different places. For example, some tools may have been purchased directly a decade ago, while others may have ended up in the SOC via a company acquisition or when a team member downloaded software in shadow IT mode. Then there are the tools used by various cloud platforms that have become part of the SOC tool collection.

Having More Tools Is Never Better

Westin says an accumulation of tools can become a waste of license fees. Worse, he adds, in a SOC environment, security tools can fight each other, resulting in missed information, duplicate information, or a slew of false positives or false negatives as tools react to other tools with which they were not designed to interact

There are many tweaks and small fixes that can be put into place to improve enterprise SOCs, but fundamental and long-lasting improvements require addressing a problem that drives personnel shortages and the use of outdated and ineffective tools: budget.

In addition, many organizations are using tools designed for network architectures and threats that are at least a decade old. And enterprises are paying a lot of money for tools that can't handle an exponential increase in data volume, let alone keep up with newer threats targeting identity and cloud environments. For example, a SIEM that was designed for on-premises environments and legacy data centers requires major retooling and configuration to handle today's cloud workloads.

Organizations should focus on leveraging cheaper cloud-native options instead of trying to salvage expensive tools, and they should focus on outcomes, not the tools themselves.

John Gunn, CEO of wearable biometric authentication firm Token, laments the accuracy problems associated with the vast amounts of data in the typical enterprise SOC today. Of the countless petabytes and sometimes exabytes of log data that is being stored, he says, the vast majority has zero value. Further, he adds, nothing of use will be gained through a more granular view of the data, which becomes less valuable with each passing moment. Logs are great for forensics, but time and money being spent on storing logs should be reprioritized and spent on analytics that would be far more effective, such as robust authentication, Gunn says.

"People are underestimating how dynamic attack mechanisms have become, especially with the integration of AI into attack methods," he adds.

SOC as a Value-Added Driver

Automation will prove essential to SOC operations and efficiencies, but only if deployed strategically, says Rob Boyce, global cyber resilience lead at consulting firm Accenture. Many organizations instead take an intelligence feed or a list of indicators of compromise (IoCs) and then try to automate the process of working with the data.

Boyce cites as an example the Log4j vulnerability. Log4j

was initially disclosed in December 2021, but it took many organizations months to find and patch affected systems because they didn't know which systems in their environment were affected.

"I think there's a huge way for automation to play a big role there to be able to fast-track the assessment of intelligence and the applicability of that intelligence within an environment," Boyce says.

Another key element with SOCs is active attack defense strategies and the role that triage should or should not play.

One school of thought is that SOCs have very limited resources, so the most valuable assets and the access points most likely to be attacked get the bulk of budget and attention.

Another school of thought suggests that professional attackers — regardless of whether they are state actors, identity thieves, ransomware extortionists, or cyber saboteurs intent on harming operations — are, by nature, contrarian. They prefer to gain access via low-priority paths that have minimal protections. Rather than directly attacking a high-value asset such as payroll records, these attackers try to gain access via a low-level asset — for example, a smart printer with its own IP address — and then quietly and slowly escalate privileges and move through the system to get to a higher-value target. For those who embrace this school of thought, identifying a path as low risk is painting a target on its back for cyberthieves.

Taking the Threat out of Threat Intel

There are many tweaks and small fixes that can be put into place to improve enterprise SOCs, but fundamental and long-lasting improvements require addressing a problem that drives personnel shortages and the use of outdated and ineffective tools: budget.

The best way to start the process, according to Accenture's Boyce, is to grab the CEO's and CFO's attention. How? Focus on business intelligence instead of threat intelligence. In other words, Boyce suggests, demonstrate to the leaders in charge of non-security lines of business how the SOC can help maintain or increase revenue. If you can do this, the CEO and CFO will be much more likely to invest more into security.

"Today, they are not showing senior management how the SOC is enabling the enterprise. No one is being shown the strategic value of the SOC in a way that informs business decisions. That is a huge opportunity," Boyce says.

For example, in the first hours after Russia attacked Ukraine in February 2022, management executives at a large multinational corporation were ordered to report to the board any likely impacts on the enterprise from the war.

The CEO believed there wasn't any meaningful direct exposure because the company did not have employees or major customers in Ukraine. However, the SOC staff carefully reviewed logs and discovered that several key partners conducted extensive data transfers with Ukraine. SOC staff prepared a report indicating that the war might cause problems with those partners, which could, in theory, impact the enterprise's operations.

"[SOC staff] moved from threat intelligence to just intelligence. In doing so, they showed the SOC to be a value-added driver," Boyce says. "Many organizations did not understand fully if they had third parties that may have operations within Ukraine. You can use AI and GenAI capabilities to scrape through even publicly available information about your third parties and find out if they did or did not have operations within Ukraine to be able to ensure that you're making appropriate contingency strategies."

The SOC's ROI

Perhaps the most popular SOC improvement advice involves contextualizing vulnerability data and prioritizing patching and remediation.

For Fred Rica, partner, advisory, for accounting firm BPM, that contextualization is where he encourages enterprise CISOs to start their SOC strategy thinking.

"There are more alerts than ever, point products litter the environment, thousands of vulnerabilities are disclosed yearly, systems produce conflicting data, and analysts can only see what the tools produce. So, what happens is qualitative arguments win over quantitative, the loudest voice tends to win, and, as a result, the outcomes aren't always those desired," Rica says.

Britive CEO Art Poghosyan fears that many enterprise CISOs have not sufficiently adapted their processes to factor in today's threat landscape. "CISOs are not seeing the opportunity to understand the new ways that the environment is getting exposed," he says.

Poghosyan describes an organization where developers created a new polling API that pushes updates submitted by clients via a Web app to a new database. Unfortunately, the security or cloud operations team have no knowledge of this API or the newly created database. Sometime later, the person behind the account is compromised by a threat actor. Security and cloud operations teams won't see the intrusion initially because they are not aware of the new database or API. Far worse, the account used to access it looks normal because there is no way on the surface to know the account is bad because it was set up initially for a legit purpose.

Poghosyan's suggested fix is to leverage just-in-time access. "With a JIT cloud access management tool in place, the developers could have set up access profiles for the account that stood up these cloud-based resources. It could detect the unusual queries to the database by a developer account that was provisioned to a contractor but from an IP address range outside of the corporate network."

None of these suggestions will — on their own — convert SOCs into the security saviors that enterprise CISOs need them to be. However, they are a start.

SOCs need to be given access to everything in their global environments, and that means that the SOC must overcome the objections of other line-of-business executives. The SOC will remain the enterprise's first line of defense against attacks. The question enterprises must properly answer is whether the SOC team will be given what it needs to do its job.

About the Author: Evan Schuman has tracked cybersecurity issues for enterprise B2B audiences for far longer than he will admit. His byline has appeared in The New York Times, Associated Press, Reuters, SCMagazine/SCMedia, VentureBeat, TechCrunch, eWEEK, Computerworld, and other technology titles. He has also repeatedly guest lectured on cybersecurity issues for graduate classes at Columbia University and New York University.

Most Enterprise SIEMs Blind to MITRE ATT&CK Tactics

Organizations are largely deluded about their own security postures, according to an analysis, with the average SIEM failing to detect a whopping 76% of attacker TTPs.

By Elizabeth Montalbano, Contributor, Dark Reading

Despite enterprises' best efforts to shore up their security information and event management (SIEM) postures, most platform implementations have massive gaps in coverage, including missing more than three-quarters of the common techniques that threat actors use to use to deploy ransomware, steal sensitive data, and execute other cyberattacks.

Researchers from CardinalOps analyzed data from production SIEM platforms from companies such as Splunk, Microsoft Sentinel, IBM QRadar, and Sumo Logic, and found that they have detections for just 24% of all MITRE ATT&CK techniques. That means that adversaries can execute about 150 different techniques that can bypass SIEM detection, while only about 50 techniques are spotted, according to the researchers.

This is despite the fact that current SIEM systems actually do take in sufficient data to cover potentially 94% of all these techniques, CardinalOps notes as part of the company's "Third Annual Report on the State of SIEM Detection Risk."

Moreover, organizations are largely deluded about their own security postures and "are often unaware of the gap between the theoretical security they assume they have and the actual security they have in practice," according to the report. This creates "a false impression of their detection posture."

MITRE ATT&CK is a global knowledge base of adversary tactics and techniques based on real-world observations that's aimed at helping organizations detect and mitigate cyberattacks. The report's data is the result of analysis of more than 4,000 detection rules, nearly 1 million log sources, and hundreds of unique log source types used in SIEM across a range of diverse industry verticals — including banking and financial services, insurance, manufacturing, energy, and media and telecommunications.

A Lack of SIEM Fine-Tuning to Blame for Detection Fails

The key issue contributing to the current state of SIEM efficacy (or lack thereof) seems to be that even though resources exist for organizations to use knowledge, automation, and other processes to detect adversaries and potential attacks on their environments, they still largely rely on manual and other "error-prone" processes for developing new detections, the researchers noted. This makes it difficult to reduce their backlogs and act quickly to fill gaps in detection.

Indeed, SIEMs themselves "are not magic" and rely on the organizations deploying them to do so correctly and efficiently, says Mike Parkin, senior technical engineer at Vulcan Cyber, a security-as-a-service provider of enterprise cyber-risk remediation.

"Like most tools, they require fine-tuning to deliver the best results for the environment they're deployed in," he says. "These report results imply that many organizations have gotten the basics working but haven't done the fine-tuning necessary to take their detection, response, and risk management strategies to the next level."

In addition to the need to scale detection-engineering processes to develop more detections faster, one key issue that seems to be tripping up detection in enterprise SIEM deployments is that, on average, they have 12% of rules that are broken, which means they will never file an alert when something is amiss, according to the report.

"This commonly occurs due to ongoing changes in the IT infrastructure, vendor log format changes, and logical or accidental errors in writing a rule," the researchers noted in the report. "Adversaries can exploit gaps created by broken detections to successfully breach organizations."

Why MITRE ATT&CK Matters

MITRE ATT&CK, created in 2013, has now "become the standard framework for understanding adversary playbooks and behavior," the researchers noted. And as threat intelligence has advanced, so has the wealth of knowledge the framework provides, currently describing more than 500 techniques and subtechniques used by threat groups such as APT28, the Lazarus Group, FIN7, and Lapsus$.

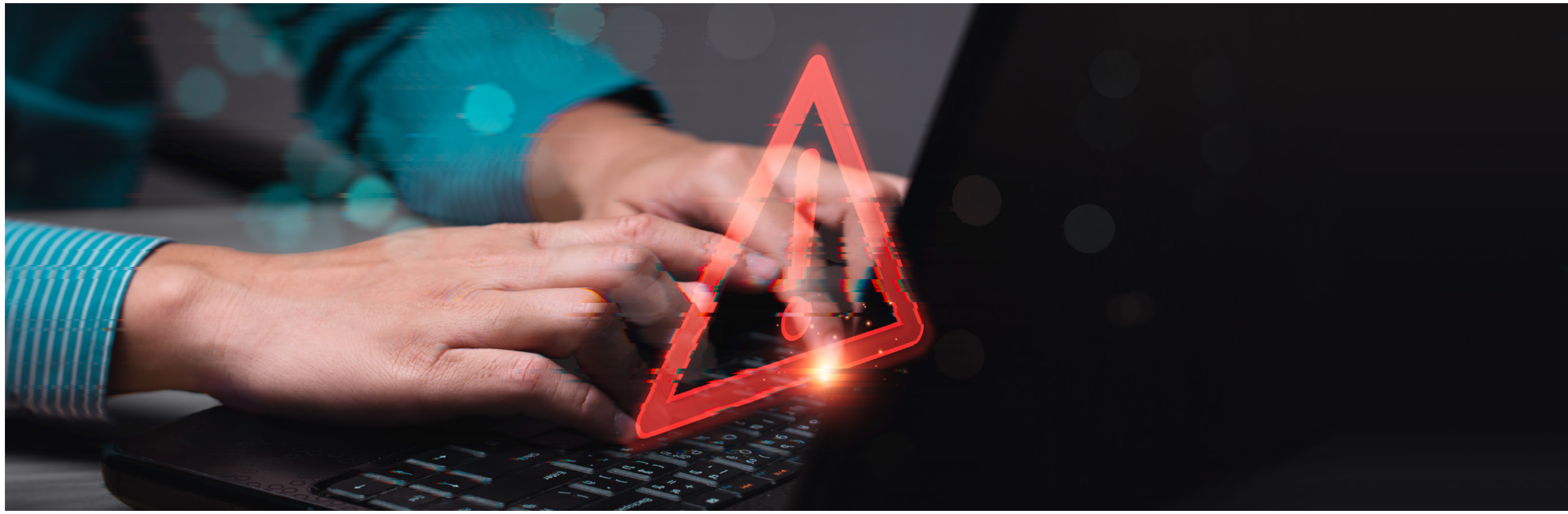
"The biggest innovation introduced by MITRE ATT&CK is that it extends the traditional intrusion kill chain model to go beyond static indicators of compromise (like IP addresses, which attackers can change constantly) to catalog all known

Previous Next

adversary playbooks and behaviors (TTPs)," according to the CardinalOps researchers.

Organizations clearly see the value in using MITRE ATT&CK to help them in their security efforts, with 89% currently using the knowledge base to reduce risk for security-operations use cases — such as determining priorities for detection engineering, applying threat intelligence to alert triage, and gaining a better understanding of adversary TTPs, the researchers noted, citing Enterprise Strategy Group (ESG) research.

However, using the framework to support SIEM efforts and using it well appear to be two very different scenarios, according to the report.



Closing the SIEM Gap

There are steps that organizations can take to help close the gap between what a SIEM is capable of in terms of cyberattack detection and how they currently are using it, researchers and security experts said.

One key strategy would be to scale SIEM detection-engineering processes to develop more detections faster using automation, something that companies already use widely to great effect in "multiple areas of the SOC, such as anomaly detection and incident response," but not so much in detection, they noted in the report.

"The detection-engineering function remains stubbornly manual and typically dependent on 'ninjas' with specialized expertise," the researchers wrote.

Indeed, having a focus on automation is critical to achieving goals with limited human and financial resources, agrees one security expert.

"This includes expanding automated detection to include Internet of things (IoT) and operational technology (OT) attack vectors, as well as having plans already in place for automated threat remediation," says John Gallagher, vice president of Viakoo Labs at Viakoo.

One key challenge that organizations continue to face is that the current attack surface — which now includes large numbers of vulnerable network-connected devices as well as the typical enterprise network — has grown well past what the IT organization is currently capable of supporting or managing, Gallagher says.

"To defend and maintain the integrity of those assets requires IT working closely with other parts of the organization to ensure those assets are visible, operational, and secure," he says.

Indeed, Parkin observes, until organizations can get a clear picture of their threat surfaces, manage their risk, and prioritize events to focus on what matters most, there will be problems.

"We have the tools to make it happen," he says, "but it can be a challenge to get them deployed and configured for best effect."

About the Author: Elizabeth Montalbano is a freelance writer, journalist, and therapeutic writing mentor with more than 25 years of professional experience. Her areas of expertise include technology, business, and culture.

Previous Next

ANALYSIS

How AI-Augmented Threat Intelligence Solves Security Shortfalls

Researchers explore how overburdened cyber analysts can improve their threat intelligence jobs by using ChatGPT-like large language models (LLMs).

By Robert Lemos, Contributing Writer, Dark Reading

Security-operations and threat-intelligence teams are chronically short-staffed, overwhelmed with data, and dealing with competing demands — all issues that large-language-model (LLM) systems can help remedy. But a lack of experience with the systems is holding back many companies from adopting the technology.

"What we're aiming for is helping organizations navigate the uncertainty, because there aren't a lot of either success stories or failure stories yet," John Miller, head of Mandiant's intelligence analysis group. "There aren't really answers yet that are based on routinely available experience, and we want to provide a framework for thinking about how to best look forward to those types of questions about the impact."

Organizations that implement LLMs will be able to better synthesize intelligence from raw data and deepen their threat-intelligence capabilities, but such programs need support from security leadership to be focused correctly. Teams should implement LLMs for solvable problems, but before they can do that they need to evaluate the utility of LLMs in an organization's environment, says Miller.

"What we're aiming for is helping organizations navigate the uncertainty because there aren't a lot of either success stories or failure stories yet," Miller says. "There aren't really answers yet that are based on routinely available experience, and we want to provide a

framework for thinking about how to best look forward to those types of questions about the impact."

In a presentation at Black Hat USA 2023, entitled "What Does an LLM-Powered Threat Intelligence Program Look Like?," Miller and Ron Graf, a data scientist on the intelligence-analytics team at Mandiant's Google Cloud, demonstrated the areas in which LLMs can augment security workers to speed up and deepen cybersecurity analysis.

Three Ingredients of Threat Intelligence

Security professionals who want to create a strong threat intelligence capability for their organization need three components to successfully create an internal threat intelligence function, Miller tells Dark Reading. They need data about the threats that are relevant; the capability to process and standardize that data so that it's useful; and the ability to interpret how that data relates to security concerns.

That's easier said than done because threat intelligence teams — or individuals in charge of threat intelligence — are often overwhelmed with data or requests from stakeholders. However, LLMs can help bridge the gap, allowing other groups in the organization to request data with natural language queries and get the information in non-technical language, he says. Common questions include trends in specific areas of threats, such as ransomware, or when companies want to know about threats in specific markets.

"Leaders who succeed in augmenting their threat intelligence with LLM-driven capabilities can basically plan for a higher return on investment from their threat intelligence function," Miller says. "What a leader can expect as they're thinking forward, and what their current intelligence function can do, is create higher capability with the same resourcing to be able to answer those questions."

AI Cannot Replace Human Analysts

Organizations that embrace LLMs and AI-augmented threat intelligence will have an improved ability to transform and make use of enterprise security datasets that otherwise would go untapped. Yet, there are pitfalls. Relying on LLMs to produce coherent threat analysis can save time, but can also, for instance, lead to potential "hallucinations" — a shortcoming of LLMs where the system will create connections where there are none or fabricate answers entirely, thanks to being trained on

incorrect or missing data.

"If you're relying on the output of a model to make a decision about the security of your business, then you want to be able to confirm that someone has looked at it, with the ability to recognize if there are any fundamental errors," Miller says. "You need to be able to make sure that you've got experts who are qualified, who can speak for the utility of the insight in answering those questions or making those decisions."

Such issues are not insurmountable, says Google Cloud's Graf. Organizations could have competing models chained together to essentially do integrity checks and reduce the rate of hallucinations. In addition, asking questions in optimized ways — so called "prompt engineering" — can lead to better answers, or at least ones that are the most in tune with reality.

Keeping an AI paired with a human, however, is the best way, Graf says.

"It's our opinion that the best approach is just to include humans in the loop," he says. "And that's going to yield downstream performance improvements anyways, so the organizations are still reaping the benefits."

This augmentation approach has been gaining traction, as cybersecurity firms have joined other companies in exploring ways to transform their core capabilities with large LLMs. In March, for example, Microsoft launched Security Copilot to help cybersecurity teams investigate breaches and hunt for threats. And in April, threat intelligence firm Recorded Future debuted an LLM-enhanced capability, finding that the system's ability to turn vast data or deep searching into a simple two- or three-sentence summary report for the analyst has saved a significant amount of time for its security professionals.

"Fundamentally, threat intelligence, I think, is a 'big data' problem, and you need to have extensive visibility into all levels of the attack, into the attacker, into the infrastructure, and into the people they target," says Jamie Zajac, vice president of product at Recorded Future, who adds that AI allows humans to simply be more effective in that environment. "Once you have all this data, you have the problem of how do you actually synthesize this into something useful, and we found that using our intelligence and using large language models … started to save [our analysts] hours and hours of time."

About the Author: Rob Lemos is a veteran technology journalist of more than 20 years and a former research engineer. He has written for more than two dozen publications, including CNET News.com, Dark Reading, MIT's Technology Review, Popular Science, and Wired News.

ANALYSIS

Don’t Overlook Social Media’s Threat Intel for Enterprise Cybersecurity

Social media data can provide critical clues to help get ahead of the next cyberattack, experts say.

By Becky Bracken, Editor, Dark Reading

Tagged, organized, and free for anyone who wants it, social media posts and data are an underused threat intelligence resource for many enterprise cybersecurity teams.

Just as cybercriminals have found social media platforms useful for gathering information on targets and launching attacks, network defenders should likewise be looking at X (formerly Twitter) and other similar public-facing social media data sources — so called open source intelligence (OSINT) — to help inform cyber defenses, according to experts.

”Social media and other digital platforms are invaluable resources for gathering intelligence on external cyber threats because it is often one of the earliest indicators of trouble brewing,” AJ Nash, vice president of Intelligence at ZeroFox, explains to Dark Reading. “Waiting until a threat materializes to the point where it sets off an alert in your SOC might mean it's too late to stop it — a truly proactive security posture includes leveraging data from digital platforms to stay ahead of these threats.”

Igal Iytzki, of Perception Point, uses X and Reddit to share threat intelligence and advises cybersecurity teams to utilize social media as part of their overall strategy.

“There is a lot of threat intelligence being posted on public platforms every day that businesses can tap into,” Iytzki explains to Dark Reading. “The infosec community has created an environment where we share our findings openly and freely, understanding the benefits this can have for the community at large, while also taking care to protect valuable data.”

Gathering Social Media Threat Intel

One way to make social media data useable, as well as accessible, is to ensure posts are tagged and easily searchable, he adds.

“If you search for a particular IP, domain, malware, exploit, or CVE in the search bar on a social platform, you can easily find related tags or tweets about a particular attack or trend," Iytzki says. "What businesses need to do is make sure their security teams are taking the time to be part of that community and experimenting with which channels, profiles, and tags are yielding the most relevant and actionable data for them."

As with any information collected from social media, it's imperative to check its veracity to be effective, he adds.

Outsourcing Social Media Threat Intel

Of course, the sheer amount of information can be overwhelming. For resource-strapped teams, an external threat intelligence provider can help manage the OSINT collection and verification process, according to Brian Wrozek, principal analyst at Forrester.

"Leveraging their expertise to gather, correlate, enrich, and analyze the data is the best way to utilize OSINT," Wrozek recommends. "It can be expensive to internally staff threat analyst resources and then gather, store, and process all that data yourself."

Outsourcing social media threat intelligence gathering can also avoid inundating beleaguered cybersecurity teams with yet another data stream filled with false alerts, Wrozek adds.

"OSINT is a valuable source of information but suffers from false positives if the assets being monitored are common words," he says. "Be on the lookout for misinformation and stale information. Prioritize providers who not only have advanced algorithms to process all that data but also trained human analysts who can provide that extra level of analysis."

Whether its outsourced or undertaken by internal enterprise cybersecurity teams, some level of social media threat intelligence gathering is a valuable addition to any organization's overall security posture, Perception Point's Iytzki says.

"It seems to me a no-brainer for security teams to leverage social media to get actionable threat intelligence in a way that's quick, effective, and budget-friendly," he adds.

About the Author: Becky Bracken writes about cybersecurity and manages webinars for Dark Reading. As the host of Dark Reading News Desk, she highlights the latest trends in security and spotlights industry experts.

GOOGLE CLOUD PERSPECTIVES

AI Is Moving the Needle in Addressing Top Security Challenges

AI is certainly the hot topic of the year, with many vendors introducing AI capabilities into their products. But can AI have a practical application for security teams? Or is it just smoke and mirrors?

By Google Cloud

If we take a step back and look at the pervasive and fundamental security challenges teams face — the exponential growth in threats, the toil it takes for security teams to achieve desired outcomes, and the chronic shortage of security talent — and ask whether AI can effectively move the needle for security teams, the answer is yes.

The key is to take a holistic approach and dig deeper to understand the challenges teams face. What's slowing them down? Without requiring more budget and people resources, what could make the team more productive? How can you add AI to provide assistance where and when teams need it? AI has tremendous potential to supercharge the capabilities of a cyber defender, but it must be applied in a thoughtful manner. AI needs to be used in the places that require a high degree of specialization or a high degree of manual effort.

When we look at modern security operations, AI can play an important role in helping transform threat detection, investigation, and response workflow for security teams. AI has the power to simplify search, complex data analysis, and threat detection engineering — reducing effort and elevating the effectiveness of each individual team member.

For example, AI can be used to boost search. Writing queries often requires specialized knowledge because each product has its own syntax and structural patterns. The need for this kind of domain knowledge narrows the list of team members who could potentially write these queries and analyze the results, thus creating a bottleneck. AI-driven natural language search enables any team member to enter questions in natural language, generating relevant queries that fit desired parameters and present a fully mapped syntax for search. All of this makes it possible for security teams to quickly refine and iterate on results.

"When you think about AI at its simplest core, it's really deep data and search and combining them into something that provides intelligence, especially in security with threats and data," says Robert Herjavec, CEO of Cyderes. "Who's one of the largest data companies in the world? Google. Super excited about the capability there."

Security teams can also improve their investigative capacity with AI. Investigations can result in an enormous amount of context and data to review — far more than any one team member could hope to get through in a timely manner. AI can be applied to automatically provide a clear summary of what's happening in cases, give context and guidance on important threats, and offer recommendations for how to respond.

Indeed, nowhere is AI needed more than in security operations, where understaffed and overwhelmed security teams struggle to defend against a threat landscape that is growing in volume and sophistication — often with tools that were designed in the pre-cloud era. The ability to successfully defend against modern threats will require a fresh approach to threat detection, investigation, and response. Intelligently applied to resolve day-to-day challenges, AI is part of this approach.

About Google Cloud: Google Cloud accelerates every organization's ability to digitally transform its business and industry. We deliver enterprise-grade solutions that leverage Google's cutting-edge technology, and tools that help developers build more sustainably. Customers in more than 200 countries and territories turn to Google Cloud as their trusted partner to enable growth and solve their most critical business problems.

Previous