OVERCOMING THE CHALLENGES OF CYBER THREAT HUNTING WITH CONTEXTUALIZED CONTENT

Modern enterprises must proactively seek out the most dangerous cyber adversaries lurking in their networks today as those are the ones that cause the real or significant damage and loss to organizations. These are the stealthy and dynamic adversaries that slip under the radar of the most advanced security tools including machine learning and artificial intelligence algorithms, the ones who study the most recent cybersecurity techniques in order to evade them. When done right, advanced threat hunting activities can go a long way toward uncovering these advanced adversaries. Threat hunters learn emerging attack techniques from industry intelligence and community channels, they make hypotheses about how these techniques could be used against their environments, and they apply those informed hunches and contextualized content to sift through security data for clues that could lead them to the covert threat actors.

The problem is that many enterprises do not have the expertise or the resources to make a proper go of advanced threat hunting today. Understaffed security operations teams or threat hunting teams (even if an organization has one at all) are drowning in unqualified or false positive generated security data that's never been vetted or even normalized, let alone contextualized against the most up-to-date threat activities.

Many organizations that aspire to achieve advanced threat hunting still depend on alerts based on reactive security tools including ML/AI systems that are dedicated to finding the most obvious threats based on unsophisticated or generic rules/signatures or content. They don't have the time or the wherewithal to generate advanced content (rules, signatures, scripts, free form algorithms, etc.) to proactively get much deeper into the data or to draw connections based on up-to-the-minute threat activities. And that's leaving the most dangerous threats still active in their systems.

Enterprises that are ready to take the next step toward threat hunting maturity need a way to augment their teams in order to break through this reactive cybersecurity stalemate.

The Factors Holding Threat Hunting Back Today

While more than eight in 10 cybersecurity organizations today would agree that advanced threat hunting should be a top security initiative to provide early detection and reduce the biggest risks, only about three

in 10 feel they have the time to search for emerging and advanced threats in their SOC. In most instances, organizations are simply treading water to keep up the cybersecurity status quo. [1]

There are a number of factors holding threat hunting teams back today. Here are some of the most significant.

Overabundance of Unqualified Information

Less than half of organizations today have confidence in the ability of their SOC to gather evidence and investigate to find the source of emerging threats. According to recent studies one of the big impediments to that is an overabundance of unqualified information. Approximately 62% of organizations say they suffer from cybersecurity information overload and 60% report they have an inability to prioritize threats.[2]

According to SANS Institute, over half of threat hunters today say their number one method for hunting threats is by using indicators of compromise (IOCs) to find adversary tools or artifacts. [3] There's nothing inherently wrong with that, but as SANS analysts note, the difficulty is that IOCs have "different levels of quality and life spans," and that the fuel to effective threat hunting is not the volume of IOCs but the quality—"successful hunting requires a well-curated set of IOCs." In other words, they need to have content developed around them that sets the attack scenarios in context. Context is the real key to development of proper advanced hunting content otherwise all an organization is doing is looking for IOC's that aren't appropriate based on wrong time frame, reused IP or hash, type of system, market, attack intentions, and many more components all resulting in an overload of false positives.

Unfortunately, that's rarely what threat hunting teams have at their fingertips today. Most vendors feeding out IOCs or threat intelligence tend to simply stream out unvetted lists of information. They may provide bad IP addresses, but no context behind it around how, when, what or why that IP was bad. An IP address may have been used for two hours last Tuesday against a very specific system. If it pops up on an analyst's radar a month later, it's probably been re-used since then and is now just a time-wasting false positive. And yet that's what most hunters are working with today.

Overreliance on ML/AI

Many in the security community have heralded the sophistication of ML/AI-backed automation as the means to dig out of the information overload. True, cybersecurity detection has come a long way and can do a lot to find the most common threats today. But even the most advanced cybersecurity ML/AI stands no chance against crafty and financially motivated adversaries who have every motive and means to evade them. That's why threat hunting arose as a discipline in the first place. Threat hunters found that the only way they could find the truly bad actors was through human ingenuity. This ingenuity comes from skilled cyberdefenders who hunt through the data, who find suspicious activity that never triggers the most recent ML/AI algorithms, who dig deeper into even more data, and who eventually uncover the new context in which attackers are operating. These hunters are at the spear tip of cyber defense and their human-powered counters to attacks devised by smart adversaries are the only reliable way to keep up with the truly bad threats. The skilled threat hunter doesn't ever know it all and is always learning and sharing with others in the community about new attacks, new concepts, and new ideas on how to detect these advanced adversaries. That is the only way it works. If we were to lock the best cyber threat hunter in a closet for a few weeks without any access to new information they would become obsolete in their abilities to find the newest threats within a few months at best.

The concern about ML and AI systems is that they're only as good as the data which gets fed into their models and rule sets. And in many instances the data they're fed is overgeneralized and it doesn't account enough for the dynamic nature of techniques and tactics that adversaries switch up by the hour. Even the most exuberant proponents for ML/AI admit that one of its biggest shortfalls today is the scarcity of human expertise to make these systems work the way they've hyped themselves to work. One recent report by Capgemini found that

---

1 https://www.cybersecurity-insiders.com/portfolio/2019-threat-hunting-report/

2 https://securityboulevard.com/2019/10/survey-finds-many-socs-are-set-up-to-fail/

3 https://www.sans.org/reading-room/whitepapers/bestprac/paper/39220

half of cybersecurity executives reported that "there is a lack of qualified cybersecurity experts who are capable of improving the logic underpinning AI algorithms to detect threats efficiently."[4]

When cybersecurity teams rely too heavily on unvalidated ML/AI results, they inevitably find themselves on their back feet time and again.

SANS analysts put it best in a recent report:

"Technology is less likely to aid hunters in finding adversaries in their organizations than a skilled hunter is. Either way, a fool with a tool is still a fool, so investing in knowledge development for hunters must become a priority for organizations to remain ahead of the curve in hunting adversaries." [5]

Cybersecurity skills shortage

Today the average percentage of SOC employees involved in threat hunting sits at just 15%.[6] And note that this stat isn't measuring employees dedicated to threat hunting, but only those involved in some hunting activities—at even the most fleeting of levels.

The harsh reality is that even the most robust SOCs simply do not have much bandwidth or expertise to funnel into threat hunting activities. The cybersecurity skills shortage that strains the entire staffing portfolio of a SOC team hits the breaking point when it's constrained even further by the extremely specialized skills requirements for hunting advanced threats. There are only a handful of truly qualified individuals out on the market who are ready-made to create their own hypotheses and dig for clues that will ultimately find the hidden threat.

Even with unlimited budgets, organizations would struggle to find and hire these people to fill out internal threat hunting teams.

What Needs to Change

Maturing SOCs need an accelerant to help them break through the cybersecurity status quo and start effectively hunting threats. One of the most effective ways to do that is to arm analysts with the right kind of informational fuel and advanced contextualized content that gives them a head-start in how they develop their threat hunting hypotheses, and to direct them where to start looking without wasting too much time in the process.

Founded by some of the most respected pioneers in threat hunting methodology and concept, Cyborg offers just the kind of additional security context and content that enterprises need to move their threat hunting analysts to the next level. Cyborg's approach to threat hunting content delivery augments analysts with the foundational information they need to speed up and enrich their hunting activities along with advanced and customized threat hunting content that can easily be ingested into the major security tools most organizations utilize in their environments today. The content feed provided by Cyborg's HUNTER Platform offers the context and the tool enhancement that teams need to get the most out of their existing staff and existing security technology at a cost of less than one experienced threat analyst, while getting the knowledge and content of hundreds of the best analysts in the world.

The content provided by Cyborg varies, but tends to fall into four major categories:

- **Contextualized threat intelligence:**
  Cyborg provides an advanced contextualized threat intelligence feed/portal that adds unprecedented context to threat data (Cybernetic Threat Mapping – Patent Pending). Contextualization includes, but isn't limited to, time frames, market segments, geographic regions, types of systems affected, strings, changing threat pattern matching, threat actor components, and much more. This data is provided in a

[4] https://www.capgemini.com/wp-content/uploads/2019/07/AI-in-Cybersecurity_Report_20190711_V06.pdf

[5] https://www.sans.org/reading-room/whitepapers/bestprac/paper/39220

[6] https://www.cybersecurity-insiders.com/portfolio/2019-threat-hunting-report/

variety of formats, including as a feed, through a searchable and pivot format portal, scripts, CSV files, and rules that can be plugged into security tools or playbooks in to SOAR platforms.

- **Security Tool Content:**

  Cyborg develops advanced and customized (to match your data sets through our patent pending technology) search content and rules that can be ingested into major SIEM, EDR, or SOAR tools. Cyborg creates search language and rules specifically for endpoints based on the newest techniques and tactics. Cyborg's patented tooling allows its analysts to write search languages and rules once for a particular piece of threat information and automatically convert that into a format that's ingestible across all of the major SIEM, EDR, or SOAR platforms and also customized to match your data sets.

- **SOAR augmented content:**

  Cyborg develops security orchestration, automation, and response (SOAR) platform rules and search language that can provide analysts with valuable next steps in the response process when they've discovered specific suspicious behavior in SIEM and EDR tooling. The steps are tied to precise threat activity and help augment a significant amount of work that a human analyst would do in the early stages of a hunt.

- **Free Form Hunting Content:**

  The Cyborg team and its hundreds of advanced threat analysts develop free form hunting concepts, scripts, and algorithms that are used to detect the most advanced attack methodologies and adversaries. These can be used to develop more specific advanced hunting content in a customer's environment or can be deployed against more open or raw data pools including open source data repositories or data lakes. As more organizations move away from expensive and cumbersome SIEM/Data collection technologies into open source alternatives this becomes a key component to develop hunting capabilities in those environments such as Elastic or ELK.

The content fed by the Cyborg HUNTER Platform is developed by some of the most skilled threat hunters on the planet. Additionally, Cyborg plans to bolster that by building out a community platform on which it will run content bounty programs that will run similar to how bug bounty programs work in the vulnerability research world.

This kind of contextualized content provides enterprises with a valuable boost in threat hunting capabilities. For the price of adding a single threat hunter onto its team, enterprises can arm themselves with a 10x multiplier on threat hunting effectiveness to get more out of their team in reducing the most severe risks hiding in their network.

To learn more about Cyborg and the HUNTER Platform, please contact us.

About Cyborg Security

The best threat hunting minds. The best threat hunting ammo. The only real threat hunting platform.

Cyborg Security is a pioneer in cybernetic threat hunting, delivering advanced, actionable threat hunting content via a first-of-its kind single platform. Cyborg's unique platform leverages the best and largest pool of threat hunting human assets and resources, applies techniques and proprietary patent pending technology, and delivers continuously updated content, context, scripts, and playbooks to be leveraged by internal teams. Cyborg provides the platform to proactively threat hunt, without outsourcing or the need to hire direct, scarce skill sets

www.cyborgsecurity.com