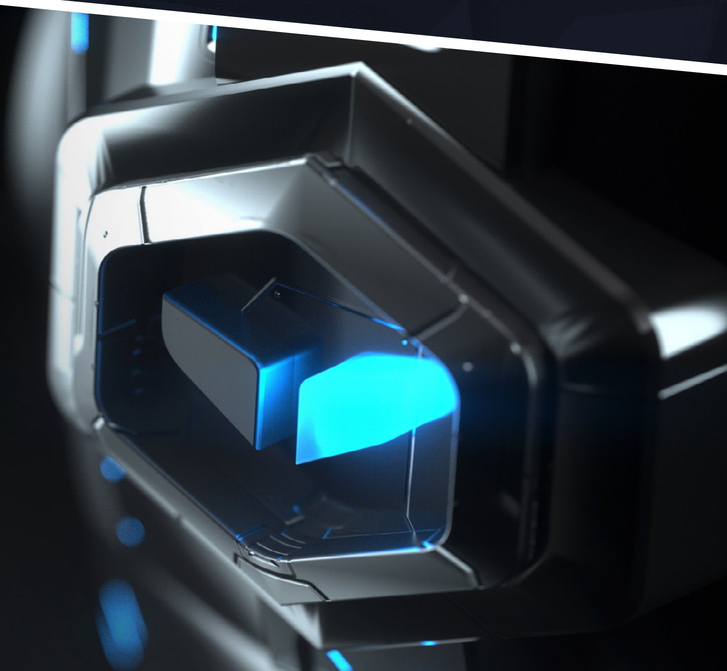
CYBORG SECURITY

THE CONTENT REVOLUTION

The Vital Role Threat Hunting Content Plays in Modern Cybersecurity



cyborgsecurity.com

Quality threat content can make or break threat hunting and detection efforts. Unfortunately, many security teams struggle to find and develop quality content, hampering their efficacy in finding hidden threats. The industry faces a big content problem, one which it must solve in order to improve cybersecurity maturity in the coming years.

WHY THREAT CONTENT MATTERS IN SECURITY

Most cybersecurity veterans understand implicitly at this point that signature-driven threat protection is a losing game for most cybersecurity organizations. They recognize that protection systems which rely on signatures to detect indicators of compromise (IOC) are always chasing the threat, with no hope of catching up.

These indicators are retroactive and grow stale quickly. They're easily evaded by polymorphic malware and new attack tools. They also have the propensity to bog down systems as new rules add up over time. This is why so many enterprise organizations have turned their collective cybersecurity efforts to getting ahead of the attackers through behavioral-based threat detection, often driven by threat hunting.

When SOC analysts and threat hunters focus more on what a threat actor is doing in an environment, rather than on what known malware or tool might or might not be present, organizations can detect malicious activity earlier and discover unknown threats more reliably.

To do this effectively, enterprises collect large amounts of data about activity on the network and endpoints, aggregating them in SIEM and big data platforms. These data repositories contain valuable clues of threat behavior, but they are typically hidden amid the volumes and volumes of everyday activity that occurs across the environment.

In order to find the most troubling signs of threat behavior, organizations also need content to help them search for those symptoms within all that data.

Content, sometimes also referred to as 'use cases' by certain vendors, typically:

- Consists of one or more queries written in a variety of query languages (SPL for Splunk, KQL for Elastic, AQL for QRadar)
- Can look for a simple match such as an event ID in a Windows event log
- Matches one or more conditions which are often defined by threat intelligence about recent threat activity
- Can be extremely complex, relying on multiple conditions to be met

Unlike signatures, which generally look for specific strings or patterns of bytes, content seeks behavioral elements and logged evidence of techniques in use that transcend specific file hashes and IP addresses used by previous attacks. These techniques, which are often learned by an attacker over their lifetime, can be much harder to change and result in a higher fidelity detection of malicious activity.

THE CHALLENGES OF BUILDING AND USING CONTENT

OPAQUE DEPENDENCIES

Most organizations today largely depend upon free open source content, vendor-provided content, or—less often—in-house developed content that staffers create based upon the threat intelligence made available to them. All of these pose transparency issues when it comes to determining the validity of the underlying security intelligence work used to develop the content's queries.

For example, free content often has hidden costs. Whether open sourced or provided by existing security vendors as part of a product or service, free threat hunting content is often very basic and lacks the nuance in behavioral patterning to create targeted searches across security data. Even when organizations invest in expensive threat intel reporting to feed internal development of content, they discover it often only incorporates low-grade IOCs into the mix. If an organization does have experienced, talented threat hunters they can at least build off of that by having these pros do additional work to layer in more data sources, context and vetting, however this is expensive and is not a resilient workflow in the face of staff turnover.

This creates a situation where security debt builds up as those underlying sources are baked into the content, with no transparency into how queries are developed, nor into the context of the data they are based on. When organizations implicitly trust opaquely developed content, their organization often operates under a false sense of security that their threat hunting is based on more advanced intel and search parameters than they think.

STRUGGLE TO SEARCH THE RIGHT PLACES

Development of threat content requires teams to have an extensive knowledge of technologies and log sources to identify the best points for detection. Not all log sources are created equally, and in order to give maximized context to an analyst, log sources to be searched must be chosen deliberately.

Organizations struggle to pick through which sources their content should target, which leads to a lot of threat hunting dead-ends and difficulty in developing hypotheses or building strong hunts.

INCONSISTENT CONTENT PERFORMANCE

The previous two challenges mean that threat hunting and detection teams often seek out threat behavior using inconsistent content.

This drives a lot of false positives and false negatives, as well as technical performance problems. Teams often struggle to properly optimize these rules to run efficiently. Systems can only run so many rules and running an infinite number of queries can bring a box to its knees, potentially causing threat hunting/ detection teams to overspend on processing resources.

When organizations pull in free content, often they have no way to validate if the content will even detect what it says it will. Testing content requires a comprehensive development environment and testbed that may not be available to all in-house threat hunting and content development teams. MSSPs are hamstrung because they have hundreds of clients and they often cannot simulate each unique environment, nor can they detonate malware in those environments, and struggle to simulate threats.

NO ANALYST-FOCUSED DOCUMENTATION

'Documentation' with regard to how content should be used by threat hunters or security analysts is often non-existent. At best, it might be a laundry list of links. Documentation lacks any kind of recommendations for analyst-focused processes or methodologies for analysis.

This results in analysts having to spend valuable time to 'fill in the blanks,' which leads to variable levels of analysis, and inconsistent methods for validating, triaging, and responding to the threat in question. This lack of documentation drastically raises the chance of negligent analysis from all but the most experienced of security teams.

STALE CONTENT

Finally, while threat content ages much better than signatures, it does grow stale. Attackers are always updating methodologies and techniques—albeit more slowly than the malware code itself. Which means content needs to be regularly refreshed to maintain its potency.

Unfortunately, many orgs don't evolve their content quickly enough to match the pace of malicious innovation. They commonly develop or depend upon content that has been developed with a one-and-done mentality where it is rarely refreshed or augmented with new intelligence.

5 TRAITS OF HIGHLY EFFECTIVE SECURITY CONTENT

In order to meet these challenges, organizations need to backstop their threat hunting and detection efforts with a more robust portfolio of content. They need content that provides analysts with the following.

1 CONTEXTUALIZED AND TRANSPARENT THREAT INTELLIGENCE

Solid threat content must be transparent in the threat intelligence it uses, and should come from a range of different open and closed sources to identify new and novel tactics, techniques and procedures (TTPs). Threat behaviors should be contextualized, with findings presented concisely and easily searchable across a range of different platforms.

2 CONTENT TAILORED TO THE ENVIRONMENT

Content needs to be tailored to an individual organization's environment for threat hunters to get the most out of it. The better customized that a content package is developed for the log sources and SIEM platform an organization has in use, the less time and money that SIEM engineers will burn in tailoring it for an organization.

3 RIGOROUS TESTING AND VALIDATION

Threat hunting and detection teams need content that has already been thoroughly validated and tested. SOC teams should be able to know that content is effective, thorough, and applicable within their environment. And organizations should be able to test the content (and their analysts) regularly to ensure that processes are being followed.

4 AMPLE DOCUMENTATION

Effective threat content doesn't just contain the content itself, but is also accompanied by clear, concise, and relevant information for the security analyst or threat hunter so they don't have to spend unnecessary amounts of time trying to "fill in the blanks." That includes:

- An overview of the threat
- Associated research about the threat, methods of exploitation, the actors using it, their objectives, etc.
- Detailed runbooks to ensure consistent and repeatable analysis
- Suggested remediations to close the incident remediation gap

5 LIVING CONTENT

Content loses value over time, as attackers adjust their methods and toolsets. It needs to be consistently reviewed and updated--and so does the accompanying documentation and context—to incorporate new TTPs.

WHY THE CHALLENGES PERSIST: RESOURCE CONSTRAINTS

Developing content that exhibits these traits requires dedicated skilled resources, which are often very expensive. These challenges persist because:

72% of organizations **identify a lack of skilled staff** as their major impediment to maturing their threat hunting capabilities.

51% of organizations reported **significant budget constraints** as impeding their threat hunting.

49.7% of organizations **lack defined processes** because secondary tasks for threat hunters, such as process development, often fall by the wayside.

Hunt teams are often highly dependent on a handful of resources, and any turnover can result in operational pauses or complete halting of threat hunting programs. These resources are often overtasked, and as a result organizations are often stuck in a state of reactivity versus proactivity.

LET CYBORG HANDLE THE CONTENT DEVELOPMENT LIFECYCLE

In order to ramp up threat hunting activities, organizations must consider how they can bolster their content development lifecycle, especially with the security debt they are baking in. At the same time, they must do so while acknowledging the realities of constrained resources.

Cyborg Security helps organizations get the most out of their efforts by developing a portfolio of living content that provides analysts with the timely queries and contextualized documentation they need to run swift hunts and investigations.

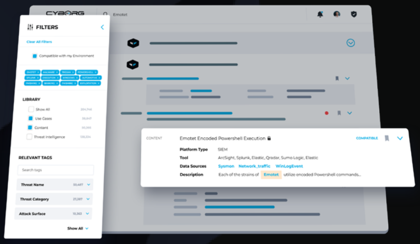
Cyborg's dedicated content development and engineering team creates the threat hunting content, allowing enterprise organizations to maintain control over their threat hunting activities without being burdened with the underlying labor of content development and vetting. This enables lower cost mid-tier resources to act as more expensive threat hunters and evolve traditional security operations into mature security and hunt teams.

CYBORG HUNTER:

1. **CAN REPLACE A TEAM OF 1-5 FTE** for the for the cost of a single resource.
2. **REDUCES THE LOAD ON MORE EXPENSIVE RESOURCES,** allowing them to focus on the primary responsibility of reducing risks to the organization
3. **PROVIDES STABILITY AND INSURES ORGANIZATIONS** against inevitable analyst turnover

CYBORG'S CONTENT IS:

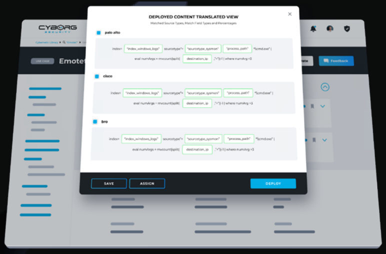
CONTEXTUALIZED AND TRANSPARENT



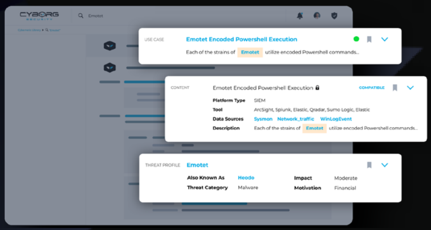
CONTENT Emotet Encoded Powershell Execution

Platform Type SIEM
Tool ArcSight, Splunk, Elastic, Qradar, Sumo Logic, Elastic
Data Sources Sysmon Network_traffic WinLogEvent
Description Each of the strains of Emotet utilize encoded Powershell commands...

TAILORED TO CUSTOMER ENVIRONMENTS



RIGOROUSLY TESTED AND VALIDATED



USE CASE Emotet Encoded Powershell Execution
Each of the strains of Emotet utilize encoded Powershell commands...

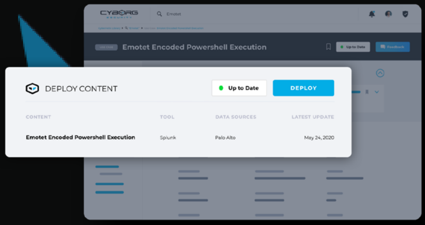
CONTENT Emotet Encoded Powershell Execution

Platform Type SIEM
Tool ArcSight, Splunk, Elastic, Qradar, Sumo Logic, Elastic
Data Sources Sysmon Network_traffic WinLogEvent
Description Each of the strains of Emotet utilize encoded Powershell commands...

THREAT PROFILE Emotet

Also Known As Heodo
Threat Category Malware
Impact Moderate
Motivation Financial

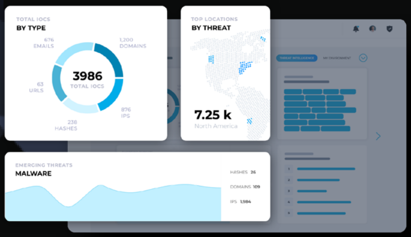
SUPPORTED BY AMPLE DOCUMENTATION



Emotet Encoded Powershell Execution

CONTENT	TOOL	DATA SOURCES	LATEST UPDATE
Emotet Encoded Powershell Execution	Splunk	Palo Alto	May 24, 2020

LIVING CONTENT



CYBORG SECURITY

CYBORG SECURITY IS A THREAT HUNTING PIONEER.

Reimagining threat hunting in a first-of-its-kind platform, Cyborg's HUNTER provides tailored threat hunt and detection packages, and a threat feed focused on operationalized threat data, to augment analysts into hunters and evolve traditional security operations into skilled hunt teams.

See the platform in action

REQUEST A DEMO

Learn more at www.cyborgsecurity.com