

Forge Threat Detection Success at the Pyramid Apex

An effective threat detection strategy
requires having the right detections



ANVILOGIC
www.anvilogic.com

ABSTRACT



Sequenced behavioral-based detections

Singular atomic-based detections have been the foundation for threat detection in security operation centers (SOCs); however, atomic-based detections alone are not enough – the concept has proven unreliable, yielding noisy detections with short operational lifespans. The pyramid of pain categorizes the various detection levels with threat actor tactics, techniques, and procedures (TTPs) being the goal of detection (see Figure 1). The apex is where threat detection should move since understanding threat adversary objectives help to eliminate the focus on chasing dynamic and easily changeable indicators.

Reliance on a single identifier is no longer enough; instead, the atomic components should be structured in sequences to enable behavioral-based detection. Anvilogic is putting our detections deep in the fire to forge a strong security framework. The framework is sequence behavioral-based detections that can help to hone in on the attacker's core objectives to provide a threat detection model that has been designed to hold its long-term strategic value, making it largely future-proof with the flexibility to modify as new TTPs are identified, while also giving security teams the ability to expand and easily detect for any unknowns.



INTRODUCTION

Operational Chaos & the limitations of signature and heuristics-based defense strategies

A practical threat detection framework has been lacking in an industry that has been struggling to keep pace with threat adversaries outmaneuvering frazzled security practitioners. Organizations that adopted signature and heuristics-based defense strategies prove to have limitations inadequately stopping threat adversaries and malware from penetrating organizations. This happens because detection capabilities that focus on the lowest levels of the pyramid of pain, with identifiers accurately categorized as “Trivial,” “Easy,” and “Simple”, quickly lose value. Due to the ease in which threat actors can change the associated indicator can result in a security posture that is constantly degrading and will only hold the short-term strategic value, causing security defenders to chase a constantly moving target.

In addition to having a SOC that is a mad hatter tea party of chaotic disarray, these detections are often noisy and unreliable, contributing to security analysts' burnout and dilution of confidence when trying to discern malicious activity in a sea of alerts. It's an unintentional cycle of operational chaos - that is ineffective when a detection strategy is based on low-level atomic indicators.

Since the threat landscape continually evolves at a pace antivirus systems can't; the focus on delineating the malicious and/or benign threats through code hasn't seemed to be the answer for the security industry.



Organizations must change their reliance on antiquated methods many still think work, or as an industry, we'll continue to go in circles talking about skills-shortages, how to keep up alert-fatigue, and all the rest of the things that hold us back.

The Anvilogic Threat Detection and Incident (TDIR) Platform approach to better threat detection embraces using research focused on threat actor tactics, techniques, and procedures (TTPs) to create detections based on patterns of attack behaviors. Leveraging this threat detection approach can help teams establish a security framework that makes the attacker's main objectives the core focus of alerting.

The Anvilogic TDIR Platform aims to create a behavioral-based framework that can help teams stabilize and modernize their security operations by breaking away from the more traditional chaotic operational cycle. With reliance no longer placed on a single identifier as alerts, teams can shift to sequenced-based threat behaviors composed of multiple threat identifiers. A detection crafted from the apex of the pyramid classified as "Tough" enables detections to operate at a level that isn't malleable, with applicability to various threat activities, eliminating the need to focus or spend time on one-off events.

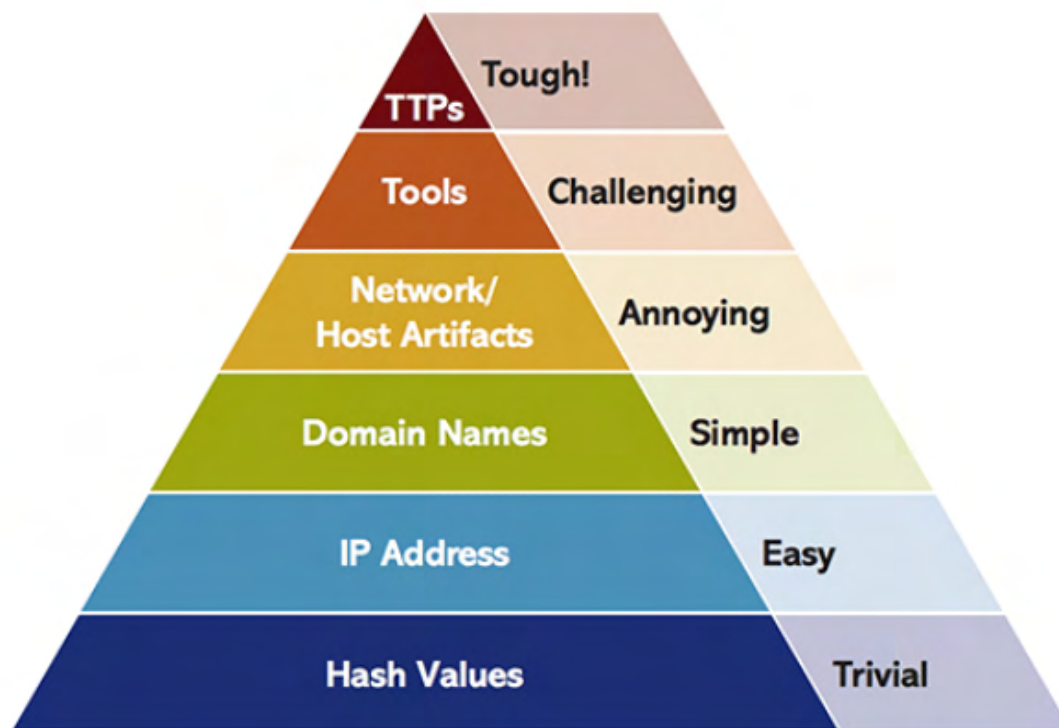
“WE WILL HAVE TO RE-THINK OUR ENTIRE SECURITY STRATEGY IF WE CAN'T HAVE ACCESS TO ANVILOGIC.”

CISO - Top Rated Electronics Retailer

The unstable foundation of the pyramid

In the beginning, there was signature-based, and people were reliant on indicators of compromise (IOC) detections to find everything. Their Intrusion Detection Systems (IDS) also relied on signature definitions looking at IOCs, unique code patterns and tracking file hashes to identify malicious activity. This signature-based method made it easy for adversaries to bypass IOCs, such as hashes through code changes, IPs with fast-flux networks, etc.

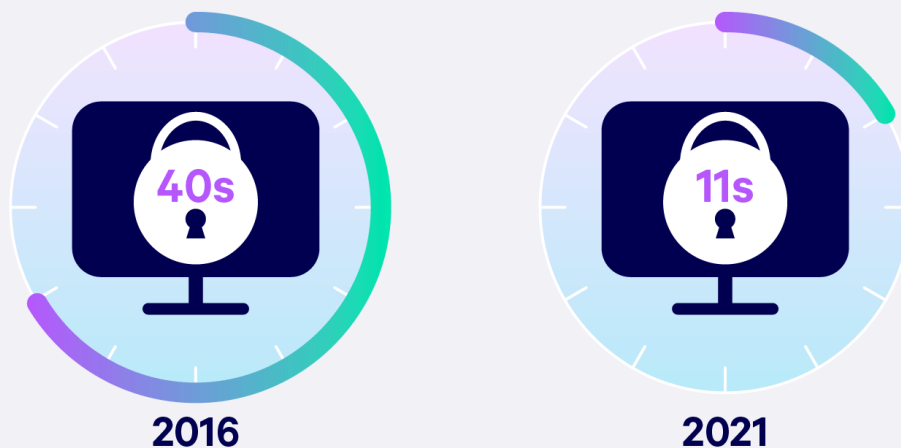
The threat adversaries have continued to compromise enterprises of every scale because they understand blue team defenses and security limitations. People turned to Antivirus (AV) engines that also haven't been able to match the complexity of malware, only creating an approach that has not been able to identify malware or adversarial tools reliably.



(Figure 1) Source: <https://www.uperesia.com/threat-hunting>

Since there was still clearly a challenge identifying threats, heuristic-based detections were created to handle these easily changeable signatures and identify specific properties within executables and processes. While the heuristic-based detections started to help detect the slight modifications of executables/scripts by looking at properties, they didn't affect other IOCs. It began to create a lot of noise for processes – as there are sysadmin/customer-developed applications utilizing similar properties. The heuristic concept, although more helpful than signature-based, more substance was required to be viable rather than inundating security analysts with high-volume alerts and producing low-confidence detections.

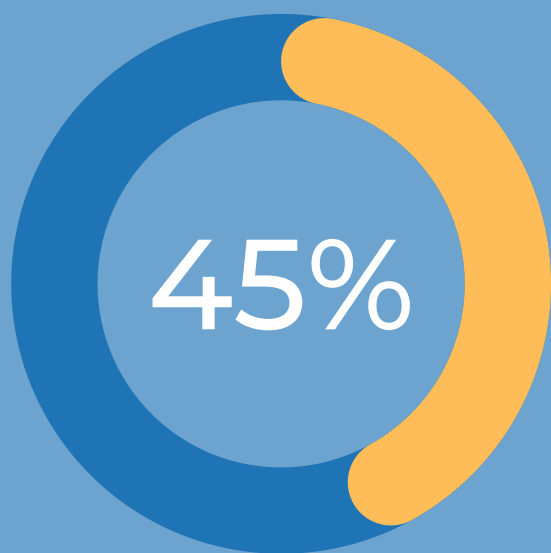
Frequency of Ransomware Attacks



Source: <https://www.embroker.com/blog/cyber-attack-statistics/>

With previous approaches still lacking, efforts to expand and help with the other IOCs started using user behavioral analytics (UBA/UEBA), data science, and machine learning mechanisms. The hope was to analyze massive amounts of data to help better identify anomalous activity and determine what could be a threat; however, it became clear there were challenges with this approach. UBA and similar tools created complex patterns and alerts to help tailor data science-based detections to specific organizational processes and procedures. Unfortunately, because they're complex, many analysts didn't understand and could not triage them.

The problems also cascade to other arms of the organization, such as engineering, who are responsible for maintaining and keeping up with changes to complicated platforms and playbooks. It seems that each evolution created new challenges and did not fully address old gaps before moving forward, which moves us further away from improving the initial foundational challenges. The cracks in the foundation make it harder for security teams to build substantial maturity, keep up, and evolve with the rapidly changing threat landscape.



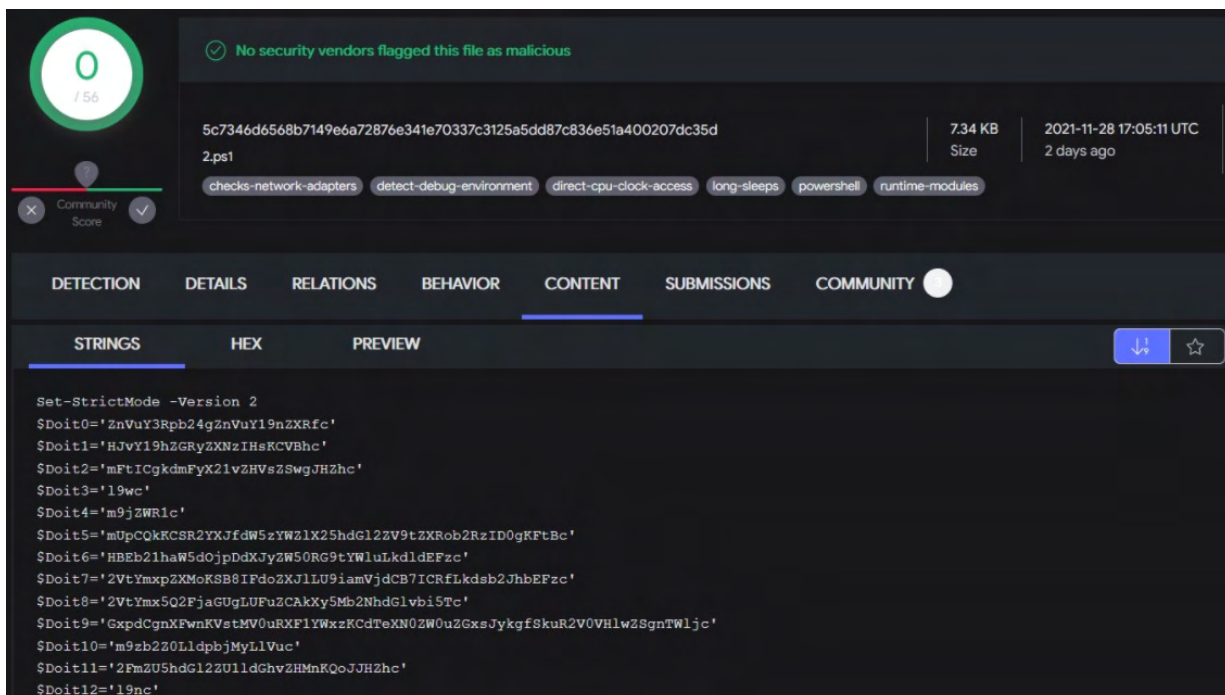
**INSUFFICIENT
SECURITY
MEASURES**

Say that their processes are ineffective at mitigating attacks.

The value of atomic parts & sequenced-based threat detections

The reliance on AV engines alone isn't a viable solution, since AV tools haven't operated at a level consistent enough to delineate benign files from serious threats, even with copious samples analyzed daily. For example, a sample (see Figure 2) identified on November 28th, 2021, was recognized as a malicious Cobalt Strike PowerShell-based payload; However, weeks after the submission, there were still no detections for the signature.

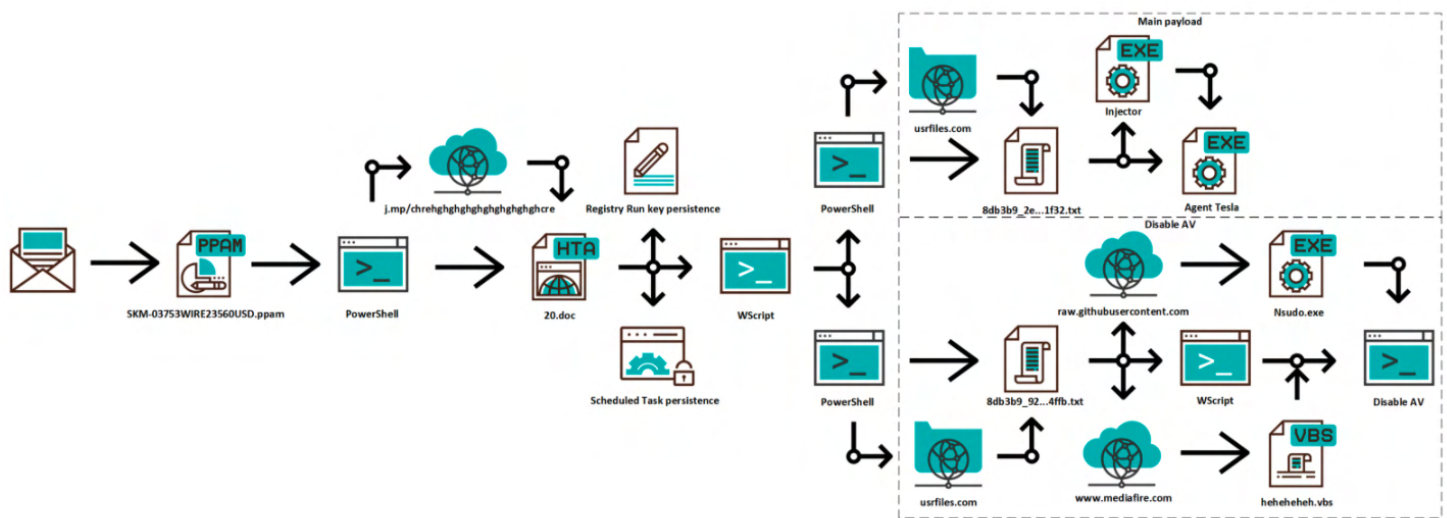
This and many other examples highlight the continued inadequacy of signature-based engines, as they are unreliable in identifying known malware, zero-days, and new variants. Since adversaries continue to utilize novel techniques and threat detection hasn't improved to the point where signature-based detections are reliable against a threat adversary that understands how to adapt and beat this detection mechanism - a new approach to threat detection must be adopted.



The screenshot displays a file analysis interface. At the top left, a green circle contains the number '0' and the text '156'. To the right, a green checkmark indicates 'No security vendors flagged this file as malicious'. The file name is '5c7346d6568b7149e6a72876e341e70337c3125a5dd87c836e51a400207dc35d.2.ps1', with a size of 7.34 KB and a submission date of 2021-11-28 17:05:11 UTC (2 days ago). Below the file name, several tags are listed: 'checks-network-adapters', 'detect-debug-environment', 'direct-cpu-clock-access', 'long-sleeps', 'powershell', and 'runtime-modules'. The interface has tabs for 'DETECTION', 'DETAILS', 'RELATIONS', 'BEHAVIOR', 'CONTENT', 'SUBMISSIONS', and 'COMMUNITY'. Under the 'CONTENT' tab, there are sub-tabs for 'STRINGS', 'HEX', and 'PREVIEW'. The 'STRINGS' sub-tab is active, showing a list of PowerShell commands with obfuscated variables: \$Doit0 through \$Doit12. The commands include 'Set-StrictMode -Version 2' and various 'Doit' commands with long alphanumeric strings.

(Figure 2) Source - Twitter: <https://twitter.com/StillAzureH/status/1465926071547613189>
5c7346d6568b7149e6a72876e341e70337c3125a5dd87c836e51a400207dc35d

As we research and understand the code and behaviors, we don't need to rely on signature-based detection. We can already recognize malicious activity patterns that involve encoded PowerShell (decoded as invoke-expression (IEX)) commands. These are consistent, proven, recognizable threat actor playbooks and attack chains. Identifying patterns leads to additional malicious activity such as initiating payload delivery, executing a living off the land binary (LOLBins), or running discovery commands (see Figure 3).



(Figure 3) Source - SANS ISC

“THIS PLATFORM IS A FORCE-MULTIPLIER FOR MY SECURITY OPERATIONS.”

Vice President of Security - Fortune 100 e-Commerce Platform

Teams can create sequenced-based threat detections by understanding these attack paths to identify that attack chain. It's possible to build a variety of threat sequences that identify malicious behaviors instead of requiring an engine to learn the coding pattern of ever-changing threats, which doesn't evaluate the larger picture. These threat behaviors do have variations – they are known tactics and techniques that threat actors need to achieve.

Along with the VirusTotal example (see Figure 2), research shared from SANS provides insight into an AgentTesla variant that has similar characteristics (see Figure 3). By breaking down the attack into atomic parts, threat identifiers specific to parts of the attack chain can be grouped accordingly with flexibility on various identifiers and sequenced with time, resulting in covering the entire attack chain. The result is a single threat scenario applicable in both use cases, unhindered from coding changes.



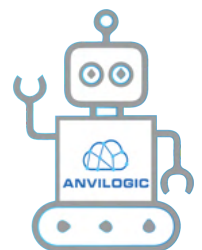
(Figure 4) Source: Anvilogic threat scenario builder – PowerShell

Anvilogic sequenced behavioral-based detection

Anvilogic's Threat Detection Team, The Forge, took a step back regarding detections and did the legwork in building behavioral signatures for how systems respond (in logs) to the same exploits occurring over the last ten years. By having targeted behavioral detections, you can utilize a higher level of detection to identify patterns and sequences in these events to identify a variety of post-exploitation sequences that use the same-old procedures (see Figure 4). Also, by introducing data science into this process, it helps to look for anomalies and differing behaviors in generated events to identify threats occurring in the network more efficiently.

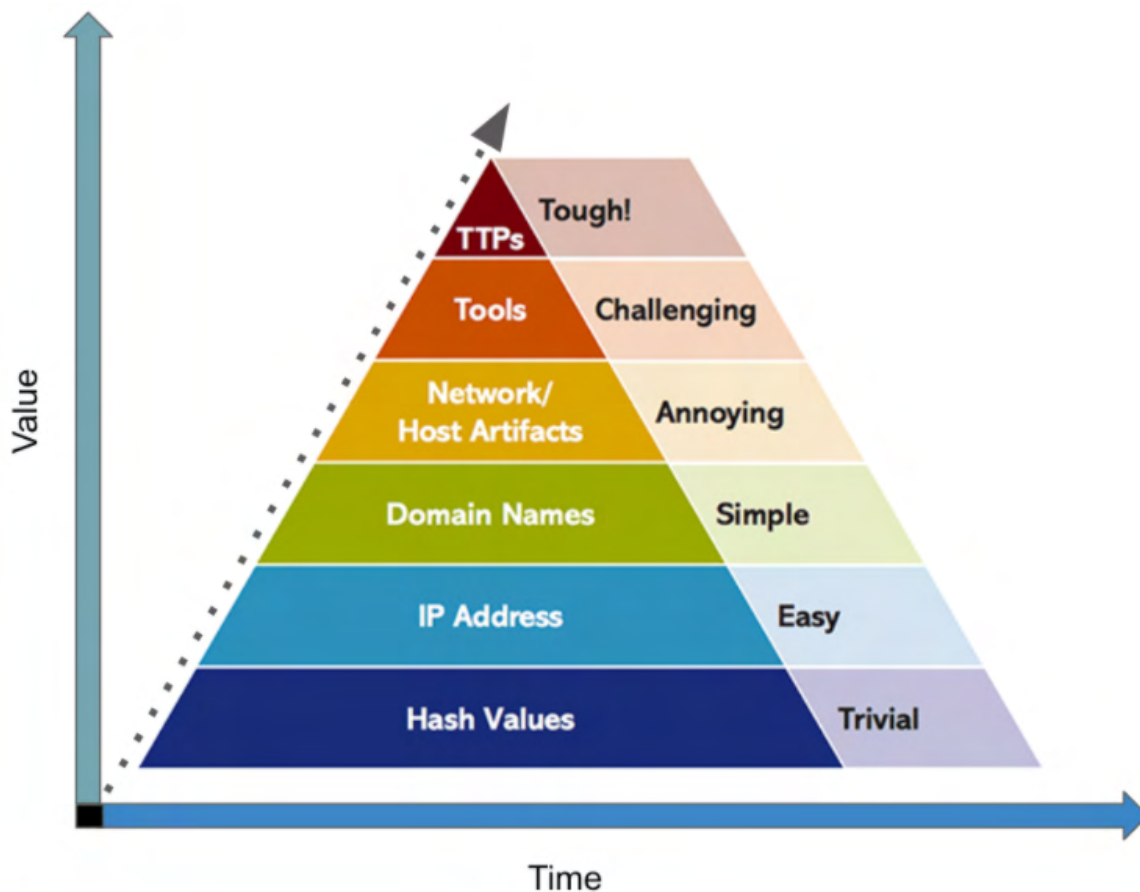
The Forge team has built use cases for various tactics, techniques, and procedures across the MITRE framework.

The Anvilogic platform aims to empower our customers to build these types of sequenced behavioral-based detections quickly. And the Anvilogic platform's no-code detection logic builder quickly and easily generates higher-level logic, performs accurate correlation across all of these generated events from disparate systems. While enriching alerts in an automated fashion instead of putting in the countless hours of research and transitioning hunting's intent from building a detection to identifying a sequence.



Behavioral Sequencing vs. Signature & Heuristic

The Forge team has built use cases for various tactics, techniques, and procedures across the MITRE framework. Using those use cases that are threat identifiers in and of themselves as the building blocks for creating a threat sequence/scenario. The result is a more enhanced, high-fidelity threat sequence composed of multiple threat identifiers that detect threat activity based on known and researched threat behaviors. The concept for detecting attack behaviors scales compared to signature libraries, as its applicability does not depend on single items or events. Still, it aims to capture threat actors' objectives (see figure 5).



(Figure 5) Pyramid of Pain: Increase value, time and scale of detections leveraging sequenced-based detections that track TTPs

Applying Behavioral Sequencing

The Log4Shell/CVE-2021-44228 vulnerability at the end of 2021 challenged the entire security industry that impacted the threat landscape on a massive scale. Researchers and organizations quickly identified samples and obfuscation techniques to create comprehensive detection logic to help identify signs of exploitation. The industry collaboration to share knowledge for a common problem is satisfying, even though it was undoubtedly a chaotic and hectic time for all involved. While the need for detection was urgent, its value will diminish significantly in a few months; thus, the time spent on such a tail chase will likely be inefficient in the long term.

In addition, the atomic indicator for the exploit is purely a detection for an initial access tactic, exploiting a public-facing application, based on its MITRE tactic technique mapping. It is a new perimeter security attack that is dangerous but not entirely indicative of an incident on its own.



ANVILOGIC

Subsequent research showed how exploits were taking advantage of the vulnerability to download additional scripts or install coin miners, for example, which are all threat activities that are known and detectable. It demonstrated how important it is for an organization to understand these attack patterns and have detection scenarios to identify these suspicious sequences of events.

A simple example would be a scenario that detects file downloads, modifications, and executions (see Figure 6). In this sequence, an activity that is otherwise common and benign when looked at individually, but together, in a shortened time-bound event, is an activity that might be worth investigating. The same concept was applicable for Log4Shell. With the atomic indicator aside, the detection needed to identify an attack that only utilized Log4Shell as an initial exploit was already available on the Anvilogic platform; the same concept is applicable for notable security events such as Zerologon and PrintNightmare.



(Figure 6) Source: Anvilogic Threat Scenario

Understanding the post-exploitation attack patterns provides a detection framework that holds long-term value, as it isn't associated with one-off-what-if scenarios. Instead, they have a known sequence of events initiated per the attacker's tactics, techniques, and procedures to compromise an organization. Understanding these procedures will enable organizations to maintain accurate visibility in post-exploitation activities. There is no complex logic or data science element to this; the techniques are outlined within the MITRE ATT&CK framework so security operations analysts can easily understand and triage them.

Clear, Defined & Controlled SOC Operations

From triaging threat sequenced alerts, analysts immediately have a complete picture of what threat activities they need to investigate. Multiple correlated events show a pattern of activity that warrants investigation, with each threat identifier used to provide contextual information to the analyst. This approach moves away from the barrage of single alerts that offer a limited scope with only a handful of available pivot points. A one-line “net group /domain admins” command becomes a time-consuming hunt for reconnaissance activity involving an unknown user, often leading to a system administrator troubleshooting. A consolidation of threat identifiers gives an abundance of information for the analysts to triage the activity quickly. With a no-code element, the development of threat content is simple. It is in the hands of the organization's security analysts who understand threats to build them, unlike a programmer who may not have security knowledge.

A consolidation of threat identifiers gives an abundance of information for the analysts to triage the activity quickly.

This concept scales with vendor tools as well. Suppose a needed detection or audit item calls for a particular CrowdStrike, CarbonBlack, or any vendor solution containing an alert of interest. In that case, the alert can be paired in sequences for known malicious activity that will help boost confidence in the pattern-based threat scenario. Threat sequencing is part of the Anvilogic platform framework. Threat sequencing helps establish a better security operations program that allows analysts to prioritize threats, focus on relevant threats, and correlate existing alerts/events from the abundance of deployed technologies.

An effective detection program relies on the organization's ability to prioritize threats, which involves understanding the infrastructure and prioritizing threat groups; that way, research can be tailored to identifying specific TTPs. We at Anvilogic understand the need to have clear threat prioritization, which is why the team developed prebuilt industry templates to help organizations have a clear understanding of their threat landscape.



Forging the path forward at Anvilogic

Anvilogic has laid the foundation for a new, more advanced detection framework that demystifies security operations. We're steering away from the focus of singular atomic indicators as their ineffectiveness has caused disarray in security operations. An effective threat detection strategy requires having the right detections that focus on understanding adversarial behaviors from their TTPs. With detailed research documenting compromises and attack chains, there's no reason why threat adversaries should continue to succeed. The play for creating formidable detections is available, and it's time to act.

Behavioral-based detection through sequencing is our path forward at Anvilogic. We aim to provide detections through proven threat behaviors to help security analysts identify suspicious network activity with high accuracy, simplifying the detection mission. The Anvilogic platform aims to restore analysts' confidence in alerting from providing high-efficacy, easy-to-build threat scenarios that enable the threat data to tell a straightforward story. While also supporting the fundamentals of security operations to ensure the organization operates as efficiently as possible, with alert recommendations and maturity scoring to ensure continuous improvements.

“ANVILOGIC PROVIDED THE NECESSARY THREAT DETECTION AUTOMATION, ADDING SIGNIFICANT ADVANTAGE. SEEMED LIKE WE DOUBLED OUR TEAM.”


CISO - SaaS Technology Company

About the Team

The Anvilogic Forge is a team of security professionals dedicated to tracking threats and crafting reliable detection strategies for our trusted clients while contributing to our peers in the security industry.

Our mission is to assess the operational behaviors of all threats to provide the community, and our customers, with actionable information and enterprise-ready detections to defend themselves in an ever-changing threat landscape.

References

- Institute for Critical Infrastructure Technology: James Scott:
https://informationsecurity.report/Resources/Whitepapers/920fb41-8dc9-4053-bd01-72f961db24d9_ICIT-Analysis-Signature-Based-Malware-Detection-is-Dead.pdf
 - Research Gate - Zahra Bazrafshan:
https://www.researchgate.net/profile/Zahra-Bazrafshan-2/publication/260729684_A_survey_on_heuristic_malware_detection_techniques/links/54df00e60cf2953c22b0d005/A-survey-on-heuristic-malware-detection-techniques.pdf
 - Institute of Electronic Engineers - Ömer Aslan Aslan & Refik Samet: <https://ieeexplore.ieee.org/abstract/document/8949524>
 - SANS Internet Storm Center:
<https://isc.sans.edu/forums/diary/PowerPoint+attachments+Agent+Tesla+and+code+reuse+in+malware/28154/>
 - 2019 Global State of Cybersecurity:
<https://www.keepersecurity.com/ponemon2019.html>
 - Cybercrime Magazine:
<https://www.embroker.com/blog/cyber-attack-statistics/>
- 



ANVILOGIC

The modern AI-Driven, automated
Anvilogic Threat Detection and
Incident Response (TDIR) Platform

www.anvilogic.com