The Gamer Theory of Threat Hunting: **A Unique Approach for Effective Defense**

For enterprises in today's threat landscape, security measures and defense in-depth strategies are often imperfect and easily penetrable. For many years, the perimeter has been the first and only line of defense to organizations' internal networks. Now perimeter defense has faded with the interconnection of devices and next generation technologies. Organizations are coming to the realization that on the detection side, SIEMs, firewalls, and detection monitoring tools serve their purpose; however, signature and event based detection is limited. In most cases, adversaries are adept at evasion tactics to bypass most perimeter detection and prevention tools used to secure and monitor malicious intrusions. "Hackers can complete an entire data breach in under 15 hours, which includes exfiltrating data" according to a recent industry report.

In a multi-layered stack of security tools, it becomes a game of peeling or stripping back layers to find the core infection layer. When looking for the unknown infection or attack vector in your enterprise ecosystem, many organizations are shifting to iterative hunting exercises based around intelligence operations. If you need a comparison to the level of effort that hunters typically stress during their campaigns, look no further than what most video gamers endure during gaming missions. In the video gaming industry it's considered *a hardcore sport that takes high-level skill, teamwork and dedication, with lots of effort based on achieving a solution as a modern definition*. I coin the relationship between gaming and hunting **"hunt gamers"** as this traditional arrangement of solitary activity can be used in cyber security and intelligence operations for hunting cyberthreats while leveraging various communities of reliance.

So how does an organization make the philosophical shift to this type of hunting for adversarial focused threats in their network?

First, organizations must define and understand the term "threat." The actors creating these threats must possess intent, capability, and opportunity to do damage.

As a practice, threat hunting starts with the hypothesis that threats are eluding you. Intelligence analysts and hunt gamers interact with adversarial behaviors,

indicators of compromise, and signal footprints to identify vulnerabilities and gaps in defensive frameworks. As they shift into this threat hunting mindset, organizations must adopt an iterative approach to ensure success in identification of adversarial behaviors. Let's dive into a few analysis layers that provide insight and vernacular around identification of threats and detection techniques.

Layer 1: Entry Point Analysis

Knock knock, I want in!

To kickoff, let's talk a bit more about peeling back the enterprise security layers and where/how exactly this is done. In this paper, a layer is the spectrum where a threat in your network can exist or an agnostic entry point of the actor. This begins with "getting into the building," or the infection point. Usually the edge of the network is where most monitoring tools reside for detection of inbound tactical indicators of threats and signature monitoring. In this layer of the end point and perimeter security stack, you typically deploy firewalls, email gateways, intrusion detection and endpoint management security solutions. These are passive in nature.

The end goal here is to try to detect anomalous attacks in progress and baseline network activity across your perimeter of defense. It's likely that suspicious network connections, downloads and registry modification, process execution, and select API call record monitoring represent front line discovery based on alerting logic. This layer has an intrinsic temporal nature to it, since data with a short half life is rapidly collected from sensor input at extremely high volumes. This includes system events with limited visibility, social engineering scams, and email phishing attempts to gather personal information to infiltrate networks at this layer.

Layer 2: Log Analysis

Am I breached?

Is someone monitoring my systems right now, logging my keystrokes, stealing my credit card information or intellectual property?

Answering these questions is a challenge for organizations, and many aren't equipped to logically decipher modern threats within their data repositories. Most organizations leverage Security Information and Event Management (SIEM) in their security measures for defining requirements, analyzing collected data sources, aggregation and tuning, and building content in the form of rules, dashboards, and alerts for prioritized detection.

Traditional hunting in SIEMs requires existing log collection in repositories (i.e. log management, indexes, RDBMS, etc.) for querying or alerting on behavioral events that are constructed with rule logic. The quality of the monitoring initiatives and value of SIEM are dependent on datastore quality and the caliber of team assigned; the security analyst is in charge of hunting through source logs to discover useful information. The team must work through initial pain points of a SIEM: product configuration, repeated rule tuning, false positives, and inaccurate source details such as timestamps. Limitations in log retention and online log access within SIEMs create a meticulous and arduous effort to scale your network to detect relevant threats and apply mitigation strategies in near real time.

However, when a system compromise occurs, being able to rapidly construct queries across larger datasets for analysis of associated threats via hunting methods decreases time to remediation. Machine learning and external curation of information pushed into SIEMs also continuously improve their effectiveness.

Layer 3: Threat Intelligence Operations (CTI)

Threat intelligence is a team exercise!

As threat actors increase the frequency and sophistication of targeted attacks, organizations rapidly come to depend on threat intelligence operations. Threat intelligence can provide evidence-based tracking, analyzing, and countering of external security threats. One of the core responsibilities of intelligence analysts, including hunt gamers, is proactively identifying security events that can be thwarted through early warning/preemptive detection. The difficulty faced by the community is the massive amount of data and information that must be fused, analyzed, and measured to form a more complete understanding of the threats organizations face.

In the current state of cyber threat intelligence collection, organizations lack the understanding to model risks and threats against targeted network systems. MITRE's Adversarial Tactics, Techniques and Common Knowledge (ATT&CK) is a select model for cyber adversary behaviors. Overall CTI program maturity models introduce a "crawl, walk, run, fly" life cycle which is important in evaluating your computer network defense readiness to threats. Threat intelligence analysts must routinely and dynamically monitor internal systems as well as external intelligence sources for threat discovery. Atomic observables such as domains, IPs, and encryption keys are collected by various analytical methods. Behavioral based observables such as Tactics, Techniques, and Procedures (TTPs), persistence mechanisms, and social engineering also need to be strategically managed and associated to tactical targets as hunt sprints produce investigative workflows.

> A great example of the usage of non-traditional tactics was in the 2016 election with nation state interference. Influential operatives built troll factories focused on campaigns that leveraged social media outlets to create mass discord. Actors used VPN infrastructure hosted in U.S. regions to create botnet accounts to distribute propaganda and weaponize information.

To make matters worse, threat actors are not static artifacts. Cyber threat actors are dynamic in nature and transform over time, rapidly changing the overall CTI landscape. Threat analysts must be able to identify changes in attack trends. From there, hunt gamer analyst teams are charged with building threat model profiles of entities they encounter. This profile information is collected from more than one source outlet and must be weighted based on relevance, state, and timelines. Sorting through various data sets to decipher intent and strategic targets is a cumbersome activity.

In order to compare actor-centric datasets with TTPs and leverage them within the cyber threat intelligence process, they must be stored in an efficient, applicable manner. This often includes an inter-relational data set within a threat intelligence platform (TIP), making it easier for orchestration of research and response within an organization.

For better security automation, threat intelligence platforms utilize algorithmic machine learning data models for scientific constructs of behavioral, atomic, and indicator analysis. This vastly accelerates the decision making process around threats ingested externally and matched internally with event data collection tools.

TIPs like ThreatStream, or threat platforms that enable managing intelligence about malicious indicators and actors, also enable the managing of intelligence about non-malicious observables used to craft data driven SIEM implementation and system control policies. However, artifacts like indicators of attack are valuable but temporal and easily modifiable by attackers. Research has shown that focusing on TTP's when hunting is challenging but they are harder for attackers to modify.

Seasoned threat intelligence analysts use graph-centric workflows to effectively piece together investigative findings in a succinct way. Incorporating force directed link analysis mapping for associating threat artifacts builds an exploratory topology for reporting. Searches can provide information on patterns that might be hidden in historic records.

Pivot tables and event timelines will provide interconnected observables for visualization, direct correlation, indicator expansion, and time plotted events of occurrence. The results of these graphs will drastically accelerate investigative reporting and campaign enrichment.

Automated contextualization via machine learning emerging threat platforms will collect new identified threats with exploit relationships, network sensor, honeynets, OSINT, and enrichment tools such as Passive DNS or WHOIS.

Working in Numbers

In most gaming communities, there is a tight sense of trust and the players are close nit teams and groups. These teams or groups could exist for short or long term durations. Team is defined as:

> *The ability to work together towards a common goal.*

Video gamers spend several hours collaborating to build trust with members of the community to gain competitive intelligence, discovery of tactics, and strategies otherwise difficult to obtain individually.

As this applies to video gaming forums, it also applies to threat intelligence operation teams and hunters. Threat analysts, SOC analysts, and even hunters are more efficient when working in cohorts or communities to interpret encountered threats. Sharing communities are effective ways to collaborate with trusted members for relevant analysis of potentially targeted attacks on an organization. Hunters are charged with mining and collecting as much detail and context around their findings; some of which exist within trusted communities and are classified by the privacy of a threat artifact or intelligence finding.

So how does hunting by peeling back the threat layers converge with a core layer of threat intelligence operations?

To answer this question, you must ask a follow-up question: *are you programmatically mature to leverage threat intelligence during hunting activities?*

First, you need to know where in the hunt maturity model your organization resides. Depending on the market source or maturity model variance chosen for your organization, the genesis is pretty similar for answering the stage of maturity state. We recommend the Hunting Mature Model as proposed by Sqrrl (see figure 1 below).

Hunt Levels of Analysis – Activity and Deep

Activity Analysis Phase:

In each phase of the hunt, the three core areas of focus to obtain levels of threat awareness and discovery:

Data input

- Internal log collection/flow collection
- Event querying via SIEM, End Point, Sensors
- Trusted intelligence source collection
- Subscription media and new outlets

Process Analysis

- Triage
- Signature, binary analysis, and malware research
- Threat Model sequence analysis (kill chain, diamond model, etc.)

Data Output

- Baseline pattern monitoring reporting
- Threat Modeling Metrics
- Business Risk ranking

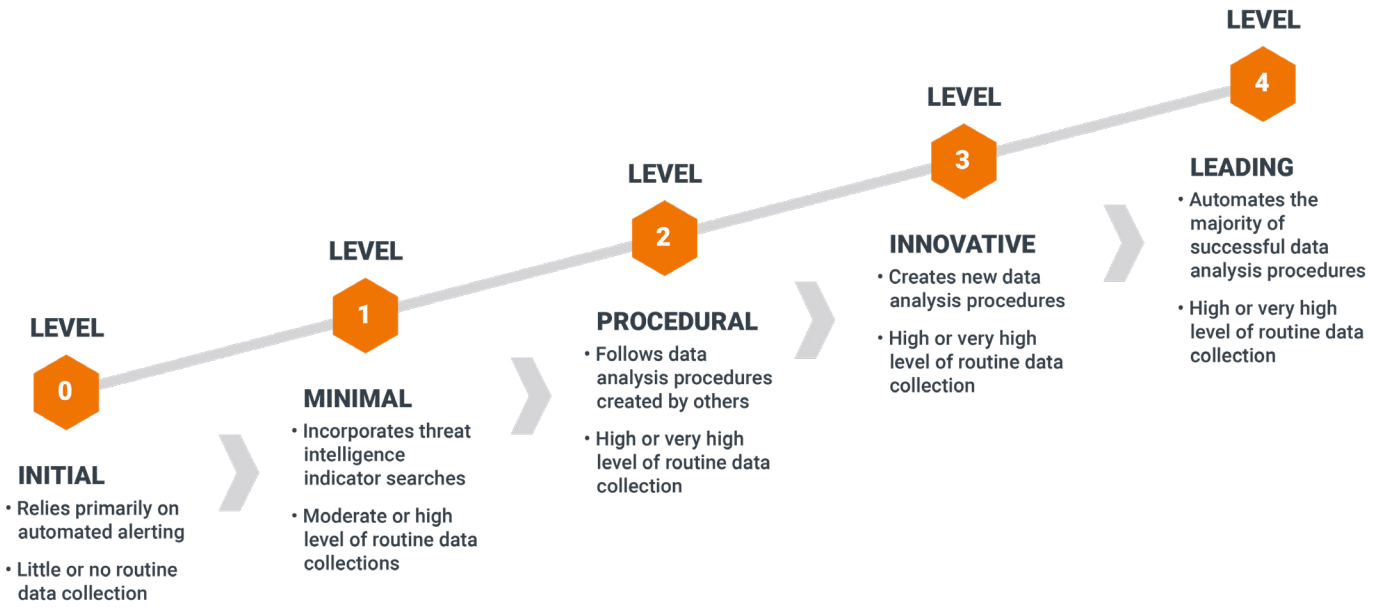

Figure 1

Deep Analysis Phase:

This layer uses all of the Activity phase criteria but goes more into the science of analysis for hunting threats:

Data input

- Hypothesis generation and examination
- Interactive question chaining

Process Analysis

- Structural analysis techniques
- Dynamic and Static Sandbox analysis

Data Output

- Targeted organizational answers to hypothesis examination
- Strategic approach to known issues for proposed solution
- Advanced visualize and graph representations
- Re-examine the proposed solutions

Hunting (Hunt Gamers) Main goals:

1. Develop hypothesis
2. Document collection requirements.
3. Analyze data collection and deep exploration to locate obscure signals from passive monitoring.
   a. Leverage data science techniques and machine learning technologies for greater impact to identify significant events.
4. Expedite adversarial detection to reduce dwell time for reduction of forensic costs

a. Defend enterprise assets (crown jewels) from exploitation tactics by actors

5. Identify, characterize, and detect persistent and advanced adversarial artifacts as early in the kill chain as possible to supplement incident response. A few example hunts:
   a. Tor exit node hunting
   b.Web Access hunting w/ missing proxy entries
   c. Sparse User Agents identification
   d. MD5 mining and collection; autoruns for PUP's
   e.Memory injection / file based triage
   f. DNS covert channel for stealth C&C presence / data exfiltration
   g. Role based credential misuse / ATO
   h. Rare indicators on file system
   i. Domain generated algorithmic distributed malware
6. Collaborate in hunt gamer communities to share and assess enterprise threats.
   a. Sharing provides the capability to annotate hunting trips, event timeline chaining, and shrink collaborative investigations to build a conclusion. Most likely internal, but possibly external driven groups.
7. Document and build test procedures for reporting and then automate with tools to repeat this cycle.

Conclusion

"Threat Hunting will introduce new possibilities into threat detection which will apprise a new hypothesis to reiterate the process."

Overall, the collation of video gaming and traditional threat hunting is conclusive when applying it to the modern outlook of adversarial coverage. Hunting should be a proactive, complementary aspect to each layer of the security stack and provide disruption to attackers to be effective. The ability to utilize machine learning fused threat platforms can exponentially increase hunt gamers effectiveness by automating the simple tasks such as aggregation of intel sources and attributes. Hunting requires sophistication and dedication to searching for elusive and adaptable threats.

Creating an iterative hunting process involving a threat intelligence ecosystem can provide optimal threat response and correlation around malicious activity, persistence, and relational threat modeling. This produces an environment for hunt gamers to provide increased coverage, orchestrate more effective data collection, and make decisions to support security operations. In essence, three key concepts hunt gamers in an organization should focus on are: assume the compromise of assets, examine stealthy compromise and breaches in all phases of an attack, and think and react like an adversary.