HYAS

SOLUTION BRIEF
HYAS Insight

Five Proven Techniques to Optimize Threat Intelligence

The most devious criminals are always one (or several) steps ahead of their victims. To stop them in their tracks, we need to figure out how they think — which is no easy feat. When we know how they work, we can glean actionable insights that empower us to strengthen our overall security posture.

The art of effective threat intelligence is the process of gathering and analyzing and then leveraging that information to anticipate, detect and respond to those threats. We review the five best practices for leveraging threat intelligence, including the most effective detection methods and strategies to safeguard against ever-evolving, increasingly sophisticated cyberattacks.

1. Start With Signature-Based Detection

Signature-based detection identifies the unique “fingerprint” of a threat, comparing incoming data against a database of known patterns of malicious activity, such as specific sequences of bytes or hashes in malware files. It’s often the first line of defense against malware.

Strengths:

- **High accuracy:** Although it’s one of the oldest methods of threat detection (it was the basis of the first anti-virus systems), signature-based detection remains popular because it’s still extremely effective at finding known threats.
- **Energy/cost efficiency:** Signature-based detection can identify known malicious files or pieces of malware without heavy resource constraints on the systems themselves (or from database resources).
- **Speed:** Searching for predefined signatures is one of the fastest ways to find threats.
- **Low incidence of false positives:** When signatures are up-to-date, false positives are minimal.

Limitations:

Signature detections can’t holistically identify, detect and investigate much of the newest malware, especially AI-generated malware.

- **Dependency on database updates:** Signature-based detection requires frequent updates to maintain effectiveness against new threats.
- **Ineffectiveness against zero-day threats:** Signature-based methods cannot detect the latest threats (or unknown threats lacking a signature).

Applications:

- **Antivirus software:** Traditionally, antivirus apps use signature-based detection to identify and remove malware.
- **Intrusion Detection Systems (IDS):** These solutions monitor network traffic for patterns matching known attack signatures.

The bottom line:

- **It’s a cybersecurity fundamental:** As one of the underlying linchpins of malware detection, signature-based detection should still be part of any organization’s overall comprehensive security program or suite.
- **Regular updates are necessary** to ensure that signature databases are amended frequently to cover the latest threats.
- **It’s not enough in itself.** Use signature-based detection in conjunction with heuristic-based detection to cover a broader spectrum of threats.

2. Add Heuristic-Based Detection

Deriving from the Ancient Greek word meaning "to discover," heuristics is a broad term that applies to psychology, user interface design and a number of other fields. But for cybersecurity purposes, heuristic-based detection solutions identify potential threats and analyze the characteristics of files (or activities) — rather than relying on known signatures. How? By using algorithms that can identify suspicious patterns and evaluate the likelihood of malicious intent. As we see more advancements in behavioral analytics in machine learning, heuristic detection approaches will be essential to keep pace with cyberthreats.

Strengths:

- **Detects unknown threats:** Heuristic-based detection is particularly effective at identifying new and previously unknown malware.
- **Behavioral analysis:** Heuristic-based strategies examine the behavior of files, which can reveal polymorphic threats (those that constantly change structure or content in an effort to evade detection).

Limitations:

- **False positives:** Heuristic approaches have a higher risk of false positives compared to signature-based detection.
- **Complexity:** These methods are more complex and resource-intensive than signature-based ones.

Applications:

- **Advanced malware detection:** Heuristic-based methods identify suspicious activities that deviate from "normal" (predetermined) behavior patterns.
- **Endpoint protection:** Heuristic applications monitor and analyze behavior on endpoints to detect potential threats.

The bottom line:

- **Seize the zero-day:** Finding new or as-yet-undiscovered threats is where heuristic analysis shines.
- **Take a balanced approach:** Combine heuristic-based detection with signature-based methods to balance accuracy and coverage.
- **Regular tuning required.** Continuously refine and update heuristics to improve detection capabilities and reduce false positives.

3. Secure All Remote Admin Tools

In our work-from-anywhere era, we heavily depend on remote administration (admin) tools like TeamViewer and Windows Remote Desktop. However, hackers are becoming increasingly adept at penetrating and using them to “legitimize” malicious behaviors.

Once bad actors gain access to an environment, their activities might appear valid, making it a lot harder for security controls to detect threatening behavior. Securing these tools involves monitoring network traffic and system processes to identify and block unauthorized remote access attempts.

Strengths:

- **Preventing unauthorized access:** Remote admin security tactics can stop potential intrusions before they escalate.
- **Real-time monitoring:** Vigilant supervision enables immediate detection and response.

Limitations:

- **Resource-intensive:** Securing remote admin software requires continuous monitoring and can tax security operations team resources.
- **Sophisticated evasion:** Advanced attackers may use sophisticated methods to bypass detection and gain access to networks by leveraging remote admin tools.

Applications:

- **Network monitoring tools:** These tools analyze network traffic for signs of unauthorized activity via remote access applications.
- **Endpoint security solutions:** Every endpoint is an inherent risk, so endpoint solutions are necessary to detect and block unauthorized tools on individual devices.

The bottom line:

- Remote admin tools are here to stay, but **they dramatically multiply the number of attack vectors.**
- **Conduct regular, frequent scans** of networks and systems to identify the presence or use of unauthorized tools.
- **Access controls:** Implement strict access controls and authentication measures to limit remote access capabilities.

4. Whitelist the Organization’s Approved Tools

What is whitelisting? Creating a list of approved applications and tools that are permitted to run within the organization’s environment, blocking all others by default. In other words, users can only take actions on their devices that an administrator explicitly allows in advance.

Strengths:

- **Regular scans:** With a whitelist, a security team can conduct frequent scans of networks and systems to identify unauthorized tools — what’s not on the list.
- **Reduced attack surface:** A whitelist limits potential entry points attackers may use to gain access to a network.
- **High security:** A whitelist can also prevent unauthorized applications from executing and stopping attacks before they begin.

Limitations:

- **Constant maintenance:** Whitelists require continuous updates to ensure currency.
- **Administrative hassle:** Whitelisting may seem “extreme” and is sometimes inconvenient and frustrating for users.

Applications:

- **Application whitelisting software:** These solutions control which applications can run on which endpoints.
- **System policies:** Whitelisting at the operating system (OS) level can restrict users from downloading, installing and/or running unauthorized tools.

The bottom line:

- **Whitelisting isn’t a one-size-fits-all tool or a security panacea,** but it can be an integral part of a comprehensive security operations program.
- **Regular updates required:** Keep the whitelist updated to include new, approved tools.
- **To optimize this strategy and reduce frustration, educate users** on the importance of whitelisting and the process for getting tools approved.

5. Employ Protective DNS Tools

Domain Name System, or DNS, is often described as the "phonebook of the internet," and protective DNS (PDNS) service is like an operator who prevents connecting with a bad actor. That's why it's a fundamental layer of any security stack.

Protective DNS blocks access to malicious domains, preventing threats such as phishing, malware, exploit kits, botnets and command-and-control communications. It's a proactive "choke point" and a prerequisite for harnessing threat actor infrastructure as a defense — essentially, using a hacker's own framework against them.

Strengths:

- **Preemptive blocking:** PDNS solutions stop connections to malicious domains before they can cause harm.
- **Cost and resource effectiveness:** PDNS is a fairly low resource-intensive solution, not only to deploy and implement, but also to manage and integrate. It's a cost-effective, straightforward way to gain a lot of information about an organization's network telemetry.
- **Broad coverage:** By blocking access to known bad domains, PDNS safeguards a network against a wide range of threats.

Limitations:

- **Dependency on DNS providers:** This strategy relies on the DNS provider to maintain an up-to-date list of malicious domains.
- **Potential overblocking:** Working at the point of a user's request to access a website, PDNS may occasionally block legitimate sites.

Applications:

- **PDNS filtering services:** PDNS filtering blocks access to malicious domains — at the "source," so to speak.
- **Enterprise DNS solutions:** Implementing DNS protection at the organizational level safeguards all connected devices on a large network.

The bottom line:

- **DNS is a foundational component of internet communication, s**o PDNS is an extremely effective frontline cybersecurity defense.
- **Choose reputable providers** known for maintaining comprehensive and up-to-date threat databases.
- **Monitor and adjust** PDNS filtering logs regularly to ensure legitimate domains are not being blocked unnecessarily.

Fortify and Future-Proof Your Network

The threat landscape is constantly changing, so cybersecurity tactics must evolve as well. By incorporating these threat intelligence best practices, any security team can build a robust defense against malware, phishing, DDoS attacks and whatever comes next. But it's critical to review and update your threat intelligence processes and tools regularly. Stay informed about new threats, technologies and the latest lines of defense — and adapt your strategies accordingly.

With HYAS solutions, including HYAS Protect (our PDNS solution) or HYAS Insight (our leading-edge threat intelligence and investigation platform), organizations of any size can integrate award-winning cybersecurity technology into their existing stacks. We make it seamless, simple and scalable, so your network stays safe — and you can focus on what you do best.

PROTECTIVE DNS

HYAS Protect

Protective DNS

Our protective DNS solution combines authoritative knowledge of attacker infrastructure and domain-based intelligence to proactively block malicious communication used by cybercriminals to conduct phishing, ransomware, and other forms of cyberattacks.

Explore HYAS Protect →

THREAT INTELLIGENCE & INVESTIGATION

HYAS Insight

Threat Intelligence & Investigation

HYAS Insights allows you to rapidly discover and investigate any IOC and related indicators. Identify and map out the complete cybercriminal campaign architecture and take a proactive stance against future attacks.

Explore HYAS Insight →

Contact Us For a Demo

hyas.com/contact

HYAS

Protecting Businesses and Solving Intelligence Problems Through Detection of Adversary Infrastructure and Anomalous Communication Patterns

HYAS is a world-leading authority on cyber adversary infrastructure and communication to that infrastructure. HYAS is dedicated to protecting organizations and solving intelligence problems through detection of adversary infrastructure and anomalous communication patterns.

We help businesses see more, do more, and understand more in real time about the nature of the threats they face. HYAS turns meta-data into actionable threat intelligence, actual adversary visibility, and protective DNS that renders malware inoperable.