RELIAQUEST

Maximize Your Threat Intelligence:

Four Proven Steps to Integrating Threat Intelligence for Higher-Fidelity Detection and Response

How can security teams organize, integrate, and apply threat intelligence across their environment to identify and take action on the most serious threats?

Introduction

Accurate, trustworthy threat intelligence is a boon if you have it – but too much of it becomes a management headache. Analyst group 451 Research, surveying security leaders for its report ***Tackling the Visibility Gap in Information Security***, found that 49% of enterprises using SIEM, EDR, and other security tools were overwhelmed by the day-to-day operation of managing and ingesting threat feeds into their growing technology stack.[1]

The problem is one of balance: Too little intel, and your organization runs the risk of failing to notice (or be prepared for) a major threat. Too many intel feeds, and the risk is that your team becomes overwhelmed by data. Just because you have a large quantity of intel doesn't mean your security teams and technologies can process it and use it effectively.

NOT ENOUGH INTEL

TOO MANY INTEL FEEDS

[1] 451 Research, ***Tackling the Visibility Gap in Information Security***, July 2019: https://www.reliaquest.com/resources/study-tacking-the-visibility-gap-in-information-security/.

If the threat intelligence balance tilts too far in either direction, the risks of being underinformed or overburdened increase. If teams can't sift through mountains of intelligence in a timely manner, they might not focus enough attention on real threats; teams may also be trying to close the intelligence gaps by spending money on tools and processes that aren't needed.

On the other hand, if intel is thin on the ground, attackers stand a better chance of gaining a toehold in organizations. Undetected threats can cause substantial damage: For example, when the WannaCry ransomware attack hit public and private enterprises worldwide, some suffered costs amounting to tens or even hundreds of millions of dollars.

The solution to managing the right amount of threat intelligence, and integrating intelligence with security controls, involves:

- evaluating the threat intelligence you are collecting
- implementing threat intelligence with detection and response systems
- reviewing threat intelligence implementation on a regular basis for more effective threat mitigation

These steps represent a critical phase in your journey towards improved visibility, end-to-end automation, powerful metrics and reporting, and maturing your security program.

> **Multiple intel feeds improve coverage, but integration with these sources poses its own challenges: duplicate entries, inconsistent formatting, and large datasets without any way to prioritize IoC consumption.**

In this paper, you'll learn:

HOW to integrate threat intelligence with security programs

WHAT processes are needed to create high-fidelity threat detection

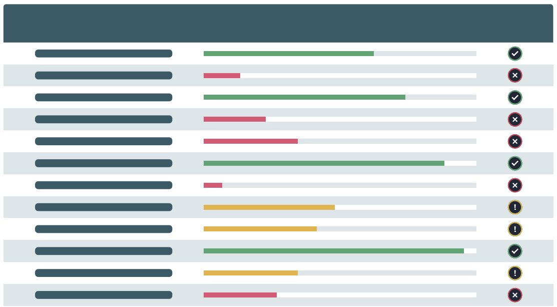
WHY examining both indicators of compromise and behavior patterns are key to improving security

Four steps for effectively implementing threat intelligence into your security program

The methodologies for implementing and using threat intel involve both IoCs (indicators of compromise) and behavioral patterns. Security teams need to address methodologies across both categories if they want to successfully automate threat detection and response, since the processes serve different purposes: IoCs are easier to implement and cover very specific threats, while behavioral patterns are harder to implement but cover a broader scope of threats.

The combination of IoCs and behavior patterns also helps build higher-fidelity threat detection. Add in automation, and you have a recipe for more accurate intelligence, fewer false positives, and faster response.

STEP 1: COLLECTION



In this process, your goal is to collect intelligence that means the most for your industry – and align that intelligence with frameworks and issues that are most relevant for your organization. As a rule of thumb, all threat intelligence must be accurate, relevant, timely, and actionable.

IoCs:
Research timely and accurate threat intelligence feeds to find those with the highest fidelity. The research step is critical: Without it, you run the risk of using old threat intelligence that may no longer be relevant to your organization. In addition, outdated feeds may have unconfirmed IoCs, which can generate unnecessary false positives.

Start by looking at feeds from sources such as SANS and DHS – and for threat intelligence specific to your industry, check out the Information Sharing and Analysis Center (ISAC) feeds, such as the FS-ISAC for the financial industry. Find a list of industry ISACs here.

Behavioral patterns:
Find a security framework that aligns with the TTPs (tactics, techniques, and procedures) of your industry's common attackers. MITRE ATT&CK® is a good place to start as it offers a detailed framework; the kill chain is also a good starting point. Aligning with a framework helps to measure progress of implementing threat intelligence, and also provides a starting point for covering all aspects of threat actors' attack paths. A bonus of aligning with frameworks is that you are better able to measure security performance and show value of security investments.

STEP 2: PREVENTION

The best defense against attackers is not letting them get that proverbial foot in the door at all, so that they never do damage.

IoCs:
Leverage knowledge of damaging attacks from other organizations to improve mitigation. Based on your discoveries, add controls to prevent threats from executing and causing damage. Consider implementing block lists on firewalls and proxies that are dynamically updated with the collected threat intelligence.

Behavioral patterns:
Use the technology that you have in your environment to ensure attackers don't get a foot in the door. For example, if intelligence shows one of attackers' first goals is to obtain administrative privileges, eliminate that easy attack pathway by limiting which users have these permissions.

STEP 3: DETECTION

Security teams need confidence that threat intelligence delivers enough information to justify blocking traffic. Automation should play a key role here: by automatically aggregating, de-duping, and ranking threat intel, you can quickly produce a high-fidelity intel feed to inform detection and minimize false positives.

IoCs:
Deploy rules that provide detections based on IoCs, such as bad domains in DNS or proxy traffic and bad hashes in endpoint technologies. Security controls rely on a steady, updated stream of IoCs to maintain efficacy. High-confidence IoCs play a role in detections, but even lower-confidence IoCs can be used in coordination with other criteria. Lower-confidence IoCs can be correlated with lower-confidence behaviors. Another option is alerting on multiple matches to the same IoC, versus alerting on the first identification of that IoC.

Behavioral patterns:
Deploy rules that will catch behaviors known to threat actors—such as using Microsoft Word macros—and keep evolving these associations as attackers refine and pivot their tactics. Threat actors often try to mimic normal activity when they enter an environment, making these threats difficult to mitigate but essential to detect. These lower-confidence actions can be tied together through effective threat intelligence to identify patterns of behavior associated with known actors.

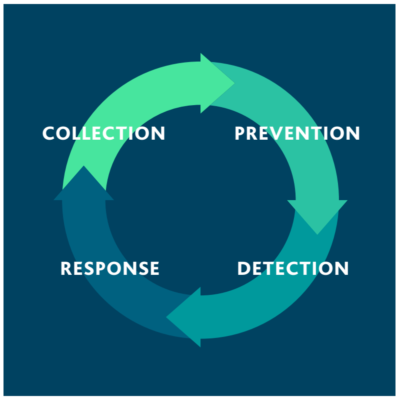
> **“By incorporating high-fidelity, aggregated, and de-duped threat intelligence into your security processes, you can minimize the number of false positives and focus analysts on the threats posing the highest risk to your business.**

STEP 4: RESPONSE

When attacks do occur, security teams want to react with the highest possible confidence. Again, this is where automation should come in: enriching the analysis process with automated information gathering during the investigation allows teams to quickly eradicate threats from the environment.

IoCs:
This process is about enrichment – that is, obtaining data and giving it context to see if it's associated with known threats. For example, if a system is known to have malware, run outbound traffic against IoCs to investigate the potentially malicious systems that the infected system is calling.

Behavioral patterns:
Associate known TTPs to one another, and search for indicators of those behaviors in the environment. One goal of the responder is to recreate the entire attack to ensure it is fully remediated. Using intelligence about the threat actors' full attack chain can provide known behaviors to search before and after detection. This process is closely linked to the IoC process above.



It's important to keep in mind that the processes above aren't just one-time operations.
As teams put the processes into practice, they should reevaluate their methodologies on a regular basis. The threat intelligence implementation processes should be part of an integrated security approach that encompasses threat hunting and validation of controls for effective end-to-end threat mitigation.

> **When attacks do occur, security teams want to react with the highest possible confidence. Automating the analysis process can add speed, so teams can take action faster to eradicate threats from the environment.**

The benefits of maximizing threat intelligence

According to ReliaQuest's *Technology Sprawl Report*, which interviewed more than 400 enterprise security leaders, security teams need new approaches to address the problems of too many intelligence feeds, and too many tools, in ways that decrease organizational risk.[2] Ninety-three percent of enterprise and IT security professionals surveyed said they want better integration and automation of disparate tools; 94 percent said they need better visibility into the results of their security program.

The processes outlined above for optimizing threat intelligence in security programs are intended to address these concerns. When the processes are managed effectively, security teams can minimize risk and reduce the financial and operational impacts of attacks in these ways:

- ✓ Mitigate against compromise
- ✓ Increase detection rates
- ✓ Speed up response times

> **Ultimately, integrating and optimizing threat intelligence across your security program is just one step on a security team's journey toward better visibility, end-to-end automation, and powerful metrics.**

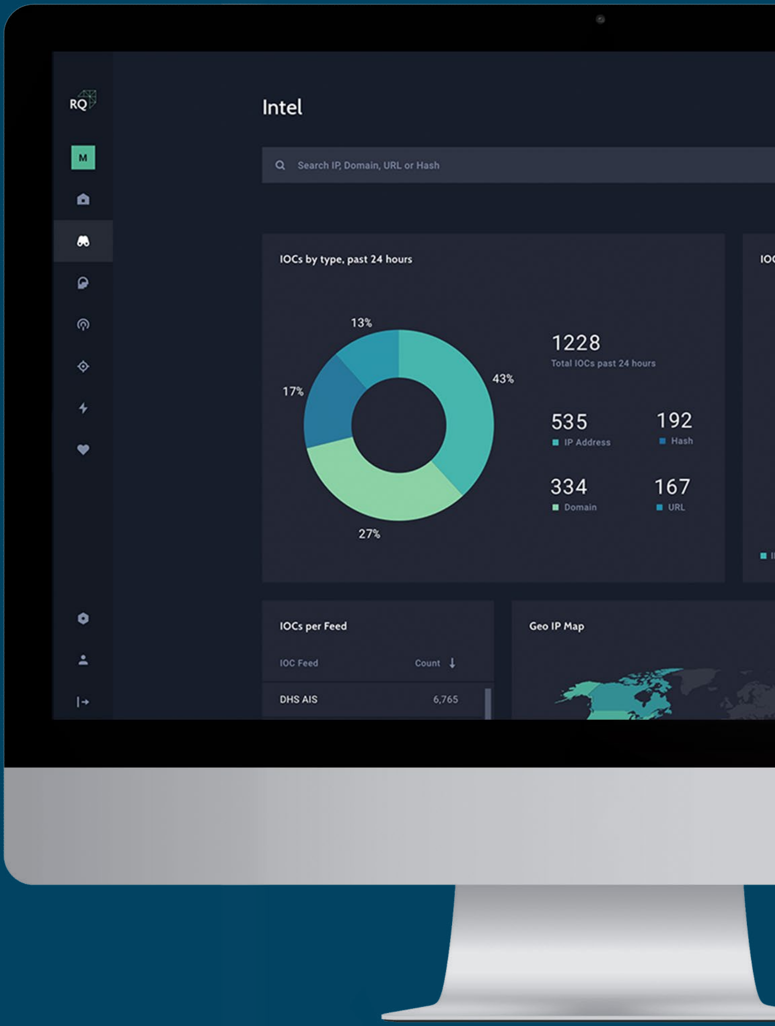
[2] ReliaQuest, *2019 ReliaQuest Technology Sprawl Report*, December 2019: https://www.reliaquest.com/resources/vendor-sprawl-survey-report/

How ReliaQuest GreyMatter Integrates Multi-Feed Threat Intelligence for Comprehensive Coverage

ReliaQuest fortifies the world's most trusted brands against cyber threats with GreyMatter, its SaaS security platform. GreyMatter provides the visibility you need from data across SIEM, EDR, multi-cloud environments, and best-of-breed tools to effectively investigate, remediate, and report with confidence. With full visibility complemented by built-in, customer-validated content and processes, you can confidently automate across investigation, detection, hunting, repair, and response. Improvement comes only with measurement. Benchmarks and models help you to continuously mature your security operations to speed detection and response to better secure and enable your business.

ReliaQuest GreyMatter automatically collects, normalizes, and prioritizes threat intelligence in a consumable format for your SIEM and EDR. ReliaQuest GreyMatter processes all IoCs and only sends those with the highest fidelity, so your security controls report fewer false positives. Customers on average receive over 35,000 new IoCs each week, ensuring up-to-date, relevant intel for comprehensive threat coverage and a 25% average increase in true positives.

LEARN MORE ABOUT RELIAQUEST



IOC Feed	Count ↓
DHS AIS	6,765

> **ReliaQuest GreyMatter provides comprehensive threat intelligence to improve the effectiveness of the security tools you already own, leading to faster threat detection and response with greater visibility across your SIEM, EDR, multi-cloud, and third-party applications.**

RELIAQUEST
Make Security Possible™

☎ (800) 925-2159 www.reliaquest.com info@reliaquest.com