RELIAQUEST

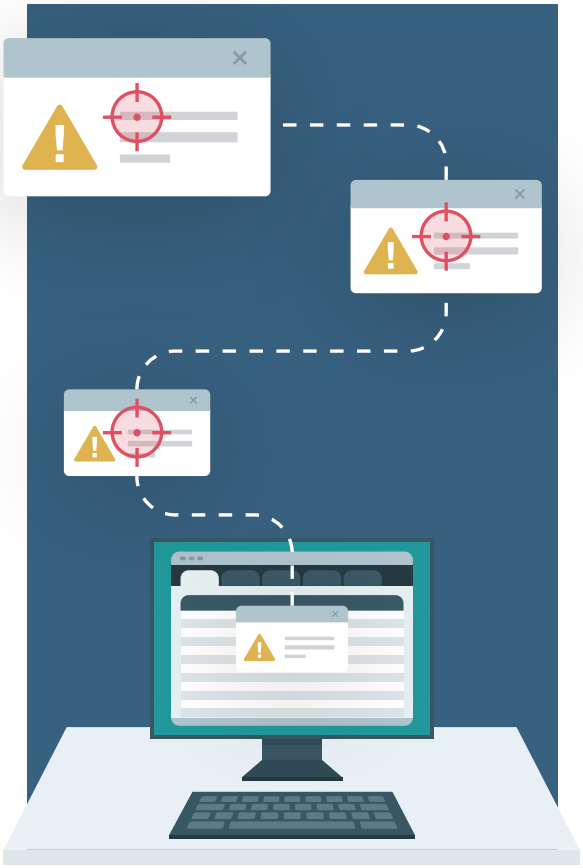
Threat Hunting 101:

A Framework for Building and Maturing a Proactive Threat Hunting Program

How can security teams make threat hunting a reality and transition from a reactive to proactive security stance?

Introduction

Waiting around for attackers to attack is often a fallback posture for overworked and overwhelmed security teams. When attackers show up at the gates, only then will the team kick into action, hopefully (but not always successfully) kicking the bad guys to the sidelines.



When your security team is mostly in reactive mode, your organization is missing out on an opportunity to take out the bad guys before they take you out. The proactive strategy for security should involve threat hunting, your most useful tool for gaining a deeper understanding of where and how attackers have breached or may breach network defenses.

If adopting proactive strategies like threat hunting is new to your security team, it's important to first understand why you might have chosen a reactive posture as your default, instead of how you can hunt for threats. Your team may be in reactive mode because there is simply too much urgent work to do, or because your security tools generate too many false positives.

Your team may also be suffering from "technology sprawl," where you have too many tools that your team must implement, manage, integrate, and pivot between during investigations, taking time away from thinking through the best security approaches. If this is the case, you're in good company: In ReliaQuest's latest survey of enterprise IT and security professionals, 71 percent said they're adding security technologies faster than they're adding the organizational capacity to productively use them.

Additionally, there are common limitations that prevent teams from taking a proactive threat hunting posture. For example, threat hunting requires very large data sets, from which teams can correlate trends, identify security gaps, and find anomalies. A threat hunt involving Windows Authentication traffic could require 30 days of data from 8-10 different Windows event IDs (i.e., 4624, 4625, 4769). It's very time-consuming for teams to manually pull and analyze this data and could take weeks to accomplish – so many may skip the effort.

Threat hunting plays a key role in a proactive security posture. That proactivity comes with real benefits, including a better understanding of your environment so that you can develop baselines and fine-tune higher-fidelity rule logic, leading to more accurate detection methods and strategic decision making. By understanding what steps are needed to build a threat hunting program, when and how to apply automation and threat intelligence, and ways to measure and mature the program, security teams will be better equipped to prioritize threats, and therefore, apply resources more effectively.

In this paper, you'll learn:

WHY threat hunting is necessary to transition organizations away from reactive security postures

WHAT prerequisites a team needs before starting to threat hunt

HOW to conduct threat hunting exercises for maximum impact

> **Threat hunting is an active form of cyber defense that is integrated within day-to-day operations. The goal is to constantly learn, understand, and improve your environment to be able to identify "abnormal" with higher fidelity.**

What is threat hunting?

Threat hunting is an active form of cyber defense that is integrated within day-to-day operations. The goal is to constantly learn, understand, and improve your environment to be able to identify "abnormal" with higher fidelity. By knowing what's normal behavior and activity, the abnormal behavior will stand out.

Threat hunting is a valuable tool for detecting sophisticated attackers who try to fly under the security radar – for example, seeking ways to circumvent static rule logic. In this way, security teams can hunt not just for the "evil" (that is, the sophisticated attackers whose exploits can do the most damage), but also, the vulnerabilities and gaps that help the "evil" attackers gain access. By identifying and mitigating vulnerabilities proactively using threat hunting, security teams can prevent threat actors from taking advantage of these gaps.

The benefits of threat hunting

Threat hunting gives your team a 20,000-foot view of the security environment. Instead of being stuck in the weeds fighting off day-to-day threats, with little insight into which threats may be lurking, the security team knows how attackers operate. With this knowledge, teams can take steps to ensure attackers' best-laid plans don't involve breaching your network.

Threat hunting helps security teams:

- ✓ Gain a better understanding of the security environment
- ✓ Use trending data to learn about the security environment on a more granular level in order to identify higher-severity vulnerabilities
- ✓ Identify more sophisticated attacks
- ✓ Identify hygiene issues such as weak protocols and abnormal usernames
- ✓ Find vulnerabilities in configurations and policies before they become problems
- ✓ Improve static correlation rules based on removing noise that gets in the way of legitimate detection
- ✓ Reduce technology sprawl by identifying priority investments
- ✓ Communicate better across the business, including plans to address up-and-coming threats

Your Security Program: Before and After Threat Hunting

BEFORE		AFTER
Reactive posture: Security teams sift through an influx of false positives and wait until vulnerabilities are exploited.		**Proactive posture:** Security teams identify and eliminate vulnerabilities before attackers can exploit them – reducing risk.
Difficulty identifying abnormal: Without baselines and a true understanding of what normal looks like in an environment, it is challenging and time-consuming to identify abnormal activity.		**Ease in identifying abnormal:** Baselines established through iterative threat hunts make it faster to identify abnormal and improve static correlation rules, prioritize remediation to remove noise, and create rules.
Communication gaps: Identifying hygiene issues, vulnerabilities, and threats is a challenge when the team is purely reactive, making it difficult to confidently communicate a plan of action for remediating vulnerabilities or defending against advanced threats.		**Clear communication:** Teams can offer a more granular understanding of the environment, including whether active, more sophisticated attacks are occurring, and if related vulnerabilities are present; this helps communicate a clear, prioritized plan of action.
Technology sprawl: Organizations invest in unnecessary tools when they're unsure of their greatest vulnerabilities and threats, causing security teams to spend too much time managing technologies and tuning alerts .		**Prioritized technology investments:** When decision makers understand their environment with higher fidelity, they can prioritize technology investments based on a clearly defined attack surface, reducing time spent managing tools and tuning alerts.

Threat hunting categories

Which type of threat hunt should you begin with? When you are first starting to threat hunt, it can be tempting to want to search for malicious right away. However, it's very difficult to identify and understand malicious if you don't know what normal looks like in your environment. That's why we recommend starting with a baselining threat hunt. Once you've established baselines, you can move into behavioral-based hunts with higher fidelity.

Here's a closer look at three categories that threat hunting activities commonly fall into:

Baselining normal vs. abnormal behavior: Baselining, the most common type of threat hunting and suitable for every industry, is a method of reporting on specific aspects of the network to determine what is "normal" in order to be able to identify deviations or "abnormal" activity more efficiently. Baselining is also useful for helping organizations reach security maturity. Once teams know what's normal and they get rid of the noise, they can start up-leveling threat hunting – for example, looking at executive accounts for evidence of compromise.

Retroactive IOC (indicators of compromise) analysis: This involves searching historical data to see if indicators of compromise have been or are currently observed in the environment. For example, if a new critical vulnerability is discovered and a hash is provided as an IOC, security teams would want to search that hash retroactively to determine if the network is affected.

Behavioral-based TTPs (tactics, techniques, and procedures): This type of threat hunting helps identify and analyze advanced persistent threats (APTs), and is also used to profile certain threat actors and outline the path or methods they use to carry out an attack from start to finish.

> **When first starting to threat hunt, it can be tempting to want to search for malicious activity right away. However, you can't identify malicious if you don't understand what normal looks like in your environment. Start with baselining threat hunts to better understand your environment; then you'll be able to identify malicious activity with higher fidelity.**

Before you start: Threat hunting considerations and prerequisites

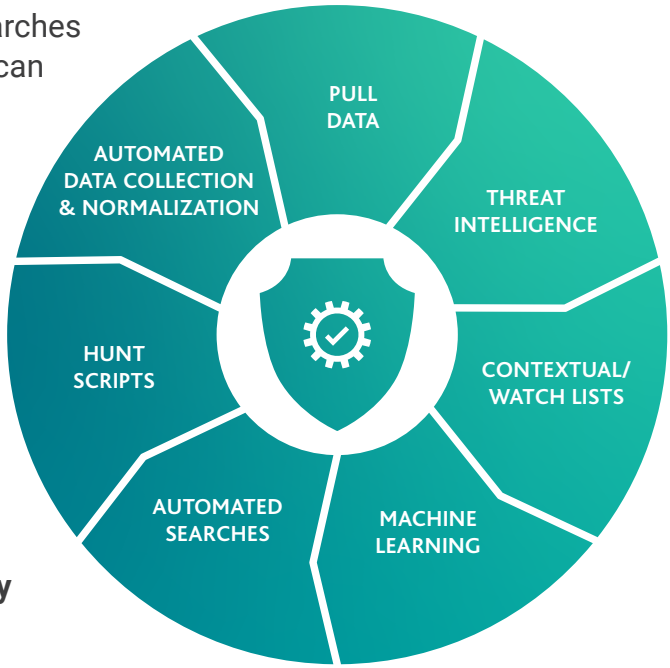
Before your team starts threat hunting, it's important to first consider a few foundational elements, such as your environment, technology requirements, and any buy-in needed to kick off and mature your program. After all, you can't build a threat hunting "house" without a solid "foundation."

YOUR ENVIRONMENT

Consider the various devices in your security environment, as well as their logging levels. Security teams need to ensure that these devices and technologies are logging and parsed sufficiently to allow threat hunters to identify valuable findings. For example, it would be difficult to threat hunt for various indicators present within PowerShell usage if you're not logging command lines within 4688 Windows events (i.e., a new process has been created) or using Endpoint Detection and Response (EDR) to search trending data for PowerShell usage and commands. Teams need to ensure that logging levels for the various log sources used for hunting are reporting logs that are verbose enough and parsed to allow security professionals to hunt efficiently and effectively.

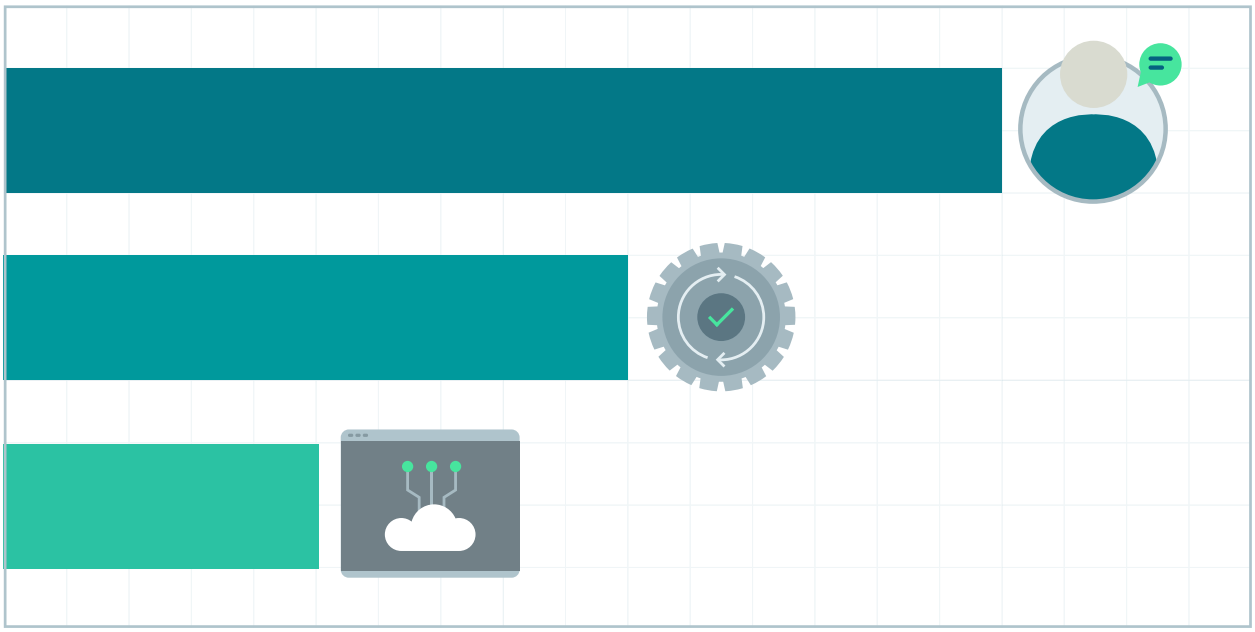
AUTOMATION

Automation is critical for threat-hunting workflows, such as streamlining the data pull and querying process. Searches can be split into individual runs, and security teams can investigate the data live as it's being pulled. Threat hunting data sets commonly utilize multiple log sources where it becomes increasingly important to incorporate a solution to normalize ingested information, such as Elasticsearch. This allows the threat hunter to more efficiently correlate activity from different sources regardless of formatting. Additionally, any type of automated correlation and/or attribution helps. When threat hunting, we know what activity is anomalous and needs further investigation. **If you can automate the identification of these common anomalies via machine learning, then threat hunters can ultimately reach desired end goals much more efficiently.**



BUY-IN

When trying to advance any strategic initiative, it's important to communicate your goals and plan of action in order to get the necessary support. Be sure to communicate your threat hunting program's goals to leadership, as well as the team that will be performing the threat hunts. For instance, your program's goal could be to identify sophisticated threats that circumvent traditional rule logic, such as low and slow brute force attacks. In this case, your plan of action would be to patch vulnerabilities and reduce "noise" from poor security practices in order to better understand your environment, fine-tune your rule logic, and ultimately detect sophisticated threats easier. Be sure to track your program's outcomes by tailoring your reporting to both a technical and non-technical audience.



Five steps to building a threat hunting program

Since baselining is the most common type of threat hunting, we'll use it in our example on the following pages to walk through a typical threat hunting exercise involving Windows authentication traffic.

STEP 1:
Define your mission.

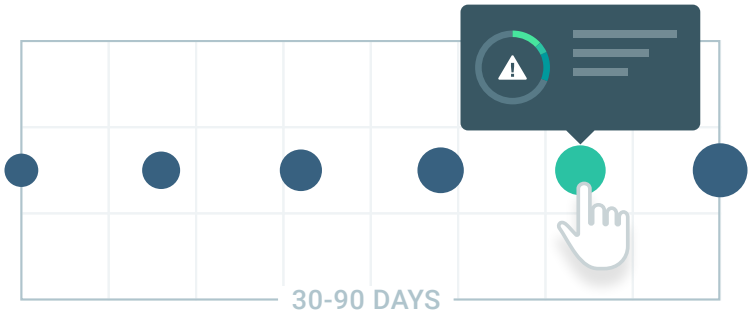
After deciding the types of hunt campaigns you'll run, the next question is: What is your mission or goal? Without a defined mission, you're just monitoring. Think of defining a mission like making a grocery list; when you go to a grocery store with a predefined list, you get your shopping done more efficiently. Creating and defining threat hunt use cases and structured processes for retroactive IOC hunting are essential to a successful threat hunting program.

ReliaQuest provides guidance on where and how to begin the hunt, including established objectives to search for, in the Threat Hunting Use Case blog series. In the hypothetical case below, we're conducting threat hunting for an organization moving to remote work and seeking to understand security weaknesses involving employees logging into enterprise networks via Windows authentication.

STEP 2:
Use trending data over time.

Threat hunters should use trending data during campaigns to identify the vulnerabilities or security gaps that lead to successful exploits. In our Windows authentication example, using trending data allows the security team to identify more sophisticated "low and slow" MITRE ATT&CK framework attacks such as Brute Force (T1110) and Kerberoasting (T1558). In addition, teams should use trending data to assist in identifying larger-scale misconfigurations or poor security practices such as weak NT LAN Manager (NTLM) protocol usage or weak Kerberos encryption usage (RC4/DES).

To generate the most useful insights from data, use larger data sets as well as data sets from multiple sources. Longer time periods are also helpful: A 30-day data set isn't useful enough. Sophisticated attacks and larger-scale misconfigurations are more accurately identified when using trending data for longer periods of time, so security teams can compare daily, weekly, and monthly trends. Machine learning can accelerate this process, identifying abnormal behavior faster and prioritizing behavior based on impact to the business.



For example, if threat actors have been in the environment intentionally running low and slow attacks, it would be almost impossible to identify them if security teams use fewer than 30 days of data. Larger amounts of trending data allow teams to identify the top offenders using outdated authentication protocols (such as NTLM), or hosts bypassing internal DNS servers – and in these cases, to prioritize configurations accordingly to mitigate vulnerabilities.

> **To generate the most useful insights, use trending threat hunt data over extended time periods, usually 30-90 days. This allows security teams to compare daily, weekly, and monthly trends to better identify sophisticated attacks and larger misconfigurations.**

3

STEP 3:
Design threat hunts to be iterative.

A hunt campaign is never a one-and-done deal. Threat hunting should be iterative: Security teams should constantly track findings and improvements. With a list of action items, the security team can undertake a more granular iteration of the hunt after clearing out the noise.

In our example of a Windows authentication hygiene hunt, security teams can build on their discoveries from the data-examination step above. For example, if teams

identify large-scale NTLM weak-protocol usage, trending authentication failures, or weak Kerberos encryptions (RC4/DES), they can work to identify outliers in terms of event count to improve security practices. Focusing on the "top offenders" in terms of the services using these protocols is the most efficient way to make the largest, most rapid impact on the security environment.

Over time, using the same query to pull data after security changes are implemented, teams can see progress toward improving authentication practices, while creating a baseline to learn the new normal. With automated processes, teams can set up queries to run automatically overnight, so the results are ready the next day for analysis. The iterative process also removes some of the noise that clouds the ability to identify actual attacks.

In our Windows authentication sample hunt, the next iteration after monitoring for new baselines could be looking for threats such as pass-the-hash attacks or Kerberoasting. Initial hunts are used to baseline and remove noise that gets in the way of accurately identifying malicious activity. For example, if the normal encryption protocol for Kerberos is weaker (RC4/DES) then it would be almost impossible to identify Kerberoasting. The goal is to identify these practices, improve them, and move towards searching for what would now be "abnormal." This is akin to a pirate following a map with 50,000 locations that might have treasure; proper research helps reduce the list of islands to as few as possible that need searching.

STEP 4:
Conduct hunts that facilitate a better understanding of your environment.

Threat hunting is not just about looking for "evil," or the bad guys – it's also about hygiene. According to Security Boulevard, 60% of breaches in 2019 involved vulnerabilities where patches were available but not applied. There are significant benefits in identifying and correcting security hygiene issues, such as unpatched vulnerabilities, misconfigured firewall rules, applications, and scripts.

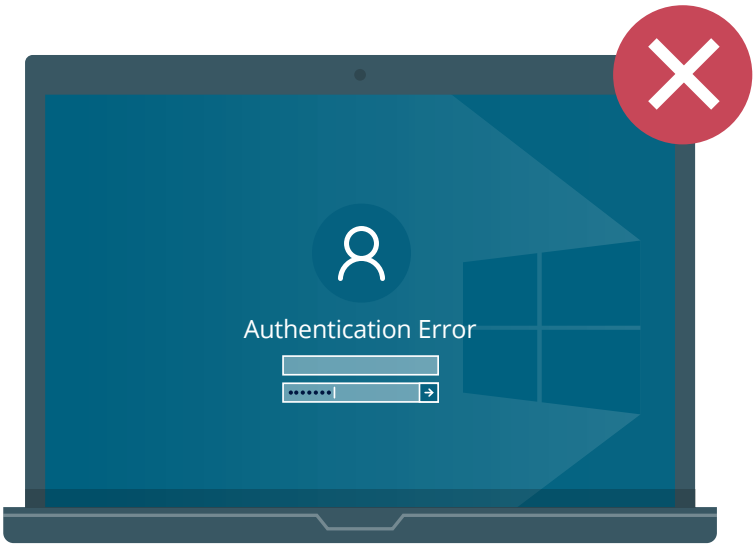
In our Windows authentication threat hunt, we can create baselines for several areas of activity that could assist in future threat hunting:

Abnormal usernames:
Confirm usage of approved naming conventions for user accounts and hosts in the environment to identify anomalous usernames and hostnames.

Weak/deprecated protocol usage:
Search for weak or deprecated protocol usage, such as RC4 or DES algorithms within Kerberos authentications, and identify a baseline for NTLM usage. NTLM is an outdated authentication protocol that's susceptible to offline brute force attacks or replay attacks. Some servers or services may use NTLM by default – in these cases, security teams must manually configure more secure protocols. (Even if older servers need to use NTLM, security teams should still ensure NTLM v2 is being used as opposed to v1, and ensure those servers are segmented on the network.)

Privileged account usage:
Visualize "special privileges assigned to new logon" authentication events using event ID 4672 to establish a baseline of the number of attempts for your accounts with administrative privileges.

Threat hunting is not just about looking for "evil," or the bad guys – it's also about hygiene. There are significant benefits in identifying and correcting security hygiene issues, such as unpatched vulnerabilities, misconfigured firewall rules, applications, and scripts.



Authentication failure:
Examine trending authentication failures to establish a baseline of average failed authentications, so the team can then identify deviations or anomalies.

Logging gaps:
Ensure all relevant Windows event logs are generating at proper logging levels to correlate potentially malicious activity.

5

STEP 5:

Augment gaps left by static correlation.

Savvy attackers are always on the lookout for static correlations that are in place in the security environment and will work to circumvent detection. Threat hunting helps identify gaps in static correlation, so you can quickly close the open doors to attackers. Ensure that proper logging levels and reporting are in place to constantly monitor threat hunt outcomes and baselines.

In our Windows authentication example, we've already worked to eliminate noise that could prevent the detection of actual malicious activity, while we concurrently develop a baseline of our environment. This groundwork allows us to take advantage of our threat hunting outcomes to create higher fidelity static correlation rules. For example, we could create a correlation rule to detect a weakness to Kerberoasting (RC4/DES). The benefit of this approach is generating higher fidelity around the data so that security teams can trust what they're seeing, and know where and how they must take action.

LEARN MORE:
Check out ReliaQuest's **Threat Hunting Use Case Blog Series** for more threat hunting use case examples.

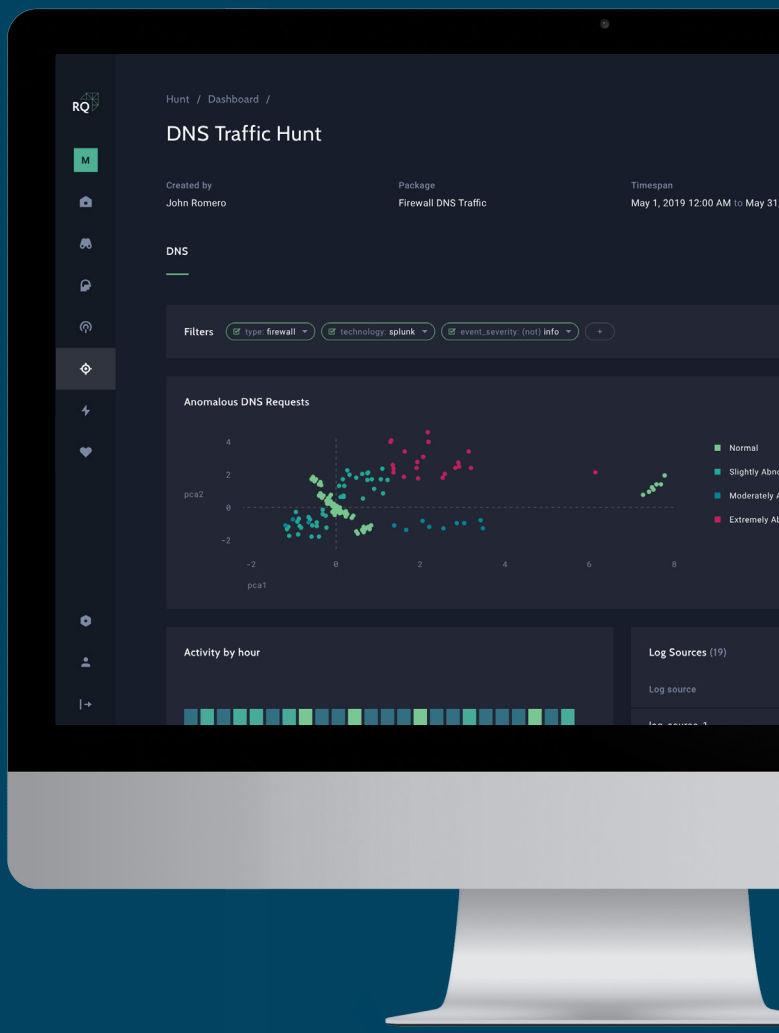
The threat hunting roadmap for maturity

Organizations seeking to build maturity into threat operations can use threat hunting as a tool to show C-suite leaders and boards that the business is indeed seeing ROI for security investments. Threat hunting lends itself to relevant and easily understood metrics. For example, security teams can report on the number of threat hunts conducted each quarter as well as the amount of the environment reviewed in each threat hunt, and how these numbers translate back to the percentage of the environment reviewed. These clearly defined metrics explain what security teams have accomplished, and provide a roadmap for future.

Your plan of action:

- Set up your foundation. Obtain buy-in, understand your environment, and consider what technology or automations you can implement to make your threat hunts more effective.
- Start with baselining threat hunts to better understand normal; then you can look for malicious activity with higher fidelity.
- Begin all your threat hunts with a goal or mission and repeat these frequently.
- Close gaps left by static correlation by tuning rules or identifying priority technology integrations.
- Measure and report on the success of your threat hunts so you continuously mature your program.

Automated Threat Hunting with ReliaQuest GreyMatter



ReliaQuest, a global leader in cybersecurity, delivers industry-leading visibility and automation on demand across complex environments with a platform purpose-built to protect organizations from security breaches. GreyMatter is the first cloud-native SaaS solution that integrates and improves an enterprise's on premise and multi-cloud technologies, unlocking the power of next generation cybersecurity. By increasing visibility through the platform's proprietary universal translator and use of automation and artificial intelligence, GreyMatter saves security teams valuable time and increases effectiveness by enabling automatic and continuous threat detection, threat hunting, and remediation.

By aggregating and normalizing your data from disparate tools, such as SIEM, EDR, multi-cloud, and third-party applications, ReliaQuest GreyMatter allows your team to run focused hunt campaigns, both packaged and freeform, that are strategic and iterative.

Use ReliaQuest GreyMatter to analyze indicators of compromise retrospectively or perform behavior assessments to visualize abnormal from normal activity. Pre-built threat hunting packages automatically gather and analyze data without performance impact while proactively finding threats.

By aggregating and normalizing your data from disparate tools, such as SIEM, EDR, multi-cloud, and third-party applications, ReliaQuest GreyMatter allows your team to run focused hunt campaigns, both packaged and freeform, that are strategic and iterative.

LEARN MORE ABOUT RELIAQUEST GREYMATTER

RELIAQUEST

Make Security Possible™

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