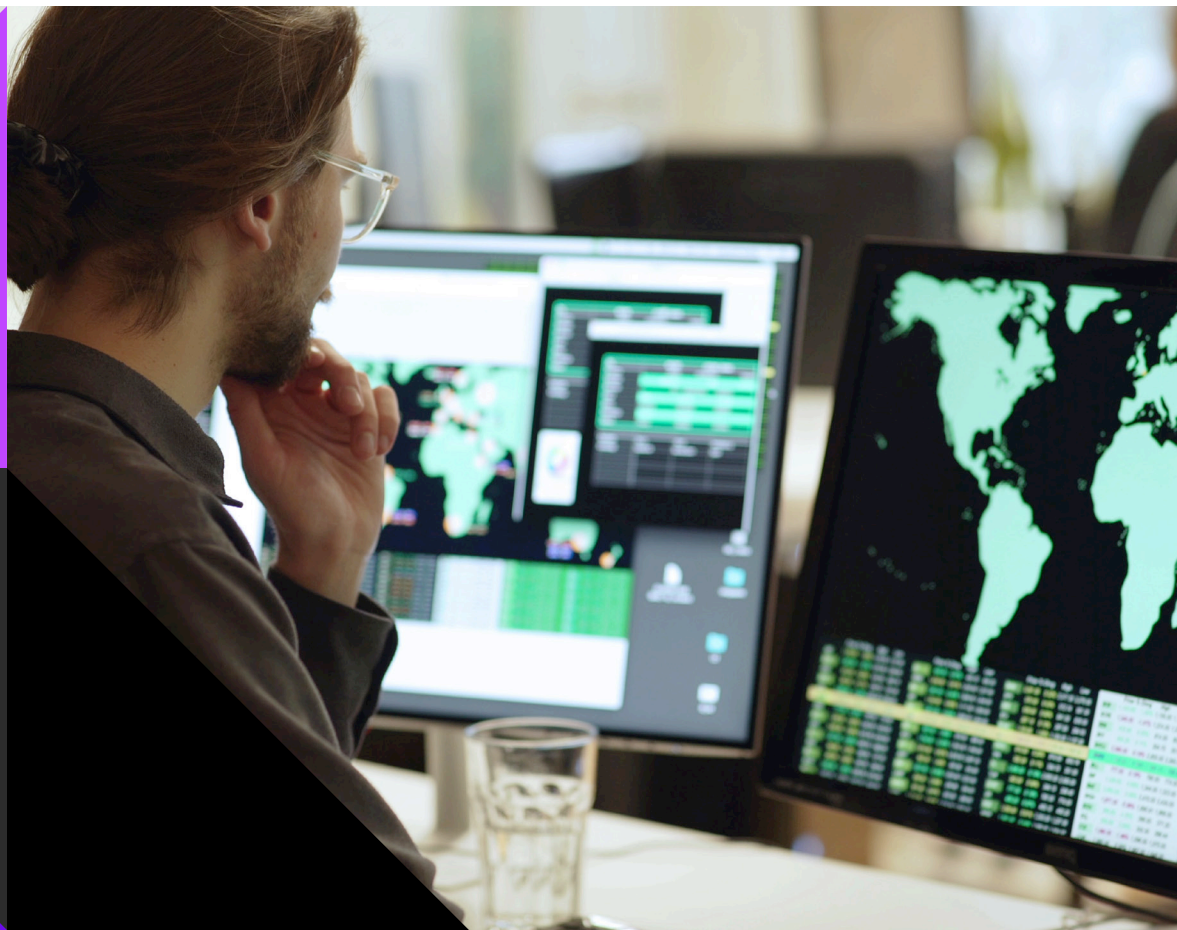
N-ABLE™

# How to develop a successful threat-hunting program

## eBook



# Introduction

The average attack "dwell time", the period between an attacker's breach of an organization's network and the point at which the organization finds out about it, is 287 days.[1] During this time, the attacker can stealthily look to gather valuable information to steal or data to compromise, incurring huge costs for affected companies. Generally, the longer the dwell time, the higher the costs. According to the 2021 Cost of Data Breach report, a breach with a lifecycle over 200 days cost an average of $4.87 million versus $3.61 million for a breach less than 200 days.

**200+ DAYS** | AVERAGE OF **$4.87 million**

**-200 DAYS** | AVERAGE OF **$3.61 million**

As an MSP or MSSP, imagine you're taking on a new customer. Do you have the right security tools and practices in place to detect and mitigate stealthy threats lurking in their environments? Or to prevent these threats from ever breaching their networks? Waiting until threats become visible or for traditional SOC monitoring tools to generate an alert can be too late. Threat hunting is a more proactive cybersecurity approach to identify threats that evade security controls before they can execute an attack or fulfill their goals.

## What is threat hunting and why do you need it?

Threat hunting is the process of searching for suspicious behavior across the entire attack surface. It is hypothesis-driven and requires an expert understanding of the expected architecture, system, application, and network behavior in order to ask targeted questions that help uncover unexpected behavior and outliers such as lateral movement or known tactics, techniques, and procedures (TTPs) that attackers use.

Simply put, threat hunting works from the premise that an attacker is already in the environment. Given its proactive nature, it effectively reduces damage and overall risk to an organization, enabling security professionals to respond to incidents more rapidly than would otherwise be possible.

# Six best practices to creating successful threat-hunting program

To be efficient, threat hunting needs an iterative combination of processes, tools, and techniques that are continually evolving and able to adapt to your organization—which can prove challenging, especially for MSPs or MSSPs who are just starting to build out their threat-hunting program.

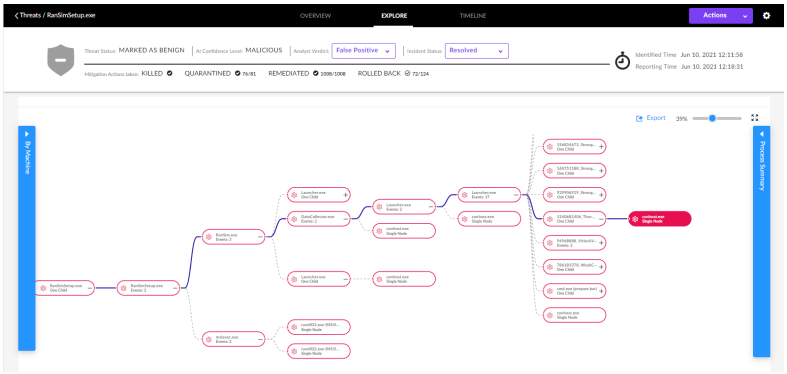
Typically, threat hunting starts with a hypothesis of what threats might be in the environment, continues with an investigation of the potential threats, and, in case the investigation confirms the hypothesis, the process ends with effective threat response and remediation of changes or damage caused.

In what follows, we'll look at six best practices that will help you build a successful threat-hunting program.

## 1. Get the right data in the right context

Having the right data to answer the right threat-related questions is key to successful threat hunting. Because your threat hunting efforts will be based on endpoint telemetry, that data needs to be comprehensive and put in the right context. Endpoint telemetry needs to capture a wide range of activity and behaviors spanning multiple operating systems, including network traffic patterns, network activity, user activity, file hashes, file operations, system and event logs, denied connections, peripheral device activity, and more. And all of the data points and different events need to be correlated so as to better understand the context of the potential threat.

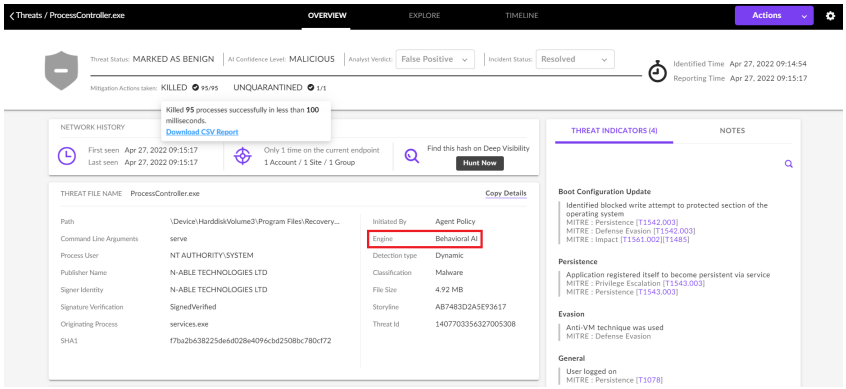
N-able EDR with Threat Hunting powered by SentinelOne® provides analysts with real-time actionable correlation and context and helps them understand the full story of what happened in the environment. It automatically correlates related activity into unified alerts, which helps reduce alert fatigue and the time and effort required to respond.




## 2. Understand what's normal in your environment

Understanding what's normal within your environment is also critical. Threat hunters need to have a good understanding of the company's profile, employee behavior, company valuable data, as well as business activities that could be of interest to attackers, so that they can baseline what is "normal". Knowing what is normal, they can look at the data points available and start asking questions that help identify any outliers.

N-able EDR's behavioral AI detection engine uses advanced data science methods to teach systems the difference between regular operations and malicious behavior. If a pattern emerges, an alert is triggered; for example, repeated login attempts from a country that are not the usual norm may indicate a potential brute force attack. This helps make threat detection and hunting faster and more accurate.




## 3. Develop threat hypotheses

Okay, so you have the right data and you've baselined what is normal behavior within your environment. How do you start hunting for threats? The answer depends on whether the threat is known or unknown.

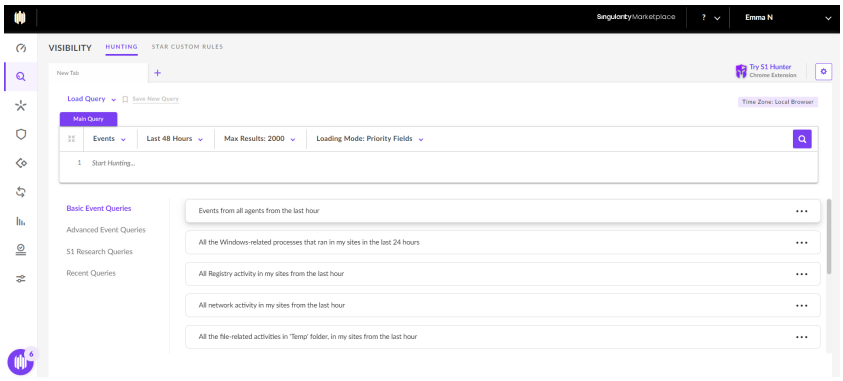
To hunt for known threats, you can start from looking at various intelligence sources that use Indicators of Compromise (IoCs), hash values, IP addresses, domain names, network and host artifacts such as Information Sharing and Analysis Center (ISAC) or the FBI. However, there are many unknown threats constantly being development and used in attacks. So, threat hunting can't rely only on known sources and methodologies.

For unknown threats, you can first create hypotheses about activities that might be taking place within the environment and then test them. You can start by asking questions such as: "If I were to attack this environment, what would I attempt to gain access to? Why do I see an abnormal volume of DNS queries from a single machine?" More ideas can be derived from tools and frameworks like the MITRE ATT&CK® framework, threat intelligence based on real incidents, information about new attack techniques appearing for the first time via social media, research blogs, conferences, penetration-testing practices, and past experiences.

N-able EDR with Threat Hunting powered by SentinelOne® lets you quickly and iteratively query and pivot across endpoint telemetry captured from endpoint devices to validate hypotheses. It then automatically correlates related objects (processes, files, threads, events, and more) of a threat. For example, a process modifies a different process by injecting code. When you run a query, all interaction between the source process, target process, and parent process shows clearly in the cross-process details. This helps you quickly understand the data relationships: the root cause behind a threat with its context, relationships, and activities. Analysts can also leverage historical data to map advanced threat campaigns across time to enable efficient hypothesis generation.

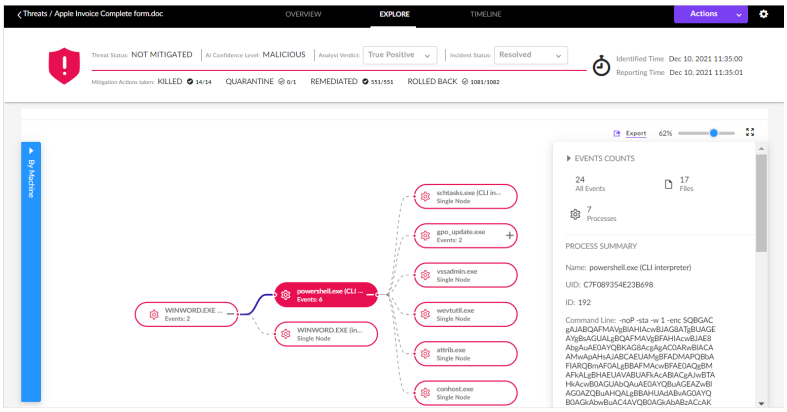
You can create powerful hunting queries with easy-to-use shortcuts. As a threat hunter, the MITRE ATT&CK framework has likely become one of your go-to tools. N-able helps make hunting for MITRE ATT&CK Tactics, Techniques, and Procedures (TTPs) fast and painless. It's as easy as entering the MITRE technique ID and using this to perform a hunt.

You can also leverage the query library of hunts that uses data from various open, commercial, and bespoke sources curated by SentinelOne® research. These hunts are the output of hypotheses that are proven across research data and are generic. For example, the use of unmanaged, unsigned Powershell is likely abnormal in most environments; and would commonly require additional investigation. Both examples are not malicious in and of themselves but fit in a hunting workflow, as they are descriptive of anomalies.




## 4. Investigate potential threats

If the hypothesis you create is correct and you find evidence of malicious activity, then you need to immediately validate the nature, scope, and impact of the finding. This is where threat investigation tools come in handy. The next step in the process is to identify new malicious patterns in the data and uncover the attacker's TTPs (Tactics, Techniques, and Procedures).

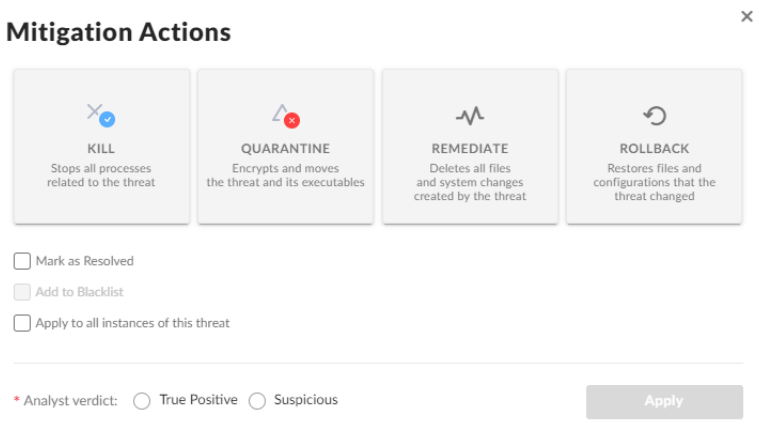



N-able EDR with Threat Hunting comes with Storyline™, a feature that enables rapid threat hunting. Each autonomous agent monitors endpoint activity and its real-time running behavior. A Storyline ID is an ID given to a group of related events in this model. When you find an abnormal event that seems relevant, use the Storyline ID to quickly find all related processes, files, threads, events, and other data with a single query. This way, you'll be able to understand the full story of what happened on an endpoint, see the complete chain of events, and save threat investigation time.

## 5. Respond effectively

Once you identify a new TTP, you need to "stop the bleeding"—effectively respond and remediate the threat. What this means is you need to not only take immediate measures to neutralize the attack and prevent it from damaging the system, but to also take measures to prevent similar future attacks. In other words, you want to expand scope of remediation beyond just responding to the threat of today but preventing the threats of tomorrow.

N-able EDR with Threat Hunting helps analysts to take the required actions needed to respond and remediate the threat with a single click. With one click, the analyst can roll back the threat or perform any other available mitigation actions. The rollback functionality automatically restores deleted or corrupted files caused by ransomware activity to their pre-infected state without needing to reimage the machine. The threat can be added to Exclusions, marked as resolved, and notes can be added to explain the rationale behind the decisions taken.

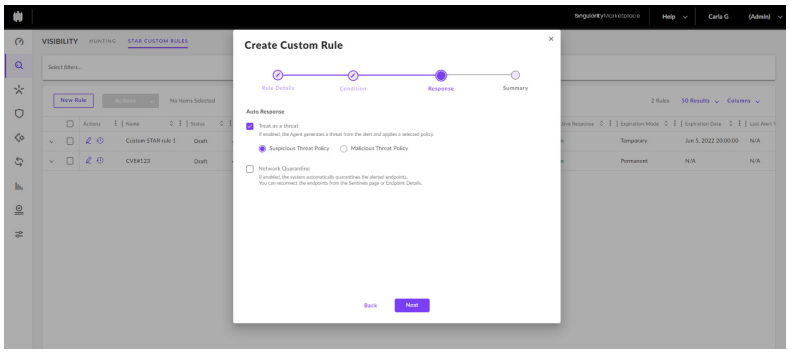



N-able EDR also can detect threats in advance through the aid of its machine learning and intelligent automation. It can anticipate threats and attacks by deeply inspecting files, documents, emails, credentials, browsers, payloads, and memory storage. It can automatically disconnect a device from a network when it identifies a possible security threat or attack.

## 6. Enhance your global security

One final step is to inform and enrich automated analytics with insights from successful hunts. This enables you to use the knowledge generated from threat hunting to improve EDR systems, which helps enhance and consolidate the security or your organization, globally.

N-able EDR with Threat Hunting provides a Storyline Active Response™ (STAR) custom detection rules capability. STAR helps you turn queries into automated hunting rules. STAR rules trigger alerts and responses when rules detect matches and gives you the flexibility to create custom alerts specific to your environment that can enhance alerting and triaging of events.




Alerts are triggered in near-real-time and show in the Activity log in the Management Console. After running the hunting query, you can select a response for the rule to automatically mitigate the rule detections. With that, you can automatically protect your environment from threats, according to your needs.

## Looking ahead

While building a threat-hunting program is no easy feat, it is worth it. The good news is that you do have advanced security solutions at your disposal to easily search for suspicious behavior throughout your network and automate the threat-hunting process as well as the remediation of damage.

According to a SANS 2021 survey,[3] organizations that implement a threat hunting program see a 10% to 25% improvement in their overall security posture from threat hunting. More specifically, some of the benefits they get from threat hunting are faster incident response times, less work for the security techs, and a reinforced SOC, better equipped to protect against rising threats.

As an MSP or MSSP, running a threat hunting operation can help improve your level of service, keep customers better protected, and scale your business.

Ready to start your own threat hunting program?

**For more information on security technologies to help you secure your business, visit n-able.com.**



Footenotes:

[1, 2] 2021 Cost of a Data Breach Report, Ponemon

[3] A SANS 2021 Survey: Threat Hunting in Uncertain Times