Autonomous Threat Hunting.

Drives down false positives with high levels of accuracy.

Addresses an urgent and critical problem.

In today's world, you have to assume that external attackers are already present inside your organization's network. Cyber threats range from commodity malware and ransomware to persistent and targeted threat actors. It is imperative that these threats are detected quickly to help reduce the risk of valuable business assets being compromised. Organizations are struggling with this challenge in the face of a daunting information security talent shortage. Verizon Autonomous Threat Hunting is a tool designed to provide an accurate and comprehensive security monitoring solution to this most critical problem: identifying potentially infected or compromised machines in your organization's network.

Autonomous Threat Hunting offers an automated, end-to-end, threat hunting solution. It applies advanced data science concepts and machine learning technologies which automate many of the tasks human analysts conduct when threat hunting. To detect potential threats, it automatically reviews historical logs against threat data refreshed daily and proactively searches for non-obvious threats. Autonomous Threat Hunting transforms gigabytes of logs, multiple threat intelligence feeds and varied raw indicators into a timely, manageable, prioritized list of high-quality alerts.

High levels of accuracy and catch rate.

Autonomous Threat Hunting eliminates a significant number of false positives and irrelevant alerts with high levels of accuracy. Many of the alerts generated represent novel threats identified by our patented supervised machine learning models' extrapolation of existing threats. This helps Autonomous Threat Hunting to detect unknown threats that may have gone previously undetected by an organization's existing security technologies.

Beyond this stellar performance, the system captures analyst feedback to help elevate accuracy over time, including training the models to identify attributes specific to each customer's compute environment.

Leverage existing investments.

Autonomous Threat Hunting offers out-of-the-box integration with several SIEM, log management, incident response and other security and IT tools and platforms. A REST API facilitates tailored integration into many environments and workflows, including proprietary and legacy technologies.

Autonomous Threat Hunting exposes novel threats that may evade other defenses, and mitigates false positives that consume scarce security personnel resources.
Autonomous Threat Hunting: How it works.

Autonomous Threat Hunting uses a combination of supervised machine learning techniques to mimic the decisions made by an extremely talented security analyst.

Our solution performs the hunting process autonomously and at scale. When a human analyst comes into play, he or she will typically be focused on high-confidence and pre-qualified investigation leads. This helps your organization to reduce valuable analyst time spent on the costly, mind-numbing, and repetitive task of sorting through irrelevant alerts and false positives.

Plus, by providing full contextual information with each lead, analysts can hit the ground running on their investigation and containment efforts.

An innovative system within the industry.

Verizon Autonomous Threat Hunting is an automated end-to-end solution for cyber threat hunting from collection to operational use. It performs many tasks typically performed by security analysts with speed, economy, objectivity, and scale. Furthermore, it:

- Helps to efficiently utilize your security team’s capabilities.
- Automatically hunts and reviews historical logs against threat data refreshed daily.
- Uses patented supervised machine learning technology to detect truly novel threats and mimic the decisions made by an extremely talented analyst. Eliminates a significant number of time-consuming, irrelevant alerts.
- Can be integrated with your existing SIEM or log management solution.
- Takes only minutes to set up and requires no agents, appliances, customization, or professional services.

Why Verizon Enterprise?

We have over twenty-five years of industry experience. In 2018, Verizon is named by Gartner as a Leader in the Magic Quadrant for Network Services, Global, and Magic Quadrant for Managed Security Services, Worldwide. We also have one of the largest IP networks in the world which gives us great visibility into security events.

If you are unsure where to start, we at Verizon Enterprise would be happy to help.