Autonomous Threat Hunting.

verizon

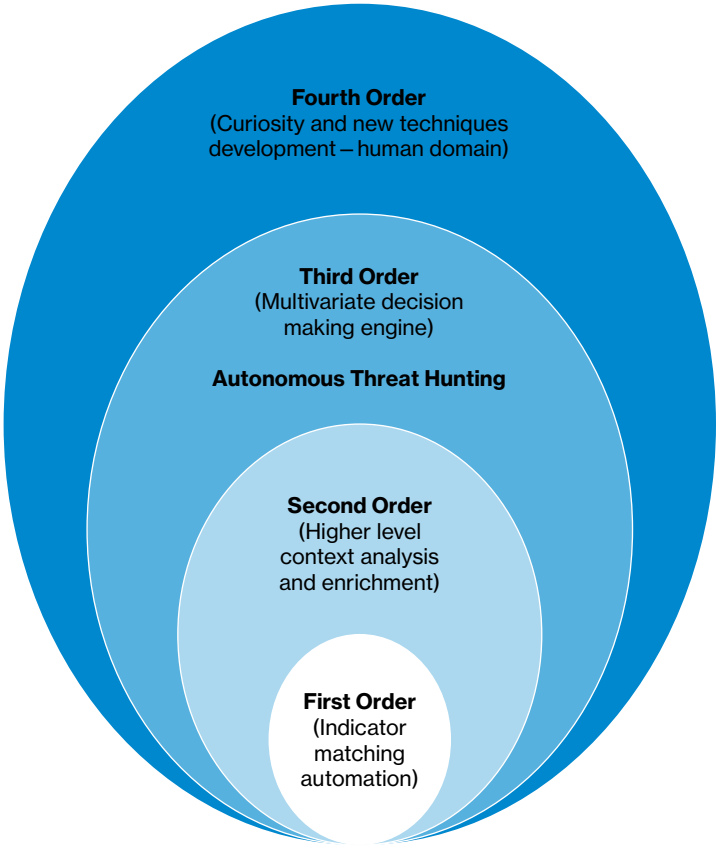
Threat Hunting Automation Maturity Model.

The discussion around "automation" in cyber threat hunting is usually defined as something tautological. The definition of threat hunting in several circles accounts for "human activity to find badness that the automated products missed". The issue with this definition is that according to it, as soon as something is automated, it ceases to be threat hunting.

This argument is rooted in the belief that the only kind of automation that exists is "signature-based" or similarly simplistic forms of rule-based automation. As per this view, humans would use intuition and knowledge to learn from the existing signatures and unusual markers in an organization's log data to supplement a static signature matching approach.

It seems obvious that a signature-based strategy does not scale with the fast and growing number of today's threats, so the idea of doing something "smarter" to complement is a good one. However, computer science is long past the point at which it was believed that humans alone could learn from experience to make complex multivariate decisions with sustained accuracy.

Here are the four distinct levels of the Threat Hunting Automation Maturity Model which explain the various automated activities:



First Order: Indicator matching automation.

The vast majority of hunting automation solutions belongs in this tier. It mostly made up by signature matching, such as matching a list of file hashes to the processes running on a machine, or an IP address search on network logs. However, this is an incomplete approach, and both prone to extensive false positives present in badly vetted lists and false negatives because those records will naturally be incomplete.

Second Order: Higher level context analysis and enrichment.

A solution in this tier is capable of calculating statistical summaries and other context-based enrichments to give additional information to a threat hunting analyst. One example of this would be to evaluate individual hunting pivoting points such as what data center an IP address is hosted at, or a domain's WHOIS information. By assessing them, you can assign a maliciousness level based on how many malicious and benign samples the system came across aggregated by the pivoting point. A system can then single out all the entries that are related to the high maliciousness pivoting points, and even provide context information to what they are linked to based on the connections to known malicious samples.

Third Order: Multivariate decision making engine.

The challenge of this tier centers on the aggregated experience done by a human analyst. Out of the First Order and Second Order matches or evaluations associated with a group of logs or events, how do we prioritize which one of those are the most relevant? Most SIEMs and security analytics tools will try to achieve that via a scoring or weighting engine. However, these do not take a particular input or a specific customer condition into consideration and have little re-configurability or transparency on how to tweak them. A system operating in the Third Order would be able to decide which variables described as First Order or Second Order are the most relevant to determine how to prioritize an incident. Purposefully designed supervised machine learning models are a natural fit for developing Third Order engines.

Fourth Order: Curiosity and new techniques development.

For automation at this level, a system would evaluate failures or successes from human feedback to make the system decide to add new First Order matching capabilities or figure out new Second Order context or statistical analysis to aggregate new capabilities to a Third Order engine. The system would be actively looking for new kinds of data to analyze based on what it has available. That would be analogous to writing a new playbook for a threat hunting team in response to a newly uncovered threat, and we firmly believe that this tier is exclusive to the human domain as of now.

Confusion in the market.

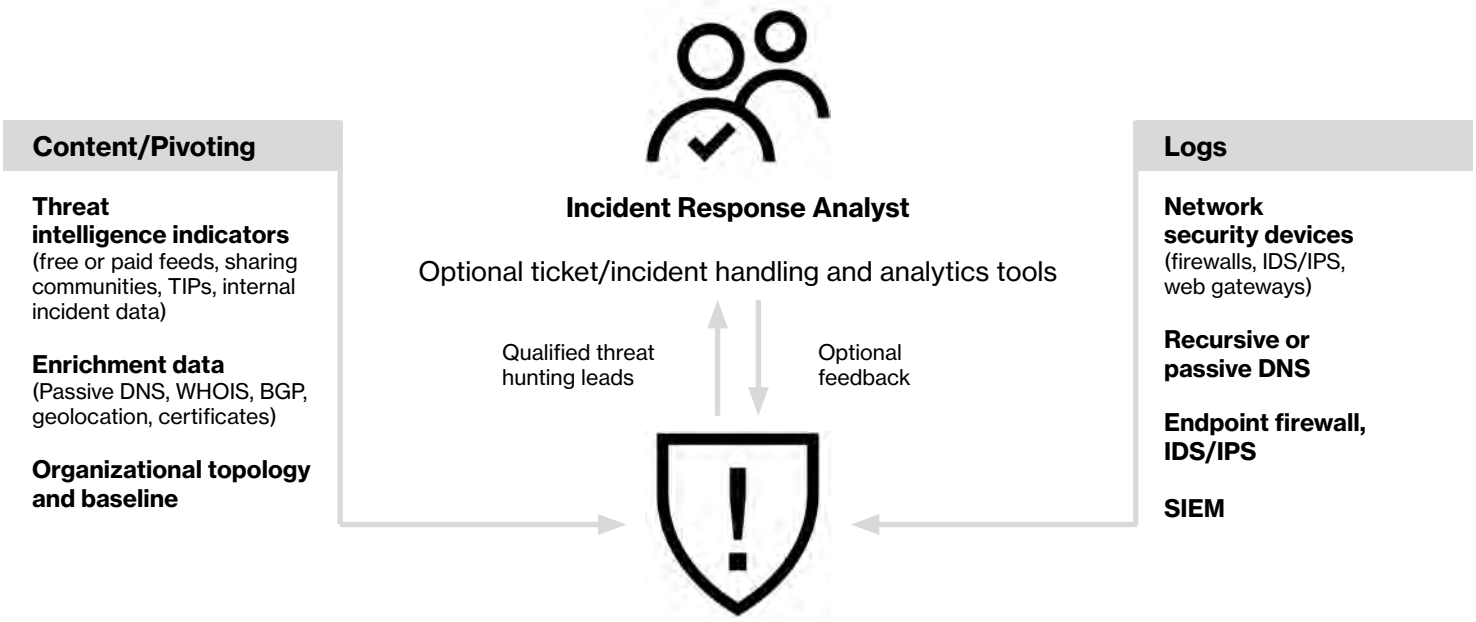
A lot of the frustration in the market place stems from the fact that marketing materials often times advertise Artificial Intelligence (AI) capabilities that seem as magical as the Fourth Order described above, while in reality they may barely deliver First Order results.

Verizon Autonomous Threat Hunting.

Autonomous Threat Hunting implements the functionalities of the First, Second, and Third Orders of this maturity model for end-to-end cyber threat hunting automation.

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 environment and workflows, including proprietary and legacy technologies.

Autonomous Threat Hunting: How it works.



Why Verizon Enterprise?

We have over twenty years of industry experience and 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.