ThreatWatch Hunt

Advanced Threat Hunting Service

Do you know if you've been hacked? Can you identify threats that don't use known malware or indicators of compromise like "fileless" attacks that leave no files or malicious tools on a hard drive?

These are questions that keep IT security professionals up at night. With an average dwell time of 197 days and an additional 69 days to contain the breach (IBM 2018 Cost of Data Breach study), attackers have ample opportunity to plan and carry out the theft of intellectual property, customer data, and other valuable information. Each additional day it takes to identify and contain a threat provides opportunities for the attackers to access more records and a greater negative impact on your brand.

The purpose of threat hunting is to reduce dwell time, the time between a breach and its discovery. Shortening that time can make the difference between spending a few thousand dollars on remediation and millions to deal with a full-on compromise.

What is Proactive Threat Hunting?

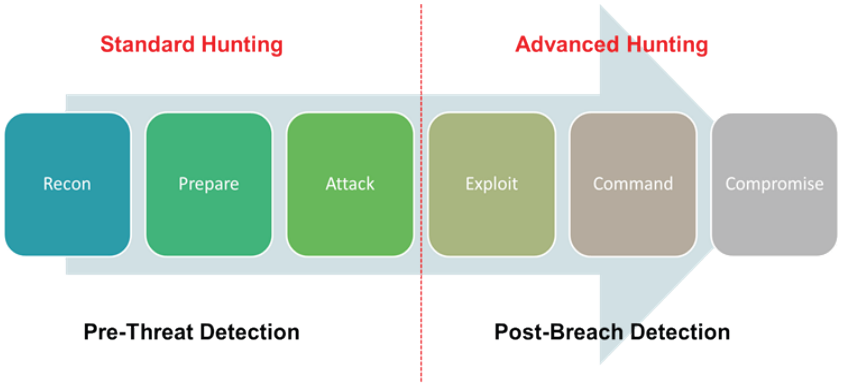
Proactive Threat Hunting requires toolsets and technology beyond what normal Security Operations maintain to perform their day-to-day threat monitoring and triage activities. When proactive methods and technologies are used, it can reduce false positives, enhance the accuracy, and speed positive confirmation of threat analysis/response activities in the SOC.

Time To Detect Business Impact

Companies that identified a breach in less than 100 days saved more than $1 million as compared to those that took more than 100 days. Similarly, companies that took contained a breach in less than 30 days saved over $1 million as compared to those that took more than 30 days to resolve.

IBM 2018 Cost of Data Breach Study.

Going beyond the standard threat hunting already included with your ThreatWatch service, ThreatWatch Hunt provides out-of-band threat hunting for malware and APTs utilizing memory forensics – it does not rely on device logs. ThreatWatch Hunt helps ensure threats that do not get detected because the device is not sending logs can still be detected through a completely different detection approach.



Standard hunting is manual in nature. It is proactive, but takes time and strong technical knowledge to ask the right questions of the day. Advance hunting is automated. It is advanced analytics, automated forensic analysis of all the end points, and machine learning layered on top of it.

Security On-Demand
sales@securityondemand.com
858.693.5655
www.securityondemand.com

Security On-Demand™ is the leading provider of advanced managed security services. Our solutions help organizations protect against security threats, adhere to compliance requirements, and manage risk. Our scalable architecture eliminates capital outlay, provides 24x7 support/monitoring coverage, and lowers management, maintenance and staffing costs.

ThreatWatch Hunt Benefits

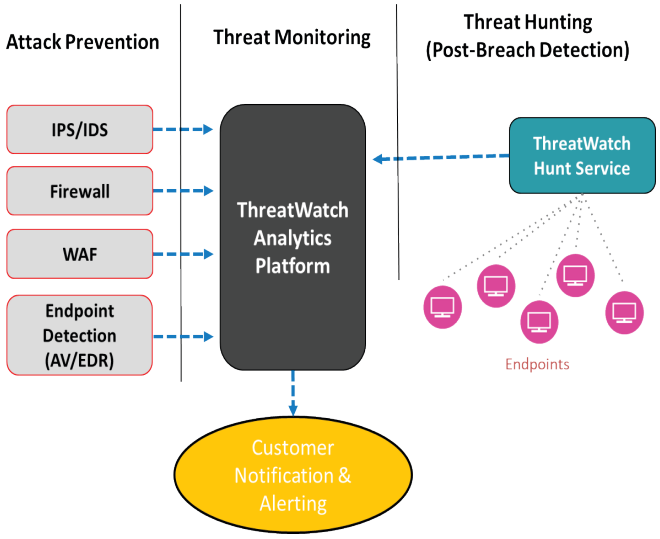
- Close the gap between post event and time to detect
  - Provides insight into malware that might be "hidden" on a device
  - More cost-effective than additional real-time detection layers
  - Denies ability of attackers to persist undetected
- Get analysis of entire customer environment, not just alerts from specific devices
  - Enables us to look at every device on the network, not just devices we are collecting data from
  - Easier to "hunt" for malicious threats
- Identify things holistically that don't belong
  - Tracks device state and identifies abnormal changes
- Layered detection – go beyond what security protection products can analyze

How it Works

ThreatWatch® Hunt integrates third-party hunting toolsets and methods with Security On-Demand's proprietary correlation and behavioral analysis capabilities, such as machine learning-based artificial intelligence and supervised learning models that use behavioral Analysis of attack patterns. As part of the service, SOD will:

- Monitor the alerts, logs, and output provided by the advanced threat hunting activities
- Correlate such activity with logs, alerts, and other information received
- Validate the threat as part of the triage and investigation process
- Tune and provide continual feedback to ensure that normal system behavior is baselined

Once an alert for a potential threat is received, the data is correlated with other security information and then our SOC team will respond to further triage and investigate the suspicious activity.



Conducts periodic scheduled scans of network devices. Implants and threats discovered during a sweep initiate an alert to the ATLAS Analytics Platform.

Capabilities

Security On-Demand's threat hunting technology capabilities are significant and are expansive beyond what a typical SOC can provide. This is because we utilize an agentless based approach on how we examine and evaluate each endpoint that is analyzed while examining six types of threat vectors that can compromise a system in the following areas:

- Process
- Module
- Driver
- In-Memory
- Auto-Start
- Hooks

Within each of these threat vector categories, there are hundreds of potential exploits that can compromise a system. Also supported is live memory analysis, rather than static file export analysis (via memory dump file), targeted surveying of volatile memory and finding malware that can masquerade as legitimate process, driver, or module components in the operating system.

Get started today. Request your 30 minute demo of our ThreatWatch Hunt Service. Contact a Security On-Demand Representative by emailing sales@securityondemand.com, or call us at 858.693.5655

*2105 Cost of Cyber Crime Study, Ponemon Institute