LYNX TECHNOLOGY PARTNERS

ThreatWatch Hunt

Breach Detection without the Data

Take the headache out of maintaining your first line of defense against malicious threats

Here's The Problem

With an average dwell time of 197 days and an additional 69 days to contain the breach*, 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 more opportunities for the attackers to access more records and have a greater negative impact on your brand.

- Attackers are getting more sophisticated every day
- The tools of the past will not protect against the threats of the future
- The budget and resources to adequately identify and mitigate attacks are limited

The Stopgap Solutions

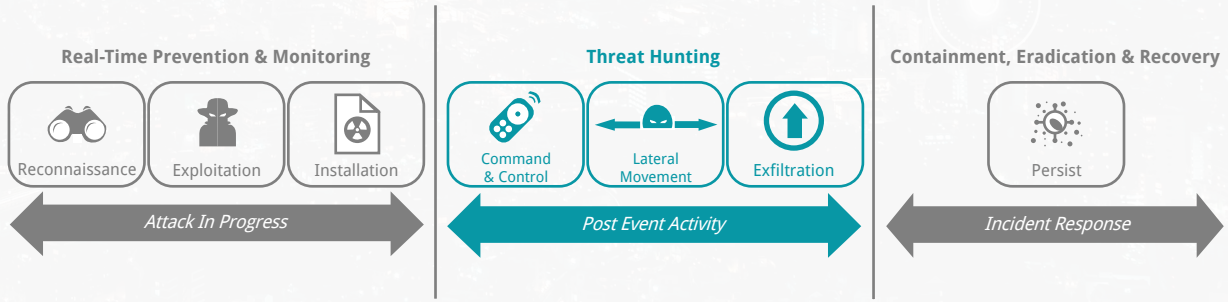
A company may have a fully compliant, well-secured enterprise complete with perimeter defenses such as firewalls, IDS/IPS, DMZ, proxy servers and more. They may have their network segmented to isolate their crown jewels and protect their critical data. They may have robust email security, the latest end-point protection program, and many other exceptional security tools.

They can employ all of these security measures and still be compromised. A hacker targeting you directly will eventually find a way in.

Proactive Threat Hunting

Detecting sophisticated attacks requires toolsets and technology beyond what normal security operations maintain to perform their day-to-day threat monitoring and triage activities. Proactive threat hunting is automated. It is behavioral analytics. It is forensic analysis of all end-points with an added layer of machine learning.

As an addition to the ThreatWatch service, ThreatWatch Hunt provides out-of-band threat hunting for malware and APTs utilizing memory forensics, not device logs, to help ensure threats are detected.



*IBM 2018 Cost of Data Breach study

Why ThreatWatch Hunt

The purpose of threat hunting is to reduce 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.

ThreatWatch Hunt will:

Close the gap between post event and time to detection

ThreatWatch Hunt provides insight into malware that might be "hidden" on a device. It is more cost-effective than additional real-time detection layers and denies the ability of attackers to persist undetected.

Get analysis of the entire environment, not just alerts from specific devices

This proactive threat hunting service enables us to look at every device on the network, not just devices where we are collecting data. This makes it even easier to "hunt" for malicious threats.

Identify things holistically that don't belong

Our proven advanced threat detection service can track the state of the device and will identify any abnormal changes. The layered detection can go beyond what security protection products can analyze.

Case Study

Significant Data Breach at a Major Regional Financial Institution

Issue

An unknown/zero-day malware attack was discovered accidentally, following the notice of abnormal network communications.

How We Detected

ThreatWatch behavioral analytics platform detected a 5.3MB executable injected into the LSASS process with read, write, and execute privileges.

The injected memory was submitted to the AI-powered engine for static, heuristic, and IOC analysis.

Customer Response & Follow-Up

This notification enabled the client to successfully protect the institution from the inevitable activation of the ransomware found.

Operational concerns had led to an erosion of defensive measures, placing the institution at an unnecessary risk.

The Bottom Line

Time is money, especially when it comes to a security breach. Companies that identified a breach in less than 100 days saved an average of $1 million, as compared to those that took more than 100 days. Similarly, companies that contained that 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)

Get Started

To request your 30 minute demo of our ThreatWatch Hunt Service, contact a Lynx Technology Partners Representative.

Sales@LynxTP.com

(800) 314-0455

LYNX TECHNOLOGY PARTNERS

Lynx Technology Partners
Sales@LynxTP.com
(800) 314-0455
www.LynxRiskSolutions.com

Lynx Technology Partners 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.