# Threat Hunting Checklist

## How to get ahead of adversaries and strengthen cybersecurity defense

According to the CISO Benchmark Study, "Prevention by gaining visibility, performing threat hunting, and establishing a zero-trust framework is now critical for protecting your infrastructure."[1] We at Nuspire couldn't agree more. Network visibility is a cybersecurity essential. You can't fight an adversary you can't see. Threat hunting, which relies on visibility, is effective in stopping would-be attackers and discovering adversaries already inside your business. And fortunately, Zero Trust adoption is accelerating in 37.4% of organizations polled.[2]

This checklist provides CISOs and other security professionals with tips and recommendations to start or strengthen a threat hunting program in three steps:

**Step 1.** Understand What Is a Threat
**Step 2.** Lay the Groundwork-Get Visibility
**Step 3.** Start Threat Hunting

## Step 1: Understand What Is a Threat

A threat is malicious activity that can lead to loss of money, information, reputation and customer trust. Before you go hunting or do anything to address cybersecurity concerns, take the time to learn about threats and which ones are most likely to target your organization and industry.

**Tip:** Invest in threat hunting because it works. Any reduction in dwell time minimizes potential loss. On average, companies required 207 days to identify and 73 days to contain a breach in 2019.[3]

### Recommended Actions:

□ **Determine intent.** Common adversary motivations are financial gain, publicity, hacktivism and deletion/destruction. Identify what's valuable or "tempting" in your organization – such as employee records, sensitive customer data and intellectual property – that might appeal to threat actors.

[1] Cisco Cybersecurity Report Series 2020, CISO Benchmark Study: Securing What's Now and What's Next.

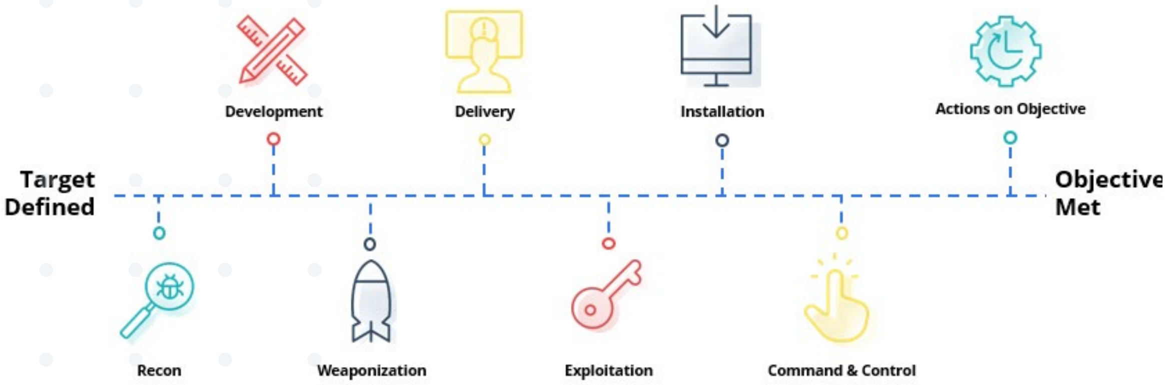
[2] Deloitte press release, Zero Trust Adoption Not Slowed by Pandemic Disruption, September 9, 2020.

[3] IBM Security, Cost of a Breach Report, 2020.

□ **Consider capability.** Threat actors have varying levels of ability to breach your organization successfully and achieve their goals. They often scope their targets by conducting reconnaissance. After you narrow the suspect list based on intent, you can do your own recon into tactics, techniques and procedures.

□ **Evaluate opportunity.** Adversaries act based on their knowledge of your environment, including its vulnerabilities, and timing. Phishing, for example, has skyrocketed during the pandemic. Assess attacker opportunities created by work from home (WFH), collaboration tools, use of mobile devices, increased reliance on cloud-based applications and internet-connected devices.

□ **Understand the threat lifecycle.** Stopping an adversary at any point is a win.



## **Step 2:** Lay the Groundwork

Threat hunting is playing offense. Why wait for someone to tell you that your organization has been attacked or breached? Architecture is a good starting point. Inventory your devices, plan, implement and update systems with security in mind – but be sure to balance technology with people and processes.

**Tip:** Operate on the assumption that there are no silver bullets, even if you have defense in depth with next-generation firewalls, antivirus software, intrusion detection systems and Zero Trust security.

**Recommended Actions:**

□ Add passive defense with systems that reduce human interaction and build from there.

□ Establish comprehensive visibility by monitoring gateways, networks and endpoints 24/7/365.

□ Begin collecting data from your assets. Not sure how many assets you have or which ones are talking to the internet? Find out with tools like CyCognito and Qualys.

□ Establish active defense by adding analysts or a MSSP to monitor, respond to and learn from adversaries within the network.

□ Start leveraging threat intelligence by integrating data from multiple sources, such as indicators of compromise, anomaly detection, Deep Instinct and Recorded Future.

## Step 3: Start Threat Hunting

A dedicated person or team is preferable to part-time resources. A good threat hunter is a curious person with security experience who likes to find the needle in the haystack. On a regular basis, take stock of technology, people and processes so you can continually improve your threat hunting program.

**Tip:** Don’t allow threat hunters to be sidelined by alert response, network maintenance or vulnerability patching tasks.

**Recommended Actions:**

□ Establish a threat hunting baseline through network analysis. Useful tools include endpoint detection and response technology with machine learning and forensics capabilities and a SIEM for correlation and analysis of security alerts.

□ Keep hunters focused on answering these questions:

- What am I looking at?
- What am I hunting for?
- What is the true threat?
- What is the outcome?

□ Work up an incident response plan, including who does what and when, so you're ready when you find a true threat.

□ Engage with a security services provider to share information and close people, process and technology gaps. Take advantage of partnerships to offset the chronic shortage of cybersecurity skills and technology debt.

**Want to Learn More? We Can Help.**

Nuspire is a leading managed security services provider (MSSP) that is revolutionizing the cybersecurity experience by taking an optimistic and people first approach. Our deep bench of cybersecurity experts, world-class threat intelligence and 24x7 security operations centers (SOCs) detect, respond and remediate advanced cyber threats. We offer comprehensive services that combine award-winning threat detection with superior response capabilities to provide end-to-end protection across the gateway, network and endpoint ecosystem. Our client base spans thousands of enterprises of all sizes, across multiple industries, and achieves the greatest risk reduction per cyber-dollar spent. At Nuspire, we are laser-focused on delivering an extraordinary cybersecurity experience that exceeds client expectations.

For more information, watch Let's Go Threat Hunting and visit www.nuspire.com and follow @Nuspire.