7tech

THE 7-STEP THREAT DETECTION PLAN FOR INTERNAL IT DEPARTMENTS

The complete slide deck to help you enhance your security with actionable steps and real-world applications.

The 7-Step Threat Detection Plan

Critical Industry Expert Strategies To Integrate Into Your Cybersecurity Protocols. Learn From Real-World Case Studies And Utilize Interactive Tools To Fortify Your Organization's Threat Detection Capabilities

The growth and sophistication of cybercriminals, ransomware and hacker attacks has reached epic levels. CISOs and IT leaders can no longer ignore it or foolishly think, "That won't happen to us."

Your business – large OR small – will be targeted and will be compromised UNLESS you take action on the information revealed in this important new cybersecurity training

Provided By: 7tech
Author: Neal Juern
2544 MacArthur Vw, San Antonio, TX. 78217
www.7tech.com
San Antonio: (855) 701-6777

7 Steps To An Effective Threat Detection Plan

SCAN ME

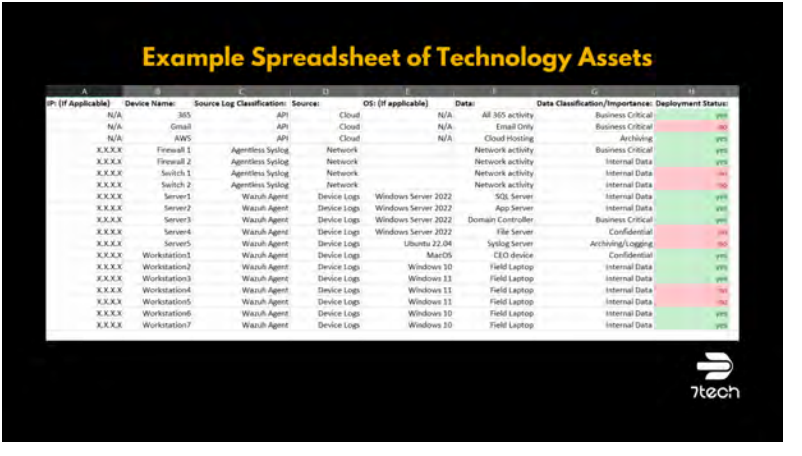
Need Help With Cybersecurity?

Talk To Our Experts Today

CLAIM YOUR FREE CONSULT AT
www.7tech.com/free-consult

"Knowing that a solid reliable group of cybersecurity experts are protecting our non-profit business helps me sleep at night!"
Vinsen Farris, CEO, Meals on Wheels SATX

As an IT leader, it's essential to conduct a comprehensive inventory of your technology assets, encompassing both physical equipment and data assets. Understanding the full scope of what exists in your environment is critical for effectively identifying and mitigating threats. This process can be challenging without the right tools or methodologies. A practical approach to begin this task is by creating a detailed spreadsheet to systematically catalog and track your assets.

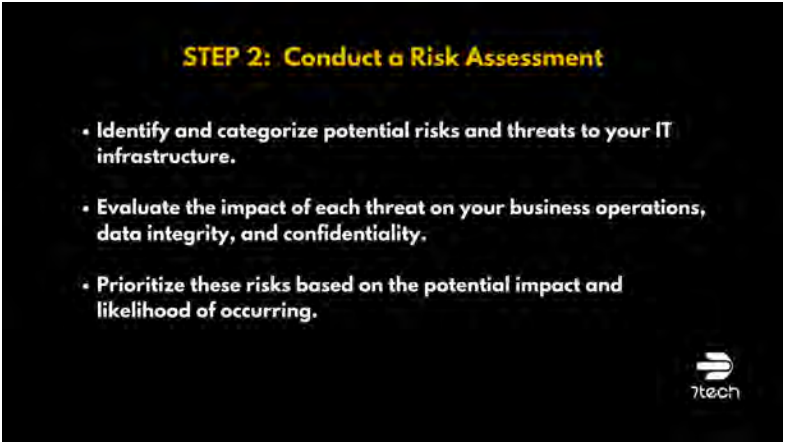


Maintaining a spreadsheet of technology assets is a strategic step. It guides you on where to focus your attention, encompassing cloud services, network infrastructure, and all connected devices. Assessing the data, determining its criticality – whether it's mission-critical or non-essential – is crucial. Such an inventory aids in prioritizing areas for implementing threat detection measures, ensuring that the most sensitive areas are secured first.

On the left: N-CENTRAL, we use this tool to build asset lists of every machine in an environment. Nodeware, we use this tool to do vulnerability scans and reporting. **On the right:** Lansweeper, Nessus, and PingCastle are less expensive alternatives you can use to inventory your assets and scan for vulnerabilities

How To Get Started: Set up a recurring task for your team to conduct network scans at regular intervals. This helps in detecting unauthorized devices on the network. Maintain an updated inventory of all network elements, including VLANs, DMZs, company and guest networks. Automate the process where possible, focusing on regular review and reporting. Consistently verifying the accuracy of your network inventory is crucial.

Your goal is to identify and evaluate potential risks to your systems and data. Then, assess the impact of these threats on business operations, data integrity, and confidentiality.



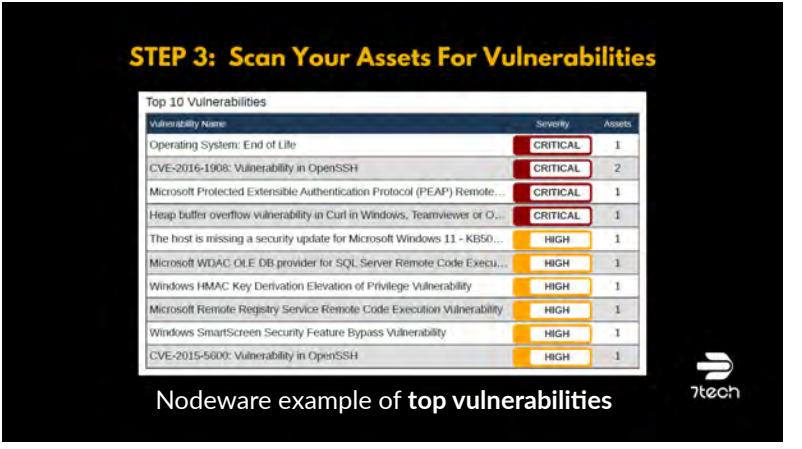
Remember: Prioritize risks based on their potential impact on your business and the likelihood of occurrence. Focus on probable threats, avoiding overemphasis on unlikely scenarios.

Compile a list of common risks, including Persistent Threats (PTs) and Advanced Persistent Threats (APTs). It's vital to detect and neutralize these threats, especially if hackers have been infiltrating your environment for an extended period. After creating a satisfactory list, expand it by rating each threat based on severity, likelihood, and potential impact on your organization.

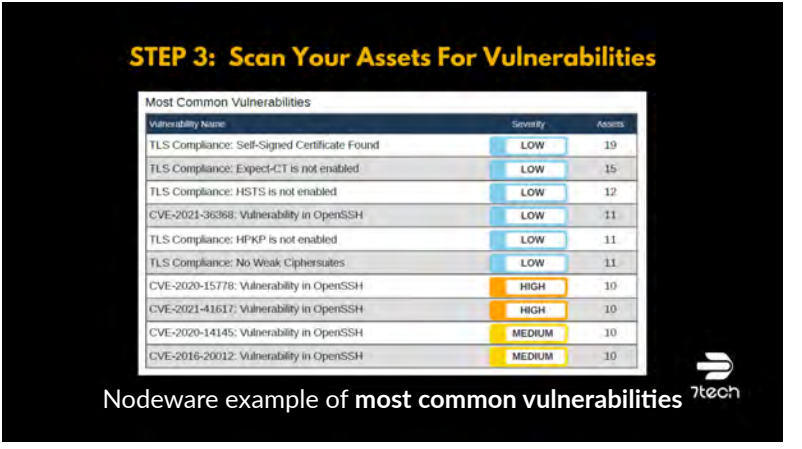
How to rate your risk: Assess your risks in two categories: potential operational impact and likelihood of occurrence. Rate each as low, medium, or high. Prioritize threat detection on systems that score 'high' in both categories, as they represent the most significant risks.

*If your organization is entirely cloud-based, the risk of data issues on your servers is low, particularly if servers are primarily used for user authentication and all data is cloud-stored. Focus less on server attacks, as their likelihood is minimal.

Having identified and rated your risks to assess your threat surface, proceed to scan all assets for vulnerabilities. Conduct these scans on a regular schedule to promptly detect threats in your environment and **see the difference over time after completing remediations.** Either finding a tool that scans for vulnerabilities on a continuous basis or make scheduled tasks to complete this for your organization regularly.

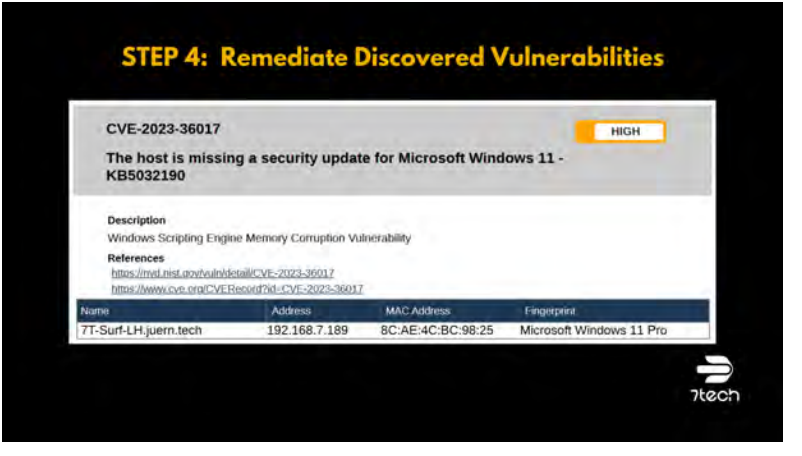


What to remediate first: After a vulnerability scan, you'll often find patch management gaps in operating systems or third-party software, resulting in a lengthy list of findings. Utilize a tool with robust reporting capabilities to categorize risks from low to high and prioritize addressing critical vulnerabilities first. Continuously scan for new vulnerabilities as software updates are released. The goal is to gradually reduce the list, seeing fewer critical vulnerabilities over time. Tools like Rapid7, Nexpos, and Nodeware, which we've found effective, provide accurate reports to efficiently target the most urgent issues for our clients. Above is an example from Nodeware.



Additionally, Nodeware will give you a list that identifies the most commonly exploited vulnerabilities in your environment. Prioritize addressing high-risk issues like open SSH vulnerabilities. Focus on remediating those that pose the greatest threat and will have the most significant impact on your security posture. Using these systems can help you discover your vulnerabilities and figure out which ones are most likely to be exploited.

But let's take a second to talk about remediation. It's crucial to act promptly. Once threats are identified in your environment, immediately begin addressing them, especially critical threats with high exploitation likelihood. Adopt a 'fix-as-you-go' approach for effective threat management.



In Nodeware, a HIGH threat is clearly identified with a CVE number. For example, a Windows 11 Pro issue might show a Windows Scripting Engine Corruption Vulnerability. Nodeware typically provides links to detailed information about the vulnerability and steps for remediation.

After identifying vulnerabilities, you must capture security events from Office 365, servers, routers, and critical workstations. Analyze these events in as close to real time as possible and take immediate action. Utilize a Security Information and Event Management (SIEM) system for automation or conduct manual analysis if needed, though it requires significant effort.

Security Information and Event Management (SIEM). Consider tools like Splunk and Wazuh, the latter being an open-source platform we currently utilize at 7tech. Wazuh offers flexibility and customization for unique security needs. If resource constraints prevent the deployment of a SIEM, adopt a manual approach to review security information. Perform daily checks and a 48-hour retrospective analysis to ensure each data set is examined twice. Focus on critical systems such as firewalls and key servers, and assign staff to scrutinize logs for suspicious activity, concentrating on security events.

Note: While Wazuh is a powerful open-source tool, it requires a significant investment of time and expertise to set up.

For Demo, watch "MasterClass: The 7-Step Threat Detection Plan" training video at:

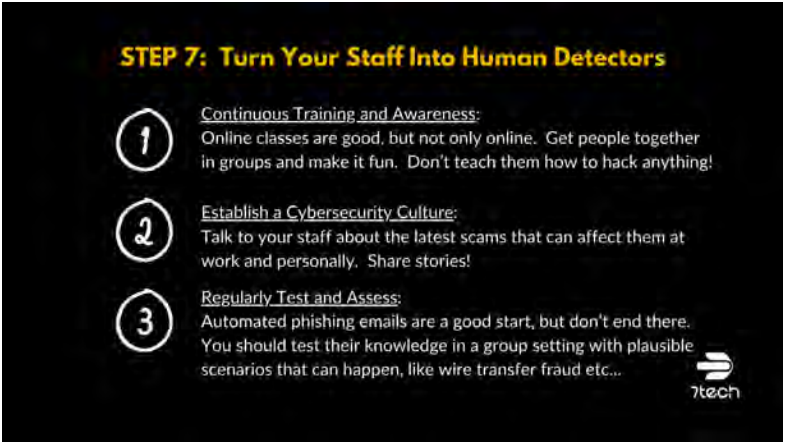
https://www.7tech.com/masterclass-the-7-step-threat-detection-plan/

Intensify monitoring of privileged user activities. Often, cyber attacks commence with anomalies in user behavior. Employ User Behavioral Analytics (UBA) tools to oversee account and group activities. Focus primarily on privileged users and groups, as monitoring and analyzing every user's behavior accross the network can be complex. Many accessible tools can assist in security monitoring. PowerShell, in particular, is invaluable for Windows environments, enabling the creation of automated tasks and the generation of clear CSV reports through Task Scheduler. These reports can be tailored to your specific needs, scheduled, and reviewed regularly.

Implement the principle of least privilege—restrict access rights for users to the bare minimum needed for their roles. Regularly audit permissions, ensuring no user has more access than necessary. Monitor for atypical actions among privileged accounts and groups, and respond promptly to any irregularities with tools like Wazuh. In the absence of a SIEM, make scheduled tasks and calendar reminders your go-to strategy for consistent monitoring. Combine this with other freely available tools, such as Nessus, to track and fine-tune permissions for privileged accounts and service accounts, ensuring they possess only the necessary privileges.

Provide employees with continuous cybersecurity training and awareness, establish a cybersecurity culture, and regularly test and assess your environment with the help of a qualified third-party.

As an IT professional, it's crucial to understand that over 90% of cyberattacks begin with email, exploiting social engineering tactics. Notable breaches, such as those at MGM and Caesar's, exemplify this trend. It's imperative to intensify staff training on recognizing and responding to social engineering techniques to bolster our defenses in this critical area.



Transform your staff into proactive human threat detectors by engaging them in interactive phishing simulation exercises. If you're already conducting these simulations, elevate the experience by forming teams and adding a competitive, fun element to enhance engagement and retention. Cultivate a strong cybersecurity culture by discussing the latest scams and sharing real-world breach stories—narratives are more memorable than mere tips or videos. Reinforce the protocol that changes to financial transactions, like wire transfers, should never be authorized by email alone, but always verified through additional methods such as phone calls to known contacts.

Continuously Evolve Your Threat Detection Strategy: In a dynamic IT landscape with frequent introductions of new systems or cloud-based services, it's crucial to adapt your threat detection accordingly. For every new element—be it a cloud service, server, or workstation—strategically plan its threat detection integration. Always focus on enhancing and updating your threat detection capabilities to match your evolving environment.

Need Help With Cybersecurity?

Talk To Our Experts Today!

CLAIM YOUR FREE CONSULT AT
www.7tech.com/free-consult

7tech