



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

Notice: This publication is intended to provide accurate and authoritative information in regard to the subject matter covered. However, no warranties are made. It is provided with the understanding that the author and the publisher are NOT engaged in rendering legal, accounting or related professional services or advice and that this publication contains opinions of its author. This publication is NOT intended as a substitute for specific legal or accounting advice for any particular institution or individual. The publisher accepts NO responsibility or liability for any individual's decisions or actions made as a result of information or opinion contained herein.

7 Steps To An Effective Threat Detection Plan

- Step 1.** Inventory Your Technology Assets.....4-6
 - Step 2.** Conduct A Risk Assessment.....7-10
 - Step 3.** Scan Your Assets For Vulnerabilities.....11-13
 - Step 4.** Start Remediating Discovered Vulnerabilities.....14-15
 - Step 5.** Capture and Review All Security Events With A SIEM.....16-18
 - Step 6.** Monitor Privileged User Activities Closely.....19-20
 - Step 7.** Turn Your Staff Into Human Detectors.....21-23
- BONUS: Never Stop Improving Threat Detection.....24
- Exclusive offer: One-on-one Data Protection Strategy Session.....25
-



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

STEP 1

Inventory Your Technology Assets (both equipment and data)



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.

Example Spreadsheet of Technology Assets

A	B	C	D	E	F	G	H
IP: (If Applicable)	Device Name:	Source Log Classification:	Source:	OS: (If applicable)	Data:	Data Classification/Importance:	Deployment Status:
	N/A	365	API	Cloud	N/A	All 365 activity	Business Critical yes
	N/A	Gmail	API	Cloud	N/A	Email Only	Business Critical no
	N/A	AWS	API	Cloud	N/A	Cloud Hosting	Archiving yes
X.X.X.X	Firewall 1	Agentless Syslog	Network		Network activity	Business Critical	yes
X.X.X.X	Firewall 2	Agentless Syslog	Network		Network activity	Internal Data	yes
X.X.X.X	Switch 1	Agentless Syslog	Network		Network activity	Internal Data	no
X.X.X.X	Switch 2	Agentless Syslog	Network		Network activity	Internal Data	no
X.X.X.X	Server1	Wazuh Agent	Device Logs	Windows Server 2022	SQL Server	Internal Data	yes
X.X.X.X	Server2	Wazuh Agent	Device Logs	Windows Server 2022	App Server	Internal Data	yes
X.X.X.X	Server3	Wazuh Agent	Device Logs	Windows Server 2022	Domain Controller	Business Critical	yes
X.X.X.X	Server4	Wazuh Agent	Device Logs	Windows Server 2022	File Server	Confidential	no
X.X.X.X	Server5	Wazuh Agent	Device Logs	Ubuntu 22.04	Syslog Server	Archiving/Logging	no
X.X.X.X	Workstation1	Wazuh Agent	Device Logs	MacOS	CEO device	Confidential	yes
X.X.X.X	Workstation2	Wazuh Agent	Device Logs	Windows 10	Field Laptop	Internal Data	yes
X.X.X.X	Workstation3	Wazuh Agent	Device Logs	Windows 11	Field Laptop	Internal Data	yes
X.X.X.X	Workstation4	Wazuh Agent	Device Logs	Windows 11	Field Laptop	Internal Data	no
X.X.X.X	Workstation5	Wazuh Agent	Device Logs	Windows 11	Field Laptop	Internal Data	no
X.X.X.X	Workstation6	Wazuh Agent	Device Logs	Windows 10	Field Laptop	Internal Data	yes
X.X.X.X	Workstation7	Wazuh Agent	Device Logs	Windows 10	Field Laptop	Internal Data	yes



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.

STEP 1: Inventory Your Technology Assets



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.

STEP 2

Conduct a Risk Assessment



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.

STEP 2: Conduct a Risk Assessment

- Identify and categorize potential risks and threats to your IT infrastructure.
- Evaluate the impact of each threat on your business operations, data integrity, and confidentiality.
- Prioritize these risks based on the potential impact and likelihood of occurring.



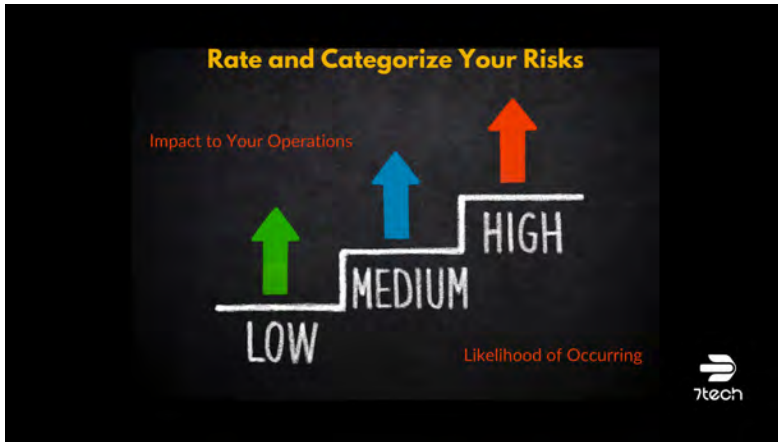
Remember: Prioritize risks based on their potential impact on your business and the likelihood of occurrence. Focus on probable threats, avoiding overemphasis on unlikely scenarios.

Identify the Risks

- Phishing / Sphere Phishing Attacks / Social Engineering
- Insider Threats - rogue employees or vendors
- Denial of Service Attacks (DoS or DDos)
- Persistent Threats (PTs and APTs)
- Password Attacks - bad password policies or leaked on the dark web
- Vulnerable Remote Access - VPN, Remote Desktop, Cloud Proxy
- Vulnerable Internet Facing Systems - Websites, Databases
- Vulnerable Internal Systems - Missing Patches or Unpatched Systems
- Cloud Security Issues - misconfigured settings and SaaS vendor failures
- Supply Chain Attacks - what data and devices could be compromised?
- Mobile Device Security - what data is stored and accessible?



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.

STEP 3

Scan Your Assets For Vulnerabilities



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.

STEP 3: Scan Your Assets For Vulnerabilities

Vulnerability Name	Severity	Assets
Operating System: End of Life	CRITICAL	1
CVE-2016-1908: Vulnerability in OpenSSH	CRITICAL	2
Microsoft Protected Extensible Authentication Protocol (PEAP) Remote ...	CRITICAL	1
Heap buffer overflow vulnerability in Curl in Windows, Teamviewer or O...	CRITICAL	1
The host is missing a security update for Microsoft Windows 11 - KB50...	HIGH	1
Microsoft WDAC OLE DB provider for SQL Server Remote Code Execu...	HIGH	1
Windows HMAC Key Derivation Elevation of Privilege Vulnerability	HIGH	1
Microsoft Remote Registry Service Remote Code Execution Vulnerability	HIGH	1
Windows SmartScreen Security Feature Bypass Vulnerability	HIGH	1
CVE-2015-5600: Vulnerability in OpenSSH	HIGH	1


Nodeware example of top vulnerabilities



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.

STEP 3: Scan Your Assets For Vulnerabilities

Vulnerability Name	Severity	Assets
TLS Compliance: Self-Signed Certificate Found	LOW	19
TLS Compliance: Expect-CT is not enabled	LOW	15
TLS Compliance: HSTS is not enabled	LOW	12
CVE-2021-36368: Vulnerability in OpenSSH	LOW	11
TLS Compliance: HPKP is not enabled	LOW	11
TLS Compliance: No Weak Ciphersutes	LOW	11
CVE-2020-15778: Vulnerability in OpenSSH	HIGH	10
CVE-2021-41617: Vulnerability in OpenSSH	HIGH	10
CVE-2020-14145: Vulnerability in OpenSSH	MEDIUM	10
CVE-2016-20012: Vulnerability in OpenSSH	MEDIUM	10

Nodeware example of most common vulnerabilities 

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.

STEP 4

Start Remediating Discovered Vulnerabilities



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.

STEP 4: Remediate Discovered Vulnerabilities

CVE-2023-36017 HIGH

The host is missing a security update for Microsoft Windows 11 - KB5032190

Description
Windows Scripting Engine Memory Corruption Vulnerability

References
<https://nvd.nist.gov/vuln/detail/CVE-2023-36017>
<https://www.cve.org/CVERecord?id=CVE-2023-36017>

Name	Address	MAC Address	Fingerprint
7T-Surf-LH.juern.tech	192.168.7.189	8C:AE:4C:BC:98:25	Microsoft Windows 11 Pro



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.

STEP 5

Capture and Review ALL Security Events (with a SIEM)



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.

STEP 5: Capture and Review ALL Security Events (SIEM)

wazuh.

splunk>

**Manually Review Security
Logs of Devices Daily**

We recommend to look back
48 hours each time



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.

STEP 5: Capture and Review ALL Security Events (SIEM)

wazuh.

DEMO



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

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

STEP 6

Monitor Privileged User Activities Closely



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 across 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.

STEP 6: Monitor Privileged User Activities Closely



NIST
National Institute of
Standards and Technology

PRINCIPLE OF LEAST PRIVILEGE

The principle that a security architecture should be designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function.



UBA
User
Behavior
Analytics

Monitor activity and behavior from accounts that already have privileged access and any account that suddenly gains privileged access.



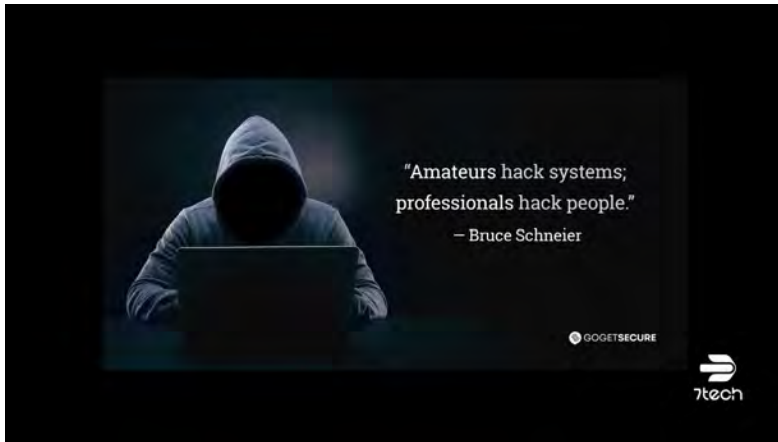
Implement the principle of least privilege—restrict access rights for users to the bare minimum needed for their roles. Regularly audit permissions, ensuring no user has more access than necessary. Monitor for atypical actions among privileged accounts and groups, and respond promptly to any irregularities 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.

STEP 7

Turn Your Staff Into Human Detectors



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.

STEP 7: Turn Your Staff Into Human Detectors

1

Continuous Training and Awareness:

Online classes are good, but not only online. Get people together in groups and make it fun. Don't teach them how to hack anything!

2

Establish a Cybersecurity Culture:

Talk to your staff about the latest scams that can affect them at work and personally. Share stories!

3

Regularly Test and Assess:

Automated phishing emails are a good start, but don't end there. You should test their knowledge in a group setting with plausible scenarios that can happen, like wire transfer fraud etc...



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.

BONUS

Never Stop Improving Your Threat Detection



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

