WHITE PAPER:

Maturing Your Endpoint Security Strategy with Tanium

www.chuco.com info@chuco.com

In 2022, there were no shortages of major attention-grabbing headlines where businesses had their sensitive customer data leaked, faced ransomware issues, and lost proprietary data to hackers.

The trend in data breaches continues to rise upwards and the consequences of data attacks have become a great concern for security leaders, as they look to navigate an increasingly complex threat and regulatory landscape.

Criminals are on the lookout for ways to breach endpoints and steal personal and sensitive information. Some of these criminals are highly sophisticated and have well-funded and organized teams who can find new vulnerabilities and exploit them in novel ways.

It may seem easy to point out how leaders and businesses could have done X, Y, or Z to prevent the breaches, but the reality is that cybersecurity is complex and there is no silver bullet to prevent the next major breach.

Regrettably, cyberattacks are big business as the FBI reported that $6.9 billion was officially lost to cybercrimes in 2021. The need to understand the threat landscape and have a well-designed plan in place to effectively detect and respond to attacks has become even more essential in the last several years.

Endpoint Security with Tanium

At Chuco, we work with Tanium customers and partners daily to ensure cyber security is a top priority. Through years of endpoint security experience, we've developed a deep understanding of what it takes to make organizations successful with Tanium endpoint products.

Here are useful and proven tips Chuco recommends to improve endpoint security operations with Tanium in your organization:

Cybersecurity is a Team Sport: — "Communicate your security goals and objectives"

At its core, Tanium is designed to deliver endpoint data from your environment at speed and scale. Through the years, Tanium has built new modules and capabilities on top of this platform that streamlined ways of viewing and interacting with your endpoint data based on demands from various IT teams.

From DevOps teams, performance analysts, compliance officers, patch admins, to security operations teams, Tanium provides valuable data and insights to many key members of your organization. This versatility can make Tanium seem overwhelming and too complex to handle. So, clarifying your security strategy and goals up front becomes paramount.

Whether you want to stop the next major breach, improve your security hygiene, or implement your security framework to abide by government regulations and policies, always set targets and prioritize goals with your team. Cybersecurity is a team sport, and every member of the team needs to understand the big picture so they can best align and focus their efforts on the larger strategies.

Enrich Tanium Threat Response with Integrations — "Better together"

Tanium developed the Threat Response module to quickly detect and respond to cyber attacks against the endpoint. The Threat Response suite includes scalable and powerful tools to help incident responders, SOC analysts, and threat hunters close the gap against attackers and gain deep visibility and control over their endpoints.

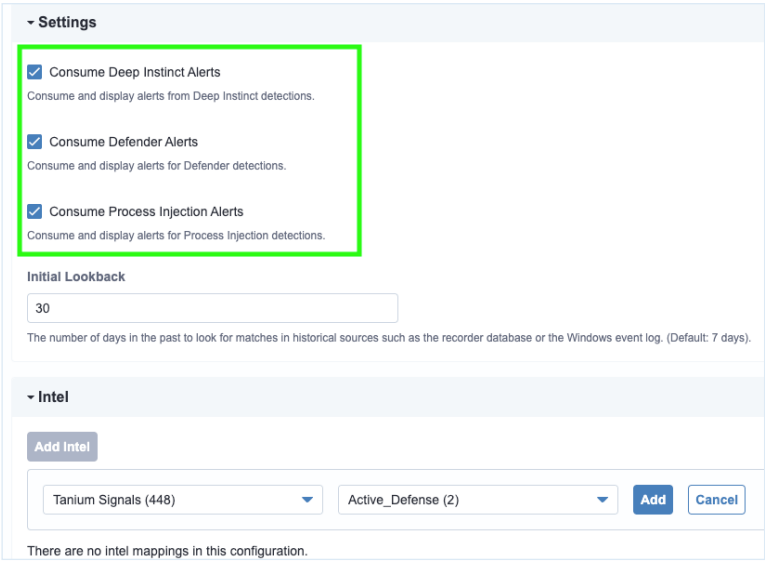
The built-in detection scan engine supports common industry IOC events, Yara files, custom event Signals, and process injection intelligence allowing security teams to hunt from loads of historical and security enriched endpoint telemetry recorded and indexed by Tanium.

However, cybersecurity leaders have complex needs and innumerable challenges to handle in a rapidly changing threat landscape. Enterprises require highly tailored and extensible platforms with powerful integrations to bolster collaboration between technologies that will better align to the dynamic needs of the security teams.

As a result, Tanium has developed relationships and powerful technical integrations with major industry partners like Microsoft, Splunk, Service-Now, and DeepInstinct. Take advantage of integrations to get the most out of the Tanium Threat Response Module to help reduce the attack surface from complex and sophisticated threats.

Below are some of the valuable Threat Response Module integrations available today:

Partner	Integration Description
Microsoft	• Feed Threat Response alerts to Microsoft Sentinel for Security Orchestration, Automation and Response (SOAR) solutions • Ingest threat alerts from Windows native Microsoft Defender
Deep Instinct	• Layered defense with Tanium Endpoint Detection and Deep Instincts Endpoint Prevention • Ingest alerts from advanced deep learning prevention platform
VirusTotal	Enrich Threat Response hashes with VirusTotal reputation scores for suspicious files, domains, IPs and URLs to detect malware and other breaches
ServiceNow	Feed Threat Response sensor data to the ServiceNow Security Operations suite
Splunk	Feed Tanium Splunk Application to display dashboards of Threat Response alerts, critical software vulnerabilities, unmanaged assets, application and process visibility, suspicious open ports and more
Chronicle Security	• Stream endpoint telemetry from Threat Response to Chronicle, to store and analyze up to a year of telemetry data • Send Threat response alerts to Chronicle security analytics platform



Tanium Integration with Deep Instinct, Windows Defender and New Process Injection Alerts

Stay Focused on the Basic Fundamentals of Good Cyber Hygiene:

From automating tasks with Artificial Intelligence to innovative technologies on blockchains, the cybersecurity industry is hot, and there is no shortage of innovative tools and technologies being developed to help find the latest sophisticated attacks. While new innovations are certainly worth researching and adopting, security leaders still need to validate and ensure the basics of security are done right on their network.

Even outside of cybersecurity, we know that essential hygiene principles such as eating vegetables or washing hands can prevent disease or illness. Yet, many people don't do it. Mastering the basics may sound easy, but technology leaders know it's hard.

There are 3 basic foundations that Tanium can help with to maintain good cyber hygiene:

1. Inventory Management
2. Automated Vulnerability Management
3. Patches and Software Updates

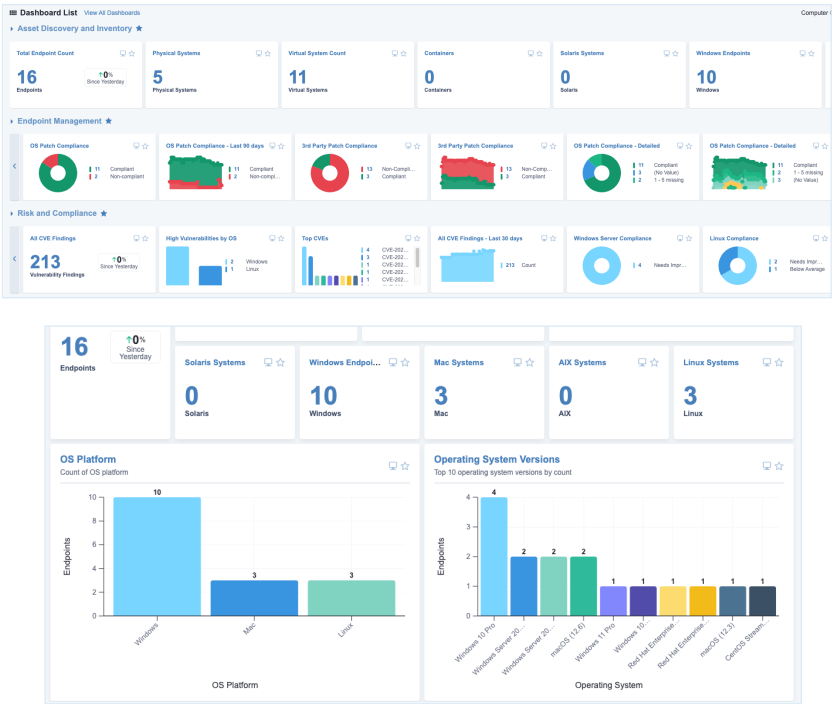
Basic Fundamental 1
Inventory Management: “You can’t protect what you can’t see”

The non-regulatory agency, National Institute of Standards and Technology (NIST) published the NIST Cybersecurity Framework which became the standard set of cybersecurity standards, guidelines, and best practices for the U.S. federal government agencies.

The first key function of the framework is to identify critical enterprise assets to develop an organization understanding to manage cybersecurity risks to systems, assets, data, and capabilities.

It’s important to have an understanding of the computer hardware and software in your organization because they are frequently the entry points of malicious actors. With Tanium Asset, you can get a complete and up-to-date view of your enterprise inventory.

The more you understand about the assets in your organization, the better you can develop a security strategy that minimizes risk effectively.



Inventory Management

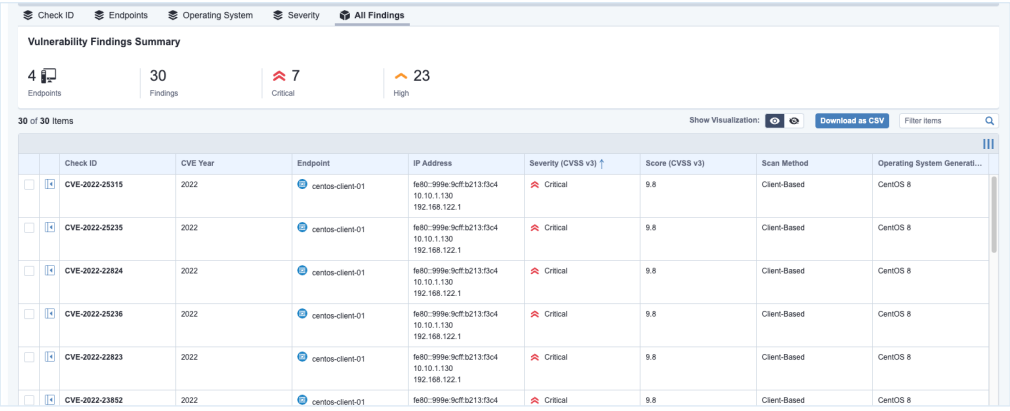
Basic Fundamental 2
Automated Vulnerability Management: "Assess your risks"

After you identify your assets where vulnerabilities may be present, conduct a risk assessment by identifying vulnerabilities in those assets. Basic Vulnerability Management involves the ongoing and regular identifying, assessing, and reporting of cyber vulnerabilities across your endpoints and systems.

Tanium Comply streamlines and automates vulnerability and compliance assessments against operating systems, applications, and security configurations and policies.

Tanium Comply aligns with the Common Vulnerability Scoring System (CVSS), an open framework for communicating the characteristics and severity of software vulnerabilities. CVSS is maintained by the Forum of Incident Response and Security Teams (FIRST), which is a US nonprofit with over 500 contributing product security teams from the government, commercial, and academic sectors.

By reporting vulnerability metrics based on CVSS scoring, security teams apply a numerical (0-10) representation of severity to provide a point of comparison between vulnerabilities, making it simpler to prioritize remediation efforts.



Vulnerabilities with CVSS 3.0 Scoring

Basic Fundamental 3
Patches and Software Updates “Patch now or pay later”

After you assess your risks and prioritize remediation efforts, take action by applying patches and software updates. Hackers around the world are actively scanning for unpatched systems in order to exploit the vulnerability.

Attackers may target known vulnerabilities for months or even years after updates are available. The best course of action is simply to patch your way out of high risk danger at your earliest opportunity.

Cybersecurity and Infrastructure Security Agency (CISA) recommends enabling automatic software updates whenever possible.

Tanium Patch and Tanium Deploy deliver world class automation, speed, and scalability when it comes to patching operating systems and third party applications. The world’s largest organizations trust the Tanium Platform for delivering customized and effective patching solutions.

Another basic best practice that often gets overlooked is to avoid unsupported End of Life (EOL) software. Sometimes vendors will discontinue support for a software program, which means the vendor no longer releases updates, fixes, or security enhancements.

Use Tanium to find all your endpoint operating systems and applications in real time and check the end of life here: https://endoflife.date/

“Patch Now, or Pay Later.”

Hiring the right talent that aligns with your cyber security strategies.

There is no doubt the cybersecurity industry is complex and difficult. While malicious attacks are on the rise, and government cyber regulations are increasing, CISOs are facing major challenges in being able to handle cybersecurity issues effectively. Gartner surveyed IT executives and 75% of respondents cited that talent availability was the main challenge for adopting IT automation. Even with the right cybersecurity tools in place, organizations need experienced professionals who can execute and get the job done.

When it comes to investing in Tanium to protect your organization's most critical assets, it's vital to have the right people on your team with the knowledge and experience to guide you through the complex and difficult journey.

Finding the right people requires you to:

1. Assess your cybersecurity strategies
2. Define the skills and experience you are looking for
3. Research and learn about the potential candidates or managed service providers who can get the job done

Especially with critical and complex platforms like Tanium, you need highly specialized skills and experience. If you hire the wrong candidates, it can cost you.

About Chuco Managed Tanium Services:

Staffed by seasoned and certified Tanium experts, including the original leadership of Tanium's product engineering and customer success teams, Chuco's consulting business focuses solely on executing Tanium projects.

Organizations look to Chuco to implement and scale Tanium across environments ranging in size from as few as 5,000 to over 1 million endpoints. And we consistently deliver on their demanding requirements. We'll engage and execute in the way that best aligns with your cybersecurity goals and priorities.

Contact us to explore how we can support your cybersecurity strategies around the Tanium platform.

References:

- https://www.secpod.com/blog/best-endpoint-security-strategies-for-ciso/
- https://www.eccouncil.org/ciso-mag-study-1-in-3-cisos-feel-the-biggest-challenge-of-endpoint-solution-is-its-complexity/
- https://www.first.org/about/
- https://csrc.nist.gov/Projects/cybersecurity-framework/nist-cybersecurity-framework-a-quick-start-guide
- https://www.cisa.gov/uscert/ncas/tips/ST04-006
- https://docs.tanium.com
- https://www.tanium.com/platform/
- https://www.fbi.gov/news/press-releases/press-releases/fbi-releases-the-internet-crime-complaint-center-2021-internet-crime-report
- https://www.darkreading.com/vulnerabilities-threats/unpatched-vulnerabilities-the-source-of-most-data-breaches
- https://www.networkworld.com/article/3633191/gartner-it-skills-shortage-hobbles-cloud-edge-automation-growth.html