TANIUM

WHITEPAPER

Tanium for Cyber Insurance

The Power of Certainty

CONTENTS

Navigating the complexities of cyber risk management

In today's dynamic, digitally driven world, managing and protecting the thousands of devices that are connected to your network has never been more challenging. The teams and executives accountable for risk, compliance, and security engage in a constant battle against cyber threats across a technology environment that is comprised of millions of globally distributed, heterogeneous assets. Hardening your endpoints with Tanium's Converged Endpoint Management (XEM) Platform is crucial. Tanium provides real-time, precise data to help protect and enforce compliance on every managed and unmanaged endpoint within your environment.

In addition to Tanium, cyber insurance is a key tool to mitigate the associated risks. However, the underwriting process can be burdensome and result in missed opportunities for both the insured and the insurer. To alleviate this burden, Tanium has partnered with leading cyber insurers to provide a solution that enhances an organization's visibility into risks, expedites the underwriting process, and can lead to significantly improved cyber insurance policy terms, including premium discounts.

Alleviating the burden

Today, most organizations spend weeks and dozens if not hundreds of FTE hours filling out applications, questionnaires, and supplements from their brokers and prospective insurers to provide various measurements of risk and security posture that will determine their insurance eligibility, premiums, limits, and retentions. These assessments are:

1. **Manual:** Requiring weeks of employee time to complete
2. **Qualitative:** Not relying on verifiable data
3. **Static:** Only offering a point-in-time snapshot of an organization's posture

As a result, insurers are missing crucial data that could increase confidence in their underwriting decisions and insurance customers are missing opportunities to reduce premiums or increase limits due to demonstration of proper cyber hygiene. Additionally, without holistic tools to continuously assess cyber risk posture, companies—and insurers—lack critical risk trend visibility.

To resolve this challenge, Tanium has partnered with leading cyber insurers to deliver a solution to ease the underwriting burden on insureds and increase confidence in results for carriers.

This solution is the Tanium Risk Assessment – Cyber Insurance Supplement (TRA-CIS). With Tanium and the TRA-CIS, the underwriting process can be:

1. **Automated:** With structured reports that can query the relevant data
2. **Quantitative:** Relying on electronic data derived directly from endpoints
3. **Continuous:** With real-time results delivered at appropriate, agreed intervals throughout the year

Automating underwriting and remediating vulnerabilities

Through the TRA-CIS, Tanium enables organizations to obtain a comprehensive assessment of their cybersecurity posture in less than a week, with minimal manual intervention. This assessment, created in partnership with insurers, gathers key data across ten different categories. These are the most relevant for qualifying for and achieving optimized terms on cyber insurance.

Once a company conducts the assessment, the results can be easily and securely shared with the insurer. An important point to note: The companies that use Tanium always retain complete control of their data— including any results from the TRA-CIS. If the assessment finds areas that warrant improvement, companies can remediate any gaps and re-run the assessment before sharing.

The TRA-CIS greatly increases the insurers confidence in their customer's security and risk posture by focusing on factual outcomes vs. documented policies and perceived reality (for example, patching policies detail a desired state, whereas patching efficacy reports actual state and outcome). As a result, they are willing to offer significant premium reductions to their participating customers. This means that in addition to underwriting efficiencies and risk reduction through remediating detected vulnerabilities, participants can realize immediate and ongoing savings in their cyber insurance policies.

Assessing cyber risk for cyber insurance

The purpose of the TRA-CIS is to help cyber insurance customers and insurers gain complete visibility through automated data reporting of the environment, so optimal decisions on coverage and pricing are determined in a timely manner. The assessment provides an in-depth analysis of the digital estate and a Tanium-calculated, objective security risk score measuring a company's risk and operational resiliency. It identifies areas of security vulnerability and provides a prioritized list of critical actions to remediate identified exposures quickly.

The TRA-CIS risk score is determined through data collection across ten categories, identified by Tanium and insurers as key indicators of cyber risk, using widely accepted frameworks such as NIST II, as well as cyber intelligence reporting. The indicators are:

1. Security products and operations

Effective Endpoint Detection and Response (EDR) is a crucial first line of cyber defense, which proactively scans and blocks known and unknown threats before they reach the endpoint. Cyber insurers want to ensure policyholders are consistently employing EDR across the estate.

Tanium detects the presence of EDR software or other Endpoint Protection Platform (EPP) technologies and all usage of remote desktop software across the environment. Results show the percentage of endpoints with active, up-to-date protection present. Tanium can be used to deploy, repair, or update EDR software where it is not present, functioning, or out of date, as well as enable firewall policies.

2. Critical data

Personally Identifiable Information (PII) on endpoints, when improperly stored, can represent a significant liability for organizations. Mishandling of this data can lead to government sanctions through HIPAA or GDPR/CCPA frameworks. A breach that leads to the removal of this data opens an organization up to potentially millions of dollars in damages and fines. Insurers must be confident that any policyholders are not storing PII unnecessarily or improperly on endpoints.

Tanium scans for the presence of PII on endpoints (e.g., social security or credit card numbers) and returns results that indicate whether HIPAA, GDPR/CCPA, or other protected data is present. For endpoints where PII is appropriately present, Tanium looks for whether proper controls, such as USB write protection and encryption, are being employed. Tanium can be leveraged to enforce these controls if not present.

3. Vulnerability and response management

Vulnerabilities (e.g., malicious code) can exist undetected on an organization's endpoints for months or even years in some instances, despite a robust ecosystem of threat intelligence reporting to identify these threats. Even when identified, many organizations fail to resolve vulnerabilities expeditiously. According to industry reports, the average time to patch is often over a year. The ability of organizations to quickly identify known threats and remediate them is a critical area of risk reduction for cyber insurers.

Tanium determines the presence of commonly exploited vulnerabilities and exposures (CVEs) on endpoints, leveraging threat intelligence tracking and Cybersecurity and Infrastructure Agency (CISA) intelligence. For CVEs found, Tanium determines which are present on critical assets or publicly-facing environments and identifies which are known to have already been exploited in other environments.

For all environments, the assessment uncovers the hardened baseline configuration, compliance level, mean time to patch, and compensating controls (e.g., storage encryption, TPM status, DeviceGuard, CredGuard, RDP Restricted Admin, and much more) for all endpoints. Tanium can be used to bring endpoints into compliance and reduce mean time to patch to meet SLAs, if necessary.

4. Data storage and machines

Most organizations heavily leverage a mix of cloud and on-premises data storage. CISOs are often unaware of database servers more than any other endpoints. As such, these servers remain particularly vulnerable to exploitation.

Tanium reports whether database servers are present—either on-prem or cloud—and whether Server Message Block (SMB) is used. Tanium can apply relevant controls where necessary.

5. Endpoint detection and protection

Visibility into an organization's entire estate is critical to ensuring an organization is managing risk appropriately. However, 94% of organizations have undiscovered endpoints in their environments, according to industry research,[1] and over 70% of organizations have experienced breaches through unknown assets.[2] Clearly, cyber insurers must understand whether their policyholders have visibility into their entire estate.

Tanium conducts a holistic assessment of endpoints and the security posture of these endpoints. This includes the total number of endpoints detected in the environment, the percentage that have AV, allow automatic login, and other controls. Tanium can ensure all endpoints are running an AV tool and enforce user-machine policies.

6. Network controls and considerations

Network-based attacks have long been a common vector for cybercriminals and other threat actors. Improperly configured, weak, or absent firewalls, certificates, and other network-focused security protocols can increase an organization's risk and leave it exposed to a costly attack. Cyber insurers are focused on reducing network-based risk.

Tanium drives an understanding of network security and controls, such as firewall usage, physical sites, SSL, TLS, insecure HTTP connections, and domains being used.

References:

1. https://www.cio.com/article/410183/dont-have-real-time-visibility-and-control-over-your-endpoints-your-business-may-be-at-risk.html

2. https://www.scmagazine.com/news/most-organizations-had-an-unknown-or-unmanaged-internet-facing-asset-exploited

7. Identity access management

Organizations must ensure endpoints have sufficient password controls and that users are changing them at consistent intervals since attackers can more easily breach endpoints with weak, old, or non-existent passwords. Insurance policyholders must close this vulnerability to limit risk.

Tanium identifies and reports password requirements and related policy compliance on endpoints and can configure endpoint configuration and enforce policies.

8. End-of-support and end-of-life considerations

Endpoints running end-of-life/support software or operating systems can be exploited by malware more easily than current, up-to-date applications. Tanium identifies endpoints running end-of-life applications and OS and can update all third-party software and perform in-place upgrades of the OS (or image endpoints with new OS if desired).

Tanium can also report on all end-of-life software exposed to known vulnerabilities to assist in prioritizing remediation activity.

9. Service account management

Understanding and managing access rights is vital to reducing and managing your organization's attack surface. Tanium can visualize and contextualize an organization's administrative realm for improved management and reduced risk, identify and report usage of service accounts, and assess the over-permissiveness of administrative rights that could fuel lateral movement during a security incident/breach.

10. Domain management

Ensuring properly encrypted connections to internet domains through SSL and other certificates reduces an organization's threat vectors. Expired, or self-signed, certificates increase an organization's exposure and must be understood during the insurance underwriting process. The Tanium assessment identifies the certificates used and highlights those that are expired, self-signed, or are otherwise a potential weakness (e.g., weak signature hash, short key, etc.). Tanium can provide ongoing visibility into the estate's certificates.

Making it happen

Running the TRA-CIS in your organization is one of the easiest ways to address your cybersecurity risk posture. Most organizations have results from the assessment back within days.

To get started, please contact Tanium for a demo

Schedule a demo