



CAPGEMINI – POWERED BY TANIUM

MANAGED VULNERABILITY SCANNING

Asset vulnerabilities and simple application misconfigurations lie at the heart of most breaches

Capgemini 

TANIUM.

Whilst zero-day threats and advanced malware get all the headlines, known asset vulnerabilities and simple application misconfigurations lie at the heart of most breaches. Keeping your organisation safe means continuously scanning your endpoints for vulnerabilities and misconfigurations, quickly analysing and prioritising the issues you find, and fixing them before they become a problem.

Unfortunately, many vulnerability management tools are:

SLOW: Scans take days or weeks to complete, ultimately serving stale data.

Siloed: They don't work together, isolating security and operations teams.

INEFFICIENT: They consume heavy bandwidth, impacting on-going network performance.

LIMITED: They lack end-to-end visibility, resulting in blind spots and missed dangers.

INCOMPLETE: Finding vulnerabilities is just the start – it's what you do with that information that really determines the security of your organisation.

Vulnerability Management-Program Drivers and Emerging Trends

31%

of companies detected attempts to exploit software vulnerabilities

Organisations required an average of

84 days

to remediate high risk vulnerabilities

Unpatched vulnerabilities are involved in

60%

of data breaches

183%

increase in vulnerabilities since 2015

80%

public exploits are published before the CVEs are published

Source: Tanium

YOU CAN'T PROTECT WHAT YOU CAN'T SEE

THE TANIUM PLATFORM

The line between business and personal computing is blurrier than ever. Employees now routinely use personal devices for work tasks, rely on company devices and software at home, and skirt IT policies by using unapproved applications. This reality poses increasing security and operational challenges and threats for every kind of organisation.

Complete visibility

Find devices within distributed networks – even if they don't have a Tanium agent – and determine whether they carry vulnerabilities, misconfigurations, or other risks. Decide whether you want to bring them under management, or block them from your network.

Use it as you need it

Assess large-scale distributed endpoint environments, without generating meaningful network strain, to collect accurate, real-time vulnerability intelligence anytime you want it.

Single, intuitive interface for all stakeholders

Seamlessly pivot between risk assessment and remediation by unifying IT operations, security and risk teams within a single dataset and platform.

Rigorous compliance

MVS supports the Security Content Automation Protocol (SCAP), can use any Open Vulnerability and Assessment Language (OVAL) content, and uses Capgemini's own content library that's updated daily with vulnerability, compliance, and CIS definitions and benchmarks.



FROM CAPGEMINI

MANAGED VULNERABILITY SCANNING

Capgemini combine global expertise and experience with a best-in-class visibility platform to deliver on-going, pro-active protection against all known vulnerabilities. Building on Tanium's single, modular, agent-based platform, Managed Vulnerability Scanning (MVS) takes the hassle – and the risk – out of the vast majority of established vulnerability management processes.

Rolling Discovery

The most basic of vulnerabilities is an unmanaged asset. At the heart of Capgemini's Managed Vulnerability Scanning service lies Tanium's light-weight visibility platform – its ability to locate and identify every asset, without any noticeable impact on network performance, allows for near real-time asset discovery across even the most dynamic of environments.

Customised Expertise

Your organisation has a unique vulnerability profile: from the industries and markets in which you operate, to the tech stack you've built over the years, to the day-to-day demands of your users and customers, not only are no two businesses the same... no two days are the same! With 15 global SOCs relentlessly investigating the latest threats to organisations across every territory, vertical and tech make-up, your Capgemini team will work with you to provide an insight into your vulnerabilities that maximises security without ever losing sight of your wider business objectives.

Frequent Scanning

Between malicious actors, careless users and failing assets, things can change in an instant. Infrequent, cumbersome scans are out of date as soon as they're completed – Tanium's single-agent approach supports multiple scans a day, providing near real-time dashboards that help you understand, analyse and remedy any vulnerabilities before they can be exploited.

Rapid Remediation

Comprehensive coverage, a single-point-of-management and advanced automation all work together to give you total control over your vulnerability management processes. Capgemini's Vulnerability Scanning service – particularly alongside our Patching-Platform-as-a-Service – gives you and your team complete confidence that your critical cyber security measures are being built on the strongest possible foundations.

TURNING INSIGHT INTO ACTION

Knowing everything that's going on across your entire IT landscape is enormously important, but it's what you do with that information that really sets your business apart. Capgemini's experts don't just help you plan, deploy and manage the best-in-class visibility provided by Tanium, they're on hand to turn the huge quantities of data produced into concise, actionable information, and to take full advantage of everything comprehensive visibility has to offer.

An end-to-end Visibility & Management Solution that keeps your business secure, agile, and efficient.



Asset Optimisation

combines comprehensive real-time visibility with business intelligence to keep your IT landscape resilient, agile and efficient – ensuring the maximum possible return on every cent you invest in your network.



CMDB Population & Support

leverages the wealth of data provided by the Tanium platform to deliver invaluable insight into your estate. Working with Capgemini, you'll design and implement a CMDB that supports your wider business objectives, drastically simplifying management and increasing efficiency whilst also providing an utterly reliable source of information to anyone who needs it.



Patching Platform as a Service

takes all of the hassle out of the crucial patching process. Taking advantage of Tanium's end-to-end real-time visibility, Capgemini will manage every step: from scanning for patch applicability, assessing the risks, and ensuring patches are applied successfully, Patching Platform as a Service turns a never-ending security imperative into something you can manage with just a single click.



Vulnerability Scanning

from Capgemini leverages the technical excellence of the Tanium platform to find, analyse and resolve the vulnerabilities at both application and OS level. A dedicated team identify vulnerabilities, analyse their impacts, and provide comprehensive mitigation recommendations to resolve any issues.



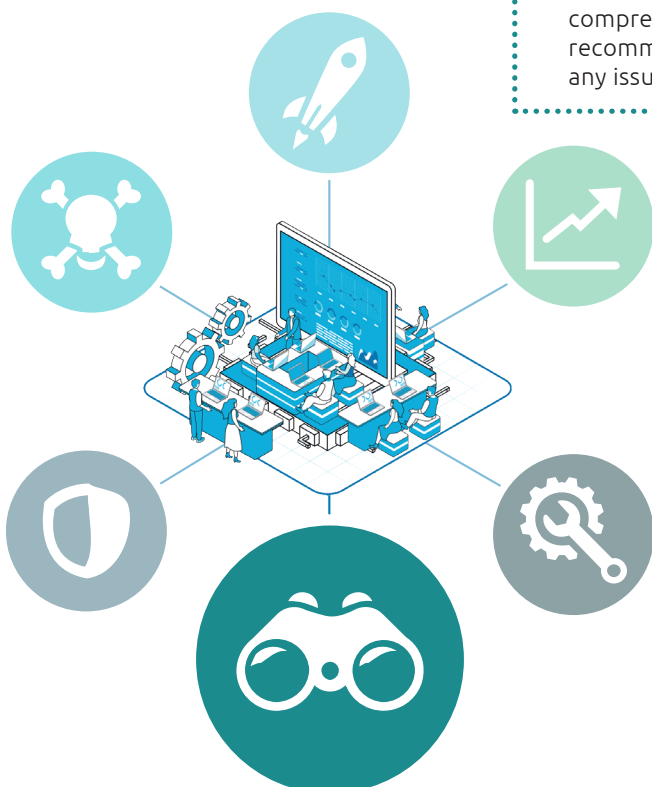
Managed End-point

Detection & Response turns Tanium's Endpoint Detection system into Capgemini action. Constantly monitoring all endpoints for indicators of compromise, your Capgemini team are ready-and-waiting to identify, analyse and respond to every malicious action.



Active Threat Hunting

offers the ultimate protection for your IT environment. Our ATH teams call on the latest research, our global network of Security Operations Centres, and a deep understanding of how malicious actors think, to constantly keep your business one step ahead. By hypothesising about possible threats, and using the Tanium platform to check your landscape for missed vulnerabilities or lurking intruders, Active Threat Hunting delivers pro-active network security.



For more details, contact:

Capgemini Nederland B.V.
Reykjavikplein1
3543 KA Utrecht
Postbus 2575 - 3500 GN Utrecht
+31 (0)30 203 0500

Visit us at
www.capgemini.com