CAPGEMINI – POWERED BY TANIUM

ACTIVE THREAT HUNTING

Cyber security is an arms race – keeping your IT landscape protected against the latest known threats is crucial

Keeping your IT landscape protected against the latest known threats is crucial, but malicious actors dedicate their lives to coming up with new and creative ways to evade detection. Unfortunately, stopping them a million times can go by completely unrecognised whilst the implications of a single breech – whether lost customer confidence, intellectual property theft or fines for data security non-compliance – can be catastrophic!

68%

of incidents take months to be discovered

Source: Tanium

Active Threat Hunting from Capgemini

Whilst a well-implemented Managed Endpoint Detection & Response solution can handle the vast majority of incidents, they ultimately rely upon detecting known threats. This does allow for massive scale and automation, but it encourages attackers to focus on staying one step ahead by developing new approaches.

The only way to truly protect yourself against constantly innovating threats is to beat malicious actors at their own game – with a team of experts better at what they do than the attackers themselves!

BECOME PART OF A WORLD-WIDE NETWORK OF EXPERTISE

GLOBAL EARLY WARNING SYSTEM

New threats can emerge anywhere, and malicious actors will often refine their techniques in the shadows before turning their attention to you and your organisation. Capgemini's 15 global SOCs, co-ordinating hundreds of cyber teams, constantly share developing information across the network – giving your ATH team all the time and information they need to keep you one step ahead of your attackers.

INDUSTRY INSIGHT

Whilst some threats are universal, others are designed to exploit the way specific industries operate. Over the years - working in every vertical in every market – we've amassed enormous insight into how to best protect against the attacks to which you're most vulnerable.

LOCAL KNOWLEDGE

Access to Capgemini's global network ensures there's always an expert on hand to help with languages, behavioural analysis and regional threat profiles.

TECHNICAL SPECIALISTS

It's not unusual for malicious actors to focus on a particular technology or service. Capgemini meet them head on with a range of hugely experienced specialists, each dedicated to identifying potential problems with – and defences for – every element of your tech stack.

YOUR UNIQUE THREAT PROFILE

An Active Threat Hunting team acts as the conduit between your organisation and Capgemini's ever-vigilant global taskforce. Backed by huge volumes of specialist knowledge, continuously gathered from around the world, they'll take the time to truly understand your business and IT landscape – developing a focussed approach that keeps everything secure whilst never losing sight of your wider business demands.

IMPACT WITHOUT DISRUPTION

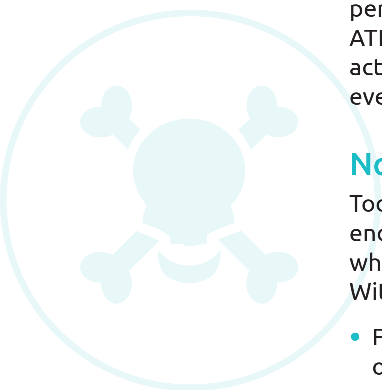
The comprehensive yet light-weight visibility and control offered by Tanium allows our ATH teams to conduct extensive 'identify and eliminate' operations without any impact on overall business performance – leaving them free to be as creative and ruthless as they need to be!

1	Hypothesise	Combine an international knowledge base with creative thinking to imagine ways in which your specific organisation might be vulnerable
2	Explore	Leverage Tanium visibility and on-demand data collection to run targeted checks across all relevant endpoints for Indicators of Compromise
3	Analyse	Analyse results to determine exactly what actions might need to be taken, including covert observation to learn more about the threat
4	Respond	Repel attackers, conduct wider search to ensure no further threat exists, work out whether any damage has been done, and dig further into the circumstances that led to the incursion
5	Protect	Whether or not it had already been exploited, our experts will help you close vulnerabilities and ensure you're protected against similar attacks
6	Repeat	With the size and complexity of modern networks, and the potential rewards for successful attackers, Active Threat Hunting never stops!

SECURITY STARTS WITH VISIBILITY

THE TANIUM PLATFORM

Whilst re-active detection and response measures are a crucial part of any cyber security solution, they're limited in the types of threats they can handle. To be truly secure you need to give experts the freedom to think outside of the box – but coming up with a potential vulnerability is of no use if you can't actually do anything with that information!



The Tanium platform is designed to provide real-time visibility into even the darkest corners of your IT landscape. The ability to run customised analysis using up-to-the-minute information – without impacting network performance – gives Capgemini's ATH teams complete freedom when pro-actively protecting your organisation against even the most innovative of attacks.

Nowhere to hide

Today's diverse, dynamic and distributed endpoints create a complex environment in which threats can lurk undetected for months. With Tanium we make it easy to:

- Find every endpoint, whether local, remote, on premises or cloud
- Identify active users, network connections and other threat data for each endpoint
- Visualise lateral movement paths that attackers can follow to access valuable targets
- Verify policies and identify gaps in key controls

Act in seconds

Only once you can see everything can you be confident you're missing nothing. Capgemini leverage Tanium's visibility to track down and root out even the most well-hidden of threats:

- Run custom scans to look for unknown threats that signature-based endpoint tools miss
- Investigate an individual endpoint – or your entire environment - in minutes, without creating large network strain
- Conduct further in-depth analysis for anything unexpected you do find

Everything on a unified platform

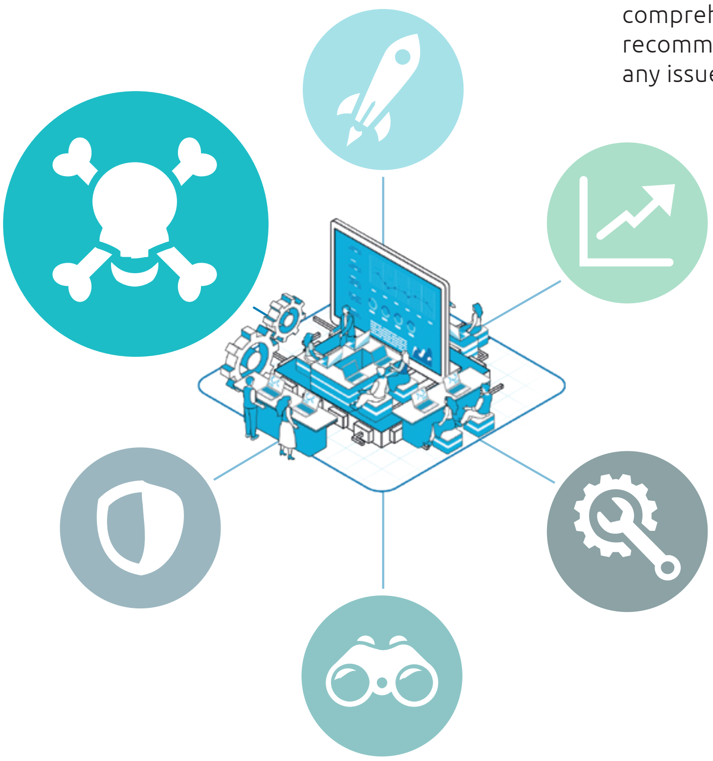
Many endpoint tools separate threat hunting from remediation, which creates friction between teams, delays response and leaves threats active. With Tanium we make sure we:

- Unify threat hunting and response with a single dataset and platform
- Enable agile and effective collaboration across multiple teams and departments
- Ensure complete understanding of any incident to deliver continuous improvement

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