



CAPGEMINI – POWERED BY TANIUM

MANAGED END-POINT DETECTION & RESPONSE

Comprehensive cyber security is more
challenging – and important – than ever

Capgemini 

TANIUM.

Comprehensive cyber security is more challenging – and important – than ever. Malicious actors are becoming more creative, the potential impacts of a breach are rising, and ever-evolving IT environments create a threat landscape that never stands still.

Organisations must find a way to maintain business-critical security across thousands of diverse, dynamic and distributed assets... without any noticeable impact on day-to-day business activities!

Unfortunately, this often means deploying a range of point solutions that make collecting, understanding and responding to potential threats slow and inefficient – exactly when you need speed and clarity.

in **93%**
of cases the attacker can
breach the network*

50%
more cyber attack attempts on
businesses per week in 2021*

*Source: <https://www.forbes.com/sites/chuckbrooks/2022/01/21/cybersecurity-in-2022--a-fresh-look-at-some-very-alarming-stats/>



FROM CAPGEMINI

MANAGED END-POINT DETECTION & RESPONSE

Capgemini combines global expertise with best-in-class visibility to offer an EDR service that evolves alongside your organisation. Building on Tanium's modular, agent-based platform, MEDR replaces the complexity of multiple point tools with a single end-to-end service that enhances everything from essential threat surveillance to cross-team collaborative responses.

| | | |
|---|----------|--|
| 1 | Detect | Continuously monitor endpoints to rapidly identify and address anomalies and Indicators of Compromise |
| 2 | Analyse | Quickly evaluate detected and potential threats with an expert team that deliver actionable insights, in-depth reporting & intuitive analytics |
| 3 | Plan | Develop quick containment, strategic mitigation and remediation recommendations designed to minimise impact whilst responding to the threat |
| 4 | Repel | Deploy co-ordinated managed responses by multiple teams from a single centralised console offering real-time visibility and control |
| 5 | Automate | Streamline responses and reduce workloads by taking full advantage of advanced automation capabilities |
| 6 | Protect | Conduct end-to-end review of the incident to educate users, improve processes and ensure greater overall resilience against future attacks |

SEE EVERYTHING, EVERYWHERE

Between Capgemini's insight into the cutting-edge of the global threat landscape, and Tanium's comprehensive visibility into even the darkest corners of your IT environment, there's no better way to avoid potentially catastrophic surprises.

GLOBAL KNOWLEDGE-BASE

Work alongside our 15 global SOCs and leading 3rd party services to ensure you're always using the latest threat intel.

CONSTANT MONITORING

Track an ever-changing IT Landscape to continuously find eliminate blind-spots and vulnerabilities.

BESPOKE THREAT PROFILE

Develop and deploy EDR processes designed for your specific organisational challenges and objectives.



YOU CAN'T PROTECT WHAT YOU CAN'T SEE

THE TANIUM PLATFORM

Before you can respond, you have to detect. Every gap in your surveillance is an opportunity for an attacker, and it's only a matter of time before you'll find yourself blind-sided. The foundation of the Tanium platform is visibility: taking advantage of its low-impact, high-efficacy insight into even the darkest corners of your IT landscape, Capgemini's MEDR service really does keep you covered.



Constant Surveillance

Many teams rely on an array of disconnected and fragmented point tools providing incomplete data, which is hours, days, or even weeks old – disastrous during a cyber attack, when every second is critical. With the Tanium platform Capgemini continuously monitors endpoints, rapidly identifying anomalous activities and Indicators of Compromise and alerting key parties in real-time.

On-demand Insight

Many EDR solutions struggle to deliver the real-time information you need when an incident is unfolding. Tanium gives Capgemini MEDR teams the ability to conduct on-demand searches throughout your entire IT environment in seconds, allowing them to bring all of their insight and expertise to bear during an unfolding incident.

Combine Analysis and Action

The coverage and control provided by Tanium allows Capgemini MEDR teams to analyse an attack as it's occurring, and then act on that information in the most efficient and effective way possible. A single up-to-date data stream and centralised management console make it possible to take decisive action across hundreds of thousands of systems simultaneously.

Constantly Evolving Protection

It's not enough to just repel an attack – to protect your organisation in the future, you must be able to see exactly what is happening. The Tanium platform collects and preserves a huge range of forensically relevant endpoint telemetry, providing detailed and precise information about every attack that ensures you're able to understand and eliminate the threat.

37%

of all businesses/organisations
were hit by ransomware in 2021

Source: Tanium

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.



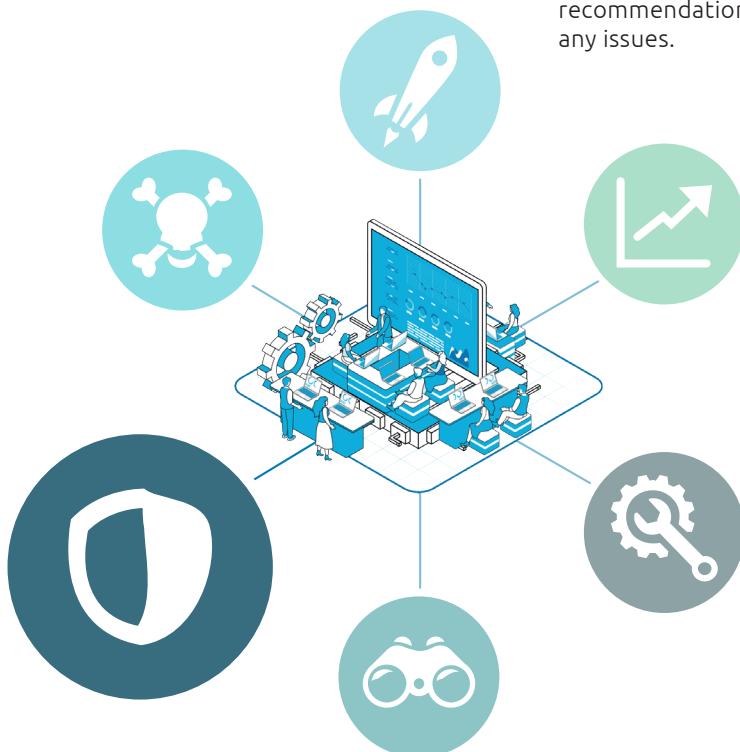
Managed End-point Detection & Response

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