Tanium Incident Response

Thank you for downloading this Tanium resource. Carahsoft is the official government distributor for Tanium cybersecurity solutions available via GSA, NASA SEWP V, CMAS, and other contract vehicles.

To learn how to take the next step toward acquiring Tanium's solutions, please check out the following resources and information:

For additional resources:
carah.io/taniumresources

For upcoming events:
carah.io/taniumevents

For additional Tanium solutions:
carah.io/taniumsolutions

For additional cybersecurity solutions:
carah.io/cybersecurity

To set up a meeting:
tanium@carahsoft.com

703-673-3560

To purchase, check out the contract vehicles available for procurement:
carah.io/taniumcontracts

For more information, contact Carahsoft or our reseller partners:
Tanium@carahsoft.com | 703-673-3560

SOLUTION BRIEF

Tanium Incident Response

Accelerate your incident response with augmented SIEM and EDR, increased SecOps collaboration, and advanced threat detection.

Dramatically reduce your Mean Time to Resolve (MTTR) for security incidents. Tanium augments SIEM and EDR – provides visibility to blind spots and replaces a stack of siloed point tools – to accelerate and improve your end-to-end incident detection, threat hunting, investigation, containment, and remediation capabilities – all from a single platform.

Your challenge: Slow responses lead to prolonged incidents, more downtime, and more damage

The data are clear. The sooner you investigate and remediate an incident, the less harm you will suffer. Yet despite heavy investment in SIEM and EDR tools, organizations still struggle to investigate incidents fast enough to remediate them before they cause harm. At a time when large organizations are losing $500K per hour to downtime caused by cyberattacks, 80% of the Mean Time to Resolution for these IT incidents is eaten up by investigations – the average forensic investigation taking 30 days to complete.

And once an organization completes their investigation, they then need to switch to a stack of complex, siloed point tools to remediate it.

The result?

500K per hour

Average cost of an enterprise outage

30 days

Average time to complete a forensic investigation of a security incident

80%

of Mean Time to Resolution of a security or operational incident is spent on investigation

50%

of incidents, intruders had access inside an organization for two weeks or more before detection or discovery

Not enough data

IT and security teams lack an optimized means to hunt with real-time data, vet alerts, gain visibility and context into incidents, and surgically contain attacks when they occur.

Slow investigations

Organizations take too long to access all the investigation data they need to identify the root cause – and recover from incidents – before significant harm occurs.

Too many tools

Investigation and IT ops teams are using too many tools to get the data they need, and they lack a shared workspace and views to seamlessly work together in a simple and efficient manner.

> "Without the visibility that Tanium supplies, we wouldn't be able to grapple with the ever–present security threats."

Tom Barker
Chief Security Officer,
BAE Systems

Your solution: Rapid, comprehensive incident response with Tanium

Tanium Incident Response solution augments and extends the capabilities of SIEM and EDR tools while replacing a stack of investigation and remediation point tools with a single, unified platform. By doing so, it provides every core capability you need to move from incident detection to remediation in one tool – while rapidly accelerating and improving your investigations.

With Tanium, you will:

- Gain real-time access to mission-critical incident data that SIEM and EDR tools do not provide, giving security teams all the endpoint data they need for hunts and investigations
- Access a single tool to efficiently analyze all the endpoint data you need to complete your hunts and investigations – along with a shared workplace where teams can collaborate
- Seamlessly switch from incident investigation to containment and remediation through a full suite of surgical capabilities built into a single console
- Enable teams to augment the threat intelligence (TI) from your SIEM and EDR vendors with additional TI in a way that can be easily managed and executed at scale

Detect, investigate, and hunt incidents

Discover incidents in-progress, investigate what caused them, and determine the full scope of the threat and how to stop it

You need a wide range of current and historical data to find and investigate incidents in full. While SIEM and EDR tools can point you in the right direction of an attack, they lack the complete set of data and telemetry you need to complete your hunts and investigations. But with Tanium, you can:

- Augment your SIEM and EDR's threat intelligence with organizational, community, and additional third-party intelligence
- Give threat hunters and incident investigators all the real-time data, queries, and insights (e.g., lateral movement) they need to fully scope an attack and its impact
- Enable security and IT ops to efficiently work together using a shared workspace that enables them to share investigative data, assign tasks, communicate, and work as a team to resolve incidents

Contain discovered threats and incidents

Automatically contain threats to stop them from spreading and causing further harm before you remediate them

After an incident is discovered and investigated, it must be mitigated and contained quickly. Yet SIEM and EDR tools lack the tailored response capabilities needed to contain an attack with minimum disruption and impact. But with Tanium, you can:

- Automatically perform surgical containment including isolation and quarantining at scale in real time
- Customize isolation and quarantine actions – totally isolate impacted endpoints or allow targeted connections
- Apply temporary or long-term mitigation actions to impacted or at-risk endpoints, including AppLocker, firewall changes, etc.

Resolve incidents and get back to operations ASAP

Stop the incident, evict the attacker, restore normal business operations, and harden against future incidents

Once an incident is contained it must be resolved, and any impacted endpoints must be restored to a secure and compliant state. SIEM and EDR lack a complete set of remediation capabilities and leave the solution of these tasks to a patchwork of other tools. But with Tanium, you can:

- Pivot from incident alert, to investigation, to remediation actions from within the same console and platform
- Perform real-time remediation actions on a single endpoint, a group of endpoints, or to every endpoint in the organization at once
- Save detection and remediation procedures that automatically apply to offline endpoints as soon as they reconnect to the network

Extend your SIEM and EDR tools, and gain a single, central platform to complete every stage of incident response, and to get to the finish line of threat remediation ASAP

Tanium gives you a range of benefits to accelerate incident response and remediate issues of any type in real time.

Complete visibility

Collect every piece of data you need on-demand in real time to investigate and remediate an incident. Tanium extends the built-in threat intelligence from SIEM and EDR tools with the organizational, community, and third-party data you need to handle advanced, targeted, and novel threats.

- Leverage historical and real-time data to better assess incidents and bring endpoints back to a compliant and secure state
- Scope the entire breadth and depth of an incident across every endpoint in the environment in seconds
- Discover attacks other tools can't see by hunting for threats using any possible piece of endpoint data in real time
- Improve your signal-to-noise ratio by quickly spotting false positive alerts and focusing only on real incidents
- Follow rich experiences that provide insights, help identify root causes and potential lateral spread, and direct investigators to the context and data they need most

Integrated collaboration

Break down siloes between the teams and experts involved in an investigation. Tanium gives you an integrated workspace where every investigator can share insights, historical and real-time data, and work together to analyze what happened and how to best stop it.

- Break down siloes between investigators and domain experts through experiences that foster collaboration at every stage of investigation
- Build a single integrated view that everyone can follow to work with and analyze 100% of the endpoint data required
- Create a shared workspace for teams to collaborate on hunting and investigating an incident
- Connect IT ops and security teams and let them seamlessly pivot through each stage of incident response from one platform
- Set granular role-based access controls to let teams work together and delegate capabilities in a manner that makes sense for your workflows

Real-time remediation

Move seamlessly from incident investigation to remediation within the same platform. Tanium offers a comprehensive set of remediation capabilities that can address any operational or security incident – at any scale, in real time, across every service and asset in your infrastructure.

- Contain incidents in either a surgical manner to minimize disruptions, or in a more sweeping manner when a bigger level of risk is detected
- Deploy any remediation capability needed to bring each endpoint back to a secure and compliant state in real time
- Repair any change made by an attacker on any of your endpoints located anywhere in your environment
- Leverage dynamic and extensible remediation capabilities to orchestrate advanced multi-step remediation actions
- Create custom dashboards to monitor remediation actions, ensure they have been executed correctly and completely, and to confirm the incident won't re-emerge

REQUEST A DEMO

Let us show you how Tanium's Incident Response solution accelerates detection, investigation, containment, and remediation – at any scale.

Learn more →

Tanium, the industry's only provider of converged endpoint management (XEM), leads the paradigm shift in legacy approaches to managing complex security and technology environments. Only Tanium protects every team, endpoint, and workflow from cyber threats by integrating IT, Compliance, Security, and Risk into a single platform that delivers comprehensive visibility across devices, a unified set of controls, and a common taxonomy for a single shared purpose: to protect critical information and infrastructure at scale. Visit us at www.tanium.com.