TANIUM

WHITEPAPER

How Tanium Threat Response Augments Endpoint Detection and Response (EDR) and SIEM solutions

Using Tanium Threat Response with your existing Endpoint Detection and Response (EDR) solution delivers expedited incident response and real-time hunting.

CONTENTS

Complete investigations more quickly and hunt with real-time arbitrary data.

Whether you're responding to alerts or conducting a hunt, once an attack has been detected, it is quite literally a race against the clock to investigate and respond.

As analysts investigate incidents and conduct their hunts, they will take advantage of a rich body of information and investigation experiences found in their Security Information and Event Management (SIEM) and Endpoint Detection and Response (EDR) solutions. Combined, these tools will give analysts a good but often incomplete sense of the extent of the attack. Analysts almost always need more visibility and control than what those solutions can offer. They need to have a high-fidelity real-time picture of exactly what has transpired and may still be lurking in the shadows.

Though SIEM and EDR solutions provide a lion's share of this information, there is threshold that many investigators run into – a point where visibility ends and forces analysts to bring in additional tools to complete the picture. This is often the long tail of the analyst's workload and requires additional expertise and where analysts spend much of their time.

Organizations measure their performance against these challenges with KPI's like Meantime to Detect (MTTD), Investigate (MTTI) and Respond (MTTR) and if you're like your peers, you're always looking for new ways to improve the numbers. Organizations have long waited for their existing SIEM and EDR providers to deliver the capabilities necessary to address this long tail of the work, but the reality is SIEM and EDR solutions are not well suited to address these remaining needs. Consequently, they've left these capabilities for others to fulfill.

Needs unaddressed with SIEM and EDR solutions.

There are several categories of critical capabilities that SIEM and EDR vendors do not provide that require additional tools and processes including:

- Investigations require access to additional data, which we refer to as arbitrary data, that go beyond what SIEM and EDR solutions have been designed to collect. Other tools are used to acquire this data on demand and it at scale which is a time-consuming task
- Analysts need the ability get real-time endpoint state data from endpoints at scale (e.g.: setting or registry key states, file). They need to be able to get this data along with historical state date to detect anomalous changes
- SIEM and EDRs collect data on a periodic cadence that varies by the source and data type so data can be minutes, hours or even older. Access to real-time data from endpoints is a requirement to successfully complete investigations and hunts

- SIEM and EDRs have data collection and retention rules that inevitably drop data, leading to gaps and missing context that is needed to complete investigations and hunts

- Beyond basic containment tools SIEM and EDRs do not provide a complete set of containment capabilities nor the ability to remediate and bring endpoints back to a secure and compliant state

- Many solutions lack comprehensive visibility to all endpoints leading to blind spots and complexity when attempting to assess the totality of the attack

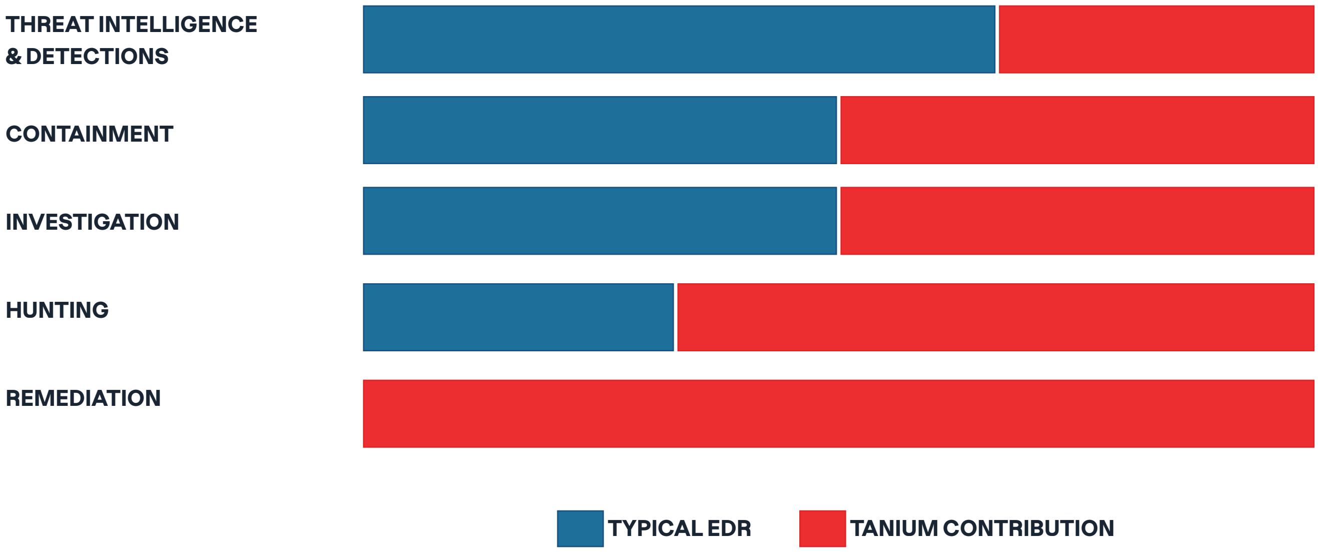
Solution

Using Tanium Threat Response in concert with your existing SIEM and EDR solutions provides your Security Operation Center (SOC) with an opportunity to dramatically expedite their work by reducing the complexity and friction analysts experience during investigations and hunting tasks.

Your SIEM and EDR investments will continue to be the primary experience for detections and to begin investigations and hunts, however with Tanium being used in conjunction you will be able to consolidate the many additional tools your teams are using to complete the long tail of their investigations and hunting processes.

With Tanium you can now:

- More easily add and manage custom detections to your environment
- Execute advanced containment and environment hardening mitigations to constrain attackers and stop attacks beyond just isolating compromised devices
- Gather and query all of the real-time, historical and forensic data you need to make sense of an incident or conduct a hunt, rather than just what you can afford to bring into your SIEM
- Conduct complete remediation actions at scale to bring impacted endpoints and services back to a secure and compliant state.



Combining your SIEM and EDR tool set with Tanium will enable your team to achieve higher levels of efficacy and boost performance for key SOC KPI's. With Tanium you'll empower all of your analysts and hunters to perform more advanced investigations and hunting tasks. They'll be able to conduct them with fewer tools, less expertise and at much greater speeds.

Tanium additive capabilities to EDR and SIEM

Investigation

Tanium provides analysts with the broad range of capabilities they need to complete the time-consuming long tail of their investigations, and it enables them to complete them with greater confidence, speed and accuracy.

Specifically, Tanium provides the ability:

- To perform investigations using real-time data which is needed to fill in the visibility and timeline gaps that SIEM and EDR solutions have which collect data on a cadence and make them a view into the past
- For analysts investigating an incident to access arbitrary data (i.e.: additional data not collected by the EDR or SIEM) of any type (e.g.: files and contents, reg keys, env variables, file handles, mutex objects, PowerShell execution, browser activity, etc.)
- For analysts to access configurable historical data, including arbitrary data not normally collected by the EDR or SIEM due to performance and cost implications. Decentralizing the storage of data to the endpoints themselves provides analysts with access to the richest possible historical data set
- To get access to all event data from your endpoints. None of the event data needs to get filtered, transformed or dropped to address the performance and storage implications of centralized storage
- To customize the forensics data set to acquire and collect it at scale which is typically challenging to perform efficiently
- To scope the breadth of an attack across all endpoints using queries that can leverage real-time and even historical data (e.g.: get list of endpoints that have vulnerable instances of log4j on them, look for endpoints that have a specific file)
- To compare data/states on endpoints over time, including long term historical data, to see if there are abnormalities or outlier issues
- To investigate incidents using customized signals (e.g.: child process from word != X) in real-time and at scale for sniper work that can be crafted to contextually match the organization or investigation exercise being done
- To import TI and create and run custom IoCs (e.g., YARA, STIX-TAXII, OpenIOC) and run them at scale, in a safe performant manner
- To look at any endpoint and understand identity related lateral movement opportunities that an attacker may have been able to exploit with a compromised endpoint or identity
- To create, execute and save simple but detailed verification queries using natural language
- To create custom dashboards to monitor and ensure that the remediation actions taken have been executed correctly, completely and confirm reemergence has not occurred

Hunting

Tanium provides hunters with a broad range of added capabilities that are complementary and augment their EDR and SIEM hunting experiences. It provides them with the capabilities they need to complete their hunts using live and more detailed data.

Specifically, Tanium provides the ability:

- To hunt using real-time data which is needed to fill in the visibility and timeline gaps that SIEM and EDR solutions have which collect data on a cadence and make them a view into the past
- For hunters tracking down a hypothesis to access real-time arbitrary data (i.e.: additional data not collected by the EDR or SIEM) of any type (e.g.: files and contents, reg keys, env variables, file handles, mutex objects, PowerShell execution, etc.)
- To hunt with configurable historical data, including arbitrary data not normally collected by the EDR or SIEM due to performance and cost implications. Decentralizing the storage of data to the endpoints themselves provides hunters with access to the richest possible data set without raising storage costs
- For hunters to get access to all event data from your endpoints. None of the event data needs to get filtered, transformed or dropped to address the performance and storage implications of centralized storage
- To hunt using customized signals (e.g.: child process from word != X) in real-time and at scale for sniper hunting that can be crafted to contextually match the organization or hunting exercise being done
- To pivot from a hunt finding to codified intel and validations that analysts can use to more quickly execute incident response
- For hunters to import TI and create and run custom IoCs (e.g., YARA, STIX-TAXII, OpenIOC) and run them at scale, in a safe performant manner
- To hunt for threats based on outlier behavior specific to their enterprise and create new detections based on the specific threat discovered.

Remediation

Tanium empowers incident response teams to play a greater role in the remediation process and to collaborate with IT Ops using the same tools. It equips them with the capabilities they need to take any action needed to bring devices back to a pre-breach state which can be executed in real-time and at scale.

Specifically, Tanium provides:

- Granular role-based access control capabilities to enable IT Ops and IR (Incident Response) teams to partner together and delegate remediation capabilities as makes sense for their organization
- The ability to pivot from an alert to data about configuration changes (e.g.: services installed, files added, registry keys modified, processes running) made to the endpoint, to the remediation actions necessary to bring the endpoint back to a pre-breach state in real-time
- Advanced targeting options that enable the real-time execution of remediation actions to a single endpoint, a select set of endpoints or even enterprise wide as is needed
- Dynamic and extensible remediations capabilities to orchestrate advanced multistep remediation actions (e.g.: low code or script-based remediation)
- To create, execute and save detection and remediation procedures that can execute automatically when previously offline endpoints reconnect to the network
- To create, execute and save simple but detailed verification queries using natural language
- To create custom dashboards to monitor and ensure that the remediation actions taken have been executed correctly, completely and confirm reemergence has not occurred

Containment

Tanium provides additional high value multi-platform containment and constraint options to complement those from your EDR vendor.

Specifically, Tanium provides:

- Containment options such as isolation/quarantine that can be executed at scale across impacted endpoints, or even more broadly, in real-time
- The ability to customize the isolation/quarantine behavior. Analysts can choose from options to totally isolate a device or they can decide what endpoints and services can continue to be contacted
- Real-time deployable mitigations that analysts can use to constrain an attacker's activity on impacted endpoints or even those that are yet to be compromised. For instance, using Tanium Enforce organizations can apply temporary or long-term mitigations in real-time like: AppLocker, Firewall changes, etc.

Threat intelligence & detections

Tanium provides the richest platform to supplement the threat intelligence and detections coming from your SIEM and EDR vendor with additional custom detections from a 3rd party or from your own organization. Custom detections can be created to reason over across historical activity, on disk evidence, and real-time process data sources allowing you to answer, "is this activity in my environment" and alert on exactly what is important to your enterprise.

Specifically, Tanium enables the:

- Consumption and transformation of external Threat Intelligence (e.g.: YARA, TAXII, STIX, CybOX) into detections that are run in Tanium and optionally sent to your SIEM.
- Use of external malware related Threat Intelligence (e.g.: Virus Total, Palo Alto WildFire) which can be used as detections that are run in Tanium and optionally sent to your SIEM.
- Creation of custom multi-condition detections that can be provisioned at scale
- Creation of custom detections that can reason over data that goes beyond simple hash-based indicators (e.g.: search specific strings like known-bad command lines, anomalous network connectivity, etc.)
- Management of all custom detections and threat intelligence that has been pulled into Tanium (e.g.: targeting, views to manage, etc.)

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.

© Tanium 2023