Tanium™ Threat Response User Guide

Version 1.0.0

May 10, 2018

The information in this document is subject to change without notice. Further, the information provided in this document is provided “as is” and is believed to be accurate, but is presented without any warranty of any kind, express or implied, except as provided in Tanium’s customer sales terms and conditions. Unless so otherwise provided, Tanium assumes no liability whatsoever, and in no event shall Tanium or its suppliers be liable for any indirect, special, consequential, or incidental damages, including without limitation, lost profits or loss or damage to data arising out of the use or inability to use this document, even if Tanium Inc. has been advised of the possibility of such damages.

Any IP addresses used in this document are not intended to be actual addresses. Any examples, command display output, network topology diagrams, and other figures included in this document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Please visit https://docs.tanium.com for the most current Tanium product documentation.

Table of contents

Threat Response overview

Tanium Threat Response is a combination of Tanium™ Trace, Tanium™ Detect, and Tanium™ Incident Response. Threat Response provides critical features that support the core incident response lifecycle:

- Detection
- Investigation
- Containment
- Eradication

Use Threat Response to expediate incident response actions from hours or days to minutes. With Threat Response, you can detect, react and recover quickly from attacks and the consequential business disruptions that they cause. Threat Response has built in integration with Tanium™ Connect, Tanium™ Protect, Tanium™ Integrity Monitor, and Tanium™ Trends for additional alerting, remediation, and trending of incident related data.

Tanium Detect

Detect provides real-time monitoring of activity as it is recorded by Trace and alerts you when it detects potential malicious behavior. Detect ingests threat intelligence from a variety of reputable source and uses this information to search endpoints for known indicators of compromise and provide reputation analysis. The reputation data that Detect uses constantly compares activity such as all processes run, autorun related files, and loaded modules against known malicious hashes defined by user black lists or other services such as Palo Alto's Wildfire, VirusTotal, and ReversingLabs.

Tanium Detect User Guide

Tanium Trace

Trace continuously records key system activity for forensic and historical analysis. Use Trace to look for specific activity across every endpoint in an enterprise and drill down into process and user activity on individual systems.

Tanium Trace User Guide

Tanium Incident Response

Incident Response features sensors and packages that provide endpoint visibility and remediation. The questions featured in Incident Response provide a means to search endpoint data quickly, collect live data for offline analysis, and quarantine endpoints. Use Incident Response to contain incidents and prevent additional compromise, data leakage, and lateral movement.

Tanium Incident Response User Guide