AUTOMATE THE HUNT

RAPID IOC DETECTION AND REMEDIATION

TANIUM™

EXECUTIVE SUMMARY

In the escalating war that is cyber crime, attackers keep upping their game. Their tools and techniques are both faster and stealthier than the IT security pro can handle with the current pace of IT security innovation.

To combat these emerging threats, the IT security pro needs an upgraded toolkit. One that powers the ability to rapidly hunt for, find, and investigate thousands of dynamic threat indicators, across platforms, and across the enterprise. Thankfully the Tanium IOC Funnel, powered by the Tanium platform, enables the IT security pro to find, investigate and fix compromised systems within seconds, no matter how large, diverse or distributed the network.

INDICATORS OF COMPROMISE

The Next Advance in Cyber Defense

In the context of IT security, there's been a balancing act between investing in prevention versus detection. The current pendulum swing is towards detection, with the realization that intrusions are nearly inevitable. The latest conventional wisdom among IT security pros is that it's no longer a matter of if, but when.

After all, when your adversary is faster and more agile than you, has infinite resources, and only needs to bypass one or two security controls, it's reasonable to assume that he's already entered the building, so to speak. Enterprises need to accelerate the pace at which attacks are detected and neutralized, with as little impact to the business as possible.

IOCs: The Basics

Indicators of Compromise (IOCs) provide a key tool for the IT security pro when hunting down attacks, and pinpointing compromised systems for remediation. At the most basic level, IOCs are like bread crumbs dropped by your adversary during an attack. IOCs are written in machine-readable format (often XML) and contain attributes and other characteristics consistent with evidence of a system compromise. These "forensic artifacts" could be malware, or represent evidence of some other nefarious activity. The active use of IOCs is on the rise, as they are more flexible and adaptable than static signatures in detecting advanced threats.

Each IOC may contain dozens of attributes and conditional expressions associated with indicators like file registry settings, filenames, IP addresses or domain names, MD5 hashes, and other data elements. IT security pros can feed this intelligence to their endpoint security "ecosystem" as evidence in hunting down compromised systems, collecting additional evidence and prioritizing system recovery and remediation.

The tricky part is automating this "detection intelligence" quickly into something that's adaptable, integrated, and scalable so that you can respond immediately and with precision… across your enterprise. Speed is especially critical since digital bread crumbs do not linger long after an attack has done its damage[1]. The faster you can find them – everywhere on your network – the faster you can remediate and stop the risks that impact your business.

What is an IOC?

Indicators of Compromise are exactly what they sound like: evidence that an adversary is conducting an attack against a system or systems. Typically, these are written in machine-readable formats (e.g. XML) for consumption by security detection and response tools.

How are IOCs developed?

IOCs are developed, distributed, and shared by a variety of proprietary sources such as threat intelligence vendors as well as open source communities such as OpenIOC or IOCBucket.

Why are they important?

IT security professionals can use IOCs to search for evidence of system compromise more effectively, pinpoint endpoints and user accounts that have been compromised and prioritize the systems to be remediated.

How are they used?

Since they're written in machine-readable format (often XML), they can be "fed" to a variety of enterprise security tools for threat discovery and alert notifications, and to support additional incident response workflows.

Where can I find more information?

There are a number of open source and community resources, including projects led by FS-ISAC and MITRE involving structured cyber threat information like STIX, OpenIOC and Yara.

[1]According to a recent FireEye Report, 82% of malware binaries disappear within an hour. Source: http://www2.fireeye.com/rs/fireye/images/fireeye-advanced-threat-report-2013.pdf

At the most basic level, IOCs are like bread crumbs dropped by your adversary during an attack.

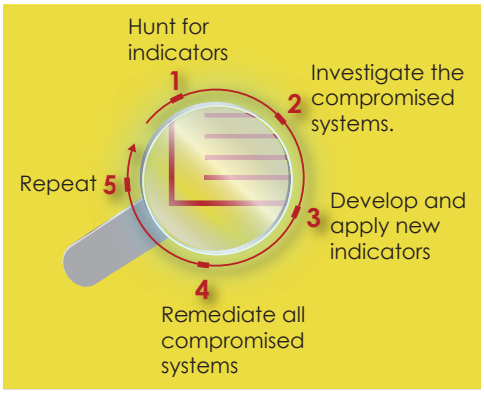
The IOC Process

By its very nature, threat detection, analysis, and investigation is an iterative exercise. As you track down evidence of a potential compromise, you discover additional evidence that can further inform your investigation, constantly fine-tuning what you're searching for when it comes to emerging threats.

In fact, the faster you can pivot, the faster you can hunt down and fight against these dynamic and advanced threats. The goal is to rapidly identity threats and neutralize them before they impact the business.

The IOC Detection Process is a Five-Step Cycle

1) **Hunt for indicators.** Using multiple threat intelligence sources, search for indicators at scale across your enterprise. Some example attributes include: MD5 hash, filename changes, registry key process handles, running processes or other process attributes.
2) **Investigate the compromised systems.** Perform deeper analysis on compromised systems to discover additional IOCs to expand or modify your search. Collect and share additional evidence with other team and/or community members.
3) **Use newly discovered evidence to develop and apply new indicators.** Apply the "new and improved" IOCs across your enterprise to find additional compromised systems.



4) **Remediate all compromised systems.** Once all compromised systems are identified, implement remediation in a way that provides containment while accelerating recovery and impacting the business as minimally as possible.
5) **Repeat steps 1-4**.

Putting IOCs to Work: Key Requirements

To support this process, organizations need tools that can **adapt** as emerging threats change, can be easily **integrated** into the existing security ecosystem and process, and can **scale** to support hundreds of thousands of endpoints across distributed networks.

As you evaluate your existing threat detection capability, consider these key requirements for making the most of IOC analysis:

- **Be Adaptable –** IOC development is as much an art as a science. Tools that ingest IOC data should therefore power iterative IOC analysis. Speed is critical here, since rapid "pivoting" and pinpointing results in more agile and faster containment and remediation. Essentially, deploying an adaptable defense requires instantaneous analysis, reporting, and response.
- **Focus on Integration –** For rapid threat detection, integrate IOCs and other threat intelligence holistically throughout your incident response process and overall toolset. This content can inform and optimize security tools like IDS, Firewall, SIEM, and AV but also systems management infrastructure such as patch management, configuration management, and software distribution. Recovery speeds up significantly when you don't have to stop to switch tools.
- **Scale without Sacrificing Speed –** Granular IOC analysis of each single endpoint, across the enterprise, can take some tools days to complete. For a network of a hundred endpoints, in the aggregate, this timeframe might be acceptable. But as soon as that number scales to thousands or hundreds of thousands of endpoints, it might be weeks before the results are complete. When the value of threat intelligence lies in its "just in-time" relevance, you're fighting a losing battle unless you can respond within seconds. Make sure any IOC detection tool or technique you implement enables instantaneous response no matter how large the network.

Sniffing out the bread-crumbs…

Some indicators to look for:

- Artifacts left by tools or toolkits.
- Anomalous activity often signaled by changes in…
  - Listening ports, system services and drivers, startup or scheduled tasks (e.g. registry settings on Windows systems).
  - File settings (permission or ownership changes).
  - Local user accounts or local firewall settings
  - DNS server settings or IP routing

When the value of threat intelligence lies in its "just in-time" relevance, you're fighting a losing battle unless you can respond within seconds.

Tanium IOC Funnel: Automating the Hunt

Tanium Features

- Supports industry standard formats such as OpenIOC, STIX, and Yara
- Integrates IOC definitions from internal sources as well as external threat intelligence providers.
- Optimizes IOC analysis by normalizing the IOC definition list
- Analyzes IOCs across hundreds of thousands of endpoints with results in seconds
- Accommodates extending, adjusting and incorporating additional IOCs on demand
- Integrates with your existing enterprise security infrastructure (e.g. SIEM, GRC, CMDB, and more)

Tanium accelerates the IOC analysis process by automating the hunt, containing and investigating the compromise and executing remediation at scale. Powered by the Tanium Platform, the Tanium IOC Funnel ingests IOCs in a variety of formats, from a variety of sources, and then scans the entire enterprise - across all of the endpoints – returning results in seconds. Seconds later, Tanium pinpoints compromised endpoints, and then rapidly executes remediation.

TANIUM Overview and How it Works

Because the IOC Funnel is powered by the Tanium Platform, it's useful to spend some time describing this revolutionary technology. Based on a resilient linear peer-to-peer communications topology, the Tanium Platform is able to deliver unparalleled speed, precision and control so that IT security pros and incident responders can respond and remediate threats in seconds, and at scale.

Only Tanium lets you ask virtually **any** question of **any** endpoint at **any** time and pivot through 10's of 1000's of potential analytical positions within seconds. And no scripting is required.

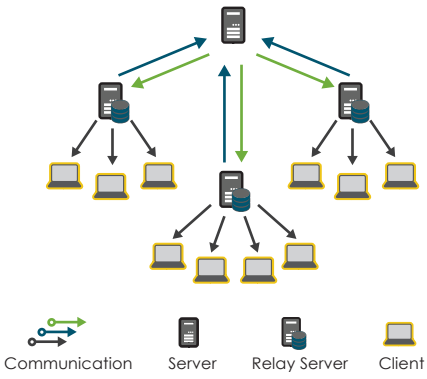
Unlike other enterprise technologies, Tanium doesn't rely on a centralized, hierarchical server infrastructure to provide data collection, aggregation, and distribution functionality. Tanium is based on an incredibly efficient, linear peer-to-peer architecture designed for fault tolerance, transient endpoints, and the global WAN segments typical of today's enterprise.

TRADITIONAL COMMUNICATIONS FLOW

Server propagates request to all Relay Servers

Relay Server collects individual responses from it's Clients

Relay Server sends series of individual responses back to Server

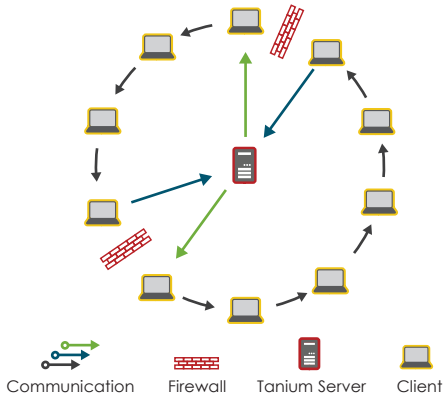


TANIUM COMMUNICATIONS FLOW

Tanium Server contacts a few Clients

Client contacts peer Client and passes aggregated response over LAN

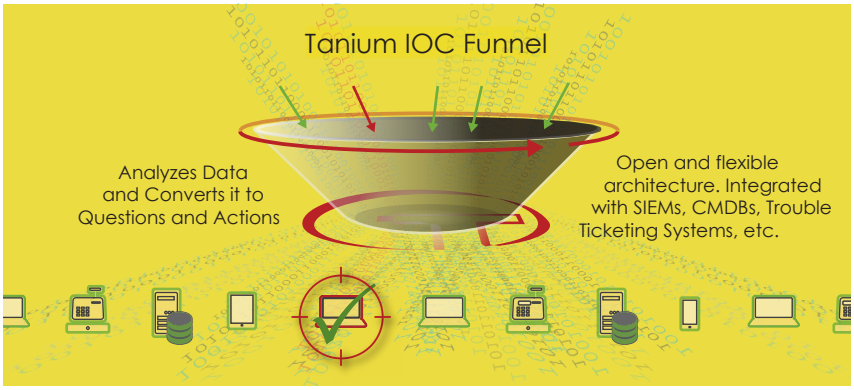
Last Client sends final aggregated response to Server



Through a lightweight and optimized agent, Tanium distributes management intelligence and data directly to the computing devices themselves. This key innovation results in radically faster, more accurate, scalable, and more adaptive security than traditional solutions. Delivering the highest value at the lowest TCO, a single Tanium server can manage over 500,000 endpoint devices, resulting in a level of resilience and efficiency not possible with alternatives.

Automated Integration Drives Incident Response

In order to drive end-to-end incident response workflows, Tanium was designed with an open and flexible architecture for quick and easy integration with other tools. Through a simple interface that requires no scripting, administrators are able to "string together" rich endpoint data surfaced through simple queries with one or more connections to back-end systems, data processing tasks, or other services.



This simple framework empowers IT security pros to:

- Send endpoint events to SIEMs such as Splunk, HP ArcSight, IBM QRadar and others
- Discover and compare new behavioral data to threat feeds
- Funnel new data insights into big data analytics tools
- Share audit and inventory data with CMDBs
- Feed actionable IOC scan results to trouble ticketing systems via REST API

This ability to easily link together configurable connectors allows Tanium to optimize security response activities and workflows - accelerating and empowering security and operations team member's analysis, response, and verification efforts.

To continuously identify emerging threats, Tanium customers use the IOC Funnel to run automated scans across the enterprise. As new IOCs are discovered, they can be shared across teams and modified, prioritized and scheduled for execution. A list of targeted IOCs can automatically run against new endpoints as they come online or exceed risk thresholds. With Tanium, IT security pros gain immediate visibility into threats across their enterprise, and can quickly seize control for remediation or deeper analysis. Additionally, Tanium can even take automatic action in response to emerging threats.

Customer Spotlight: Racing Against Time with Tanium

A large global retailer was struggling to pinpoint and resolve a malware outbreak they discovered in one of their South American offices. Out of 15,000 endpoints connected to that office, they guessed that 2,000 were infected, and their IT security team struggled to contain the outbreak. They were in a race against time, and their existing toolset had a stalled engine.

They had two key operational challenges working against them. First, this was a new piece of malware, which meant they were waiting for an updated DAT file from their AV vendor. And the other was the constrained, highly latent network links connecting them to the region. Their existing solution wasn't flexible enough to evaluate IOCs containing mutexes to identify infected machines, so they turned to Tanium.

With Tanium, they were able to verify the infected machines, quarantine them, make registry repairs to roll-back the threat temporarily and then push out an updated DAT file once it was released from their AV vendor. With their existing remediation solution, pushing out a 150MB file across those constrained network links would have failed. Thanks to Tanium, each DAT file reached its destination without error. Tanium also automated a forced AV rescan to put these protections into place immediately. Additionally, as new machines came online, they automatically received the updated AV DAT file from their peers, saving network bandwidth, and eliminating future windows of vulnerability.

SUMMARY

Indicators of compromise (IOCs) provide the essential building blocks to power a much more dynamic defense than traditional approaches can. The challenge is easily and quickly incorporating IOCs into your existing toolset and process.

Coupled with the Tanium Platform, and the IOC Funnel, rapidly convert emerging IOCs into your existing threat detection ecosystem – enabling instantaneous detection and remediation across platforms and networks. Additionally, Tanium's adaptability and extensibility supports the iterative nature of IOC hunting and remediation.

No matter how large, distributed or varied your environment, Tanium can find and fix vulnerabilities and neutralize emerging threats - within seconds.

NEED MORE INFO?

Please contact us today at sales@tanium.com. We'll provide more information on how Tanium can help you rapidly hunt down and fight against emerging threats for a truly revolutionary approach to IT operations and security. You can also find product overview videos and other resources on our website at www.tanium.com.

ABOUT TANIUM

Tanium was founded in 2007 by a team with extensive experience providing security solutions and systems management capabilities to Fortune 500 customers. Having worked closely with some of the largest, most carefully managed enterprises in the world, Tanium's founding team understands the specific challenges and constraints that must be addressed to keep large network environments running smoothly.

Tanium allows enterprises to manage, secure, and maintain the endpoints across their entire network. It enables enterprises to ask questions in plain English, identify and diagnose problems as they occur, and instantly interrogate, update and secure nodes.

1625 Shattuck Avenue, Suite 200 Berkeley, CA 94709
info@tanium.com www.tanium.com

10714-IOCFWP