ACCELERATE THE HUNT
INSTANTANEOUS THREAT DEFENSE FOR FINANCIAL SERVICES

TURN THE TABLES ON CYBER ATTACKERS WITH AUTOMATED IOC DETECTION & REMEDIATION FROM SOLTRA EDGE AND TANIUM.

Automated IOC threat detection to pinpoint exploits in seconds, and remediate seconds later. At scale.

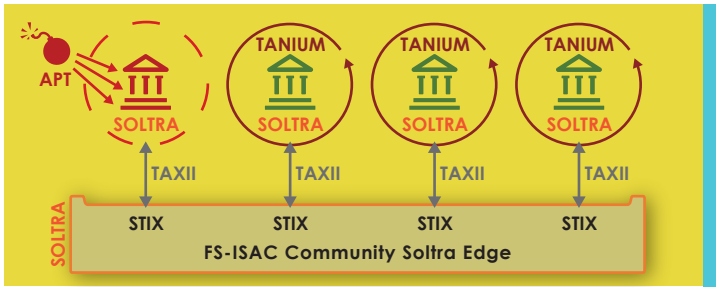
The latest cyber attacks against the financial industry demonstrate an uncomfortable truth. Despite having access to the best IT security talent available, financial services firms still suffer from multiple data breaches every year, mainly due to the inability to respond quickly enough, with precision, and at scale. IT security pros at financial firms across the world are in a race against time. They need to find, fix, and investigate any and all threat indicators across all their devices before confidential or proprietary data is stolen or operations are compromised.

Operationalize shared intelligence from FS-ISACs. The collaborative threat intelligence exchange offered by Soltra Edge has significant promise for turning the tables on cyber attackers. By consolidating, sharing, and distributing IOCs, Soltra Edge makes it more difficult and costly for cyber attackers to be successful. Through its partnership with Soltra Edge, Tanium provides instantaneous, end-to-end threat detection and remediation for some of the largest enterprises in the world.

Targeted attacks require targeted defenses. Sophisticated attacks typically combine a variety of techniques, across the cyber "kill chain". In many cases, at any stage of these attacks, the perpetrator will leave key threat indicators (IOCs). Unfortunately, however, most tools lack the speed to find these IOCs quickly enough, and also lack the precision necessary to target, quarantine and remediate the compromised systems before the damage is done.

The need for speed. Especially at scale. Industry research reflects that the latest malware "disappears" within an hour, much faster than traditional IT security tools can detect or remediate. Virtually instantaneously, IT security pros need to know which devices have been compromised, no matter how distributed their network, users, or data. Fixes need to be applied within seconds, in order to combat device compromise and data leakage, even at scales as high as hundreds of thousands of endpoints.

Thankfully, Tanium delivers instantaneous threat detection and remediation for all of the endpoints in your network. Within seconds, Tanium can hunt for the presence of hundreds of indicators of compromise (IOCs) across your environment. Seconds later, it can implement targeted remediation.



Customer Spotlight

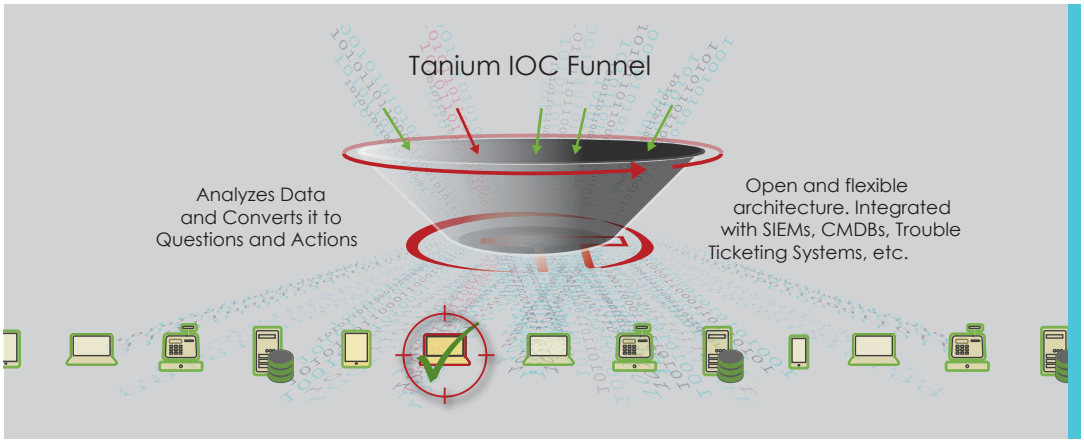
A global financial services firm recently learned how much difference a few minutes can make, when you're the victim of a malware outbreak. An employee accidentally opened an email attachment, soon realizing their mistake a few minutes after the exploit already launched and started to infiltrate other systems on the network. It was clear from the start that the malware was attempting to gather, steal and exfiltrate as much data as possible, as quickly as possible. The IT security team contacted Tanium for help, providing the sha1 hash of an unnamed malware variant. With this initial bread crumb, Tanium engineers quickly produced an IOC that led to additional details about the malware, which helped to further refine the initial IOC. Within minutes, Tanium scanned their enterprise network of tens of thousands of endpoints, discovering several infected systems, and remediating minutes later. The IOC scanning continued for several cycles every hour over the next 24 hours, to ensure that all compromised systems were detected and remediated before any additional system compromises or data loss could occur. Since this was a newly discovered piece of malware, their AV vendor needed at least 48 hours to develop a signature. Thankfully, they had Tanium to bridge the gap, with instantaneous IOC detection and remediation, at scale.

TANIUM IOC DETECTION: HOW IT WORKS

Tanium provides advanced cyber defense by automating the hunt for IOCs, containing and investigating threats and executing remediation at scale. Powered by the Tanium Platform, the Tanium IOC Funnel ingests IOCs in a variety of formats such as OpenIOC, STIX, and Yara and then scans the entire enterprise – across all of the endpoints – returning results in seconds. Seconds later, Tanium pinpoints compromised endpoints, and then executes remediation at the same speed.

Unlike other enterprise technologies, Tanium doesn't rely on a centralized, hierarchical server infrastructure to provide data collection, aggregation, and distribution. It is based on an efficient, patent-protected, linear peer-to-peer communications topology designed for fault tolerance, transient endpoints, and the global WAN segments common in the financial services industry.

Through a lightweight and adaptive agent, Tanium exchanges management intelligence and key compromise data directly with 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 500,000 endpoint devices, resulting in a level of resilience and efficiency not possible with alternatives.



Key Features

- Gathers live results from hundreds of thousands of endpoints in seconds
- Uses a single server to support 500,000 endpoints vs. hundreds of servers with incumbent solutions
- Detects attacker behavior as well as malware
- Supports more industry standard IOC formats than incumbents, including OpenIOC, STIX and Yara
- Integrates with your existing enterprise security infrastructure (SIEM, GRC, CMDB, and more)
- Consumes IOCs from any internal source or external threat intelligence provider

TANIUM™

1625 Shattuck Avenue, Suite 200
Berkeley, CA 94709

info@tanium.com
www.tanium.com