FORTRA™

WHITE PAPER (TRIPWIRE)

Actionable Threat Intelligence

Automated IoC Matching with Tripwire

A key challenge facing government agencies and other security-minded organizations is finding and rooting out malware that has already become embedded on key assets. Organizations today have myriad threat intelligence sources to leverage. However, simply getting the intelligence into your organization is not enough. Unless you have a way to operationalize that knowledge to make it actionable and useful, threat intelligence is just further fueling the problem that many agency security teams face: too many security products generate mountains of events but offer little ability to figure out what is actually important.

The solution is to ensure that threat intelligence programs address the "last mile" issue by connecting inbound threat intelligence sources directly to the monitoring systems that are already in place. Fortra's Tripwire has been working with its customers, partners, federal standards organizations and industry groups to make this connection a reality, helping to address the key question when a new indicator of compromise comes in, "Do I have any of that on my network?"

This white paper addresses how to operationalize automated "Indicators of Compromise" (IoCs) from threat intelligence workflows for use in finding malicious embedded binaries—and adapting one's security posture for prevention in the future.

Background Information

Despite cybersecurity focuses at the federal level, threat intelligence programs are a constantly evolving element within many agencies. Contrast the challenge of forming and maturing a threat intelligence program with that of building an incident response capability. With incident response, best practices have emerged over the years, and guidelines for building and assessing a program can be found from sources such as NIST SP 800-61 R2: *Computer Security Incident Handling Guide*, CMU SEI's *Handbook for Computer Security Incident Response Teams* and ENISA's *How To Set Up a CSIRT and SOC*. For the more specific discipline of threat intelligence programs, the landscape changes continually preventing a single handbook from remaining permanently relevant. A good reference though is the publication NIST SP 800-150: *Guide to Cyber Threat Information Sharing*. On the topic of operationalizing threat intelligence, the NIST guide states, "Information received from external sources has value only to the extent that an organization is equipped to act on the information."

Threat Intelligence Standards

Threat intelligence can come into an agency's organization from a variety of sources and formats. While documents and text describing threats can be useful, the subset of threat intelligence known as machine-readable threat intelligence (MRTI) containing specific IoCs tends to be the most actionable intelligence. The standards for MRTI sharing are STIX and TAXII. These standards, developed by MITRE working with the U.S. Department of Homeland Security (DHS) as part of a community-driven effort to enable structured definition and sharing of intelligence have transitioned to OASIS, a global open standards organization. The adoption of STIX and TAXII by threat intelligence providers, consumers and tools vendors help create an interoperable ecosystem that can span organizations and provide the kind of adaptive security architecture that is necessary to defend against modern threats.

These standards are being used; the FS-ISAC in the financial services community has been a leader in the adoption of these standards for threat intelligence sharing amongst its member companies. However, adoption is still limited and Tripwire has yet to encounter any organization, federal or commercial, that can declare that they rely solely on the use of these standards to handle inbound threat intelligence sources. The reality is that the most common format for delivering threat intelligence continues to be unstructured indicators sent via e-mail. Other common formats encountered in real-world situations are CSV files, plain text files and proprietary web interfaces providing intelligence via REST or SOAP APIs.

The types of MRTI commonly being shared today reflect only a very limited subset of the full capabilities of STIX. STIX defines a flexible, extensible, format that can encapsulate sophisticated threats that include multiple threat actors using a variety of techniques against numerous targets. Some effort has gone into modeling the kind of sophisticated intelligence that represents a complete advanced persistent threat, but the reality is that simple indicators, observables and sightings are the bulk of actual threat intelligence being currently shared. On the network side, a list of "bad" IP addresses and DNS names associated with malicious activities are the most common IoC an organization can expect to receive. On the systems side, file hashes associated with malicious files (e.g., malware and rootkits) would be expected.

The use of standards can take place in multiple parts of a threat intelligence workflow. The challenge and benefit over the last two years has been to enable and promote threat intelligence sharing between organizations using STIX and TAXII. Once the intelligence reaches an organization, the challenge shifts to how can this intelligence be utilized by the groups, products and tools within the organization. There has been less progress made on this front to date, with only a limited number of security control vendors opening up the proprietary interfaces between their own intelligence and related products or providing a standards-based interface for ingesting threat intelligence from external sources.

This position is understandable, as it takes time to prioritize and deliver this functionality. Given the current state of adoption, a security vendor has to be prepared to not only adopt a STIX and TAXII standards-based approach to this problem, but also still deal with the real-world environment where intelligence is being received in a variety of other formats.

Applying Threat Intelligence to Tripwire Enterprise: Hash Matching and Beyond

Federal agencies use Tripwire® Enterprise to provide comprehensive system integrity monitoring, security configuration management and change auditing. System integrity monitoring (also known as file integrity monitoring, or FIM) encompasses monitoring attributes such as files, configuration settings, users, security policies and databases, to name a few. Detecting and auditing changes on systems is a fundamental security control that can be used for both detecting threats, as well as being a critical part of an incident response and forensics capability. This control is also critical for making system-level threat intelligence actionable.

The question for the threat intelligence team to answer with any new piece of inbound intelligence is how does this apply to our organization? For a specific indicator, such as a file hash, the three questions to answer are:

1. Has this been seen in our environment in the past?
2. Is it present in our environment now?
3. How can I become aware if this appears in our environment in the future?

Tripwire has developed a threat intelligence integration for Tripwire Enterprise aimed directly at answering these questions. In an organization that has adopted a STIX/TAXII standards approach for consolidating threat intelligence, Tripwire can receive intelligence in STIX format via a TAXII feed. Although this could also come directly from an external source, the more common approach here would be to connect Tripwire Enterprise to an organization's internal TAXII server (such as the freely available Soltra Edge virtual appliance). The internal TAXII server itself may be receiving intelligence feeds from external TAXII servers, or imported through adapters or its user interface.

Acknowledging that many organizations have not yet reached that level of adoption of the standards to consolidate intelligence into TAXII for internal dissemination, Tripwire has built this integration to work with any common format in which indicators may already exist, including CSV files, text files and a command line interface that can be used directly or integrated with scripts.

> Tripwire Enterprise integrates with a variety of threat intelligence technology partners to deliver increased visibility into real risks to agencies, along with the essential information needed to respond with agility.

Once the indicator is imported, the forensic history is reviewed to see if the hash has been previously identified, and it is put into a database of indicators to match against in the future. Matching an indicator sets a property associated with a file to signal that this is malicious content. During the import process, specific metadata can be provided about the source of the IoC. The integration can also leverage the asset management capabilities within Tripwire Enterprise to tag an asset containing a matching indicator.

Setting a property and tagging an asset is a very simple—yet powerful—capability within the context of using Tripwire Enterprise. This information can be exposed in dashboards and reports, and drive automated workflows to alert, escalate and drive mitigation and remediation actions within an organization. Extending an existing workflow established for integrity monitoring and change auditing is

particularly powerful for complex organizations, where asset owners may be independent of the security operations and system administration teams.

Although the integration established above is specifically hash-based, this is only the beginning of the type of threat intelligence that can be automated through an integration with Tripwire Enterprise. As threat intelligence sources become increasingly sophisticated in the type of threats being shared, the integration can be extended to answer these same questions for any of the elements Tripwire is capable of monitoring. Similarly, the Tripwire Enterprise architecture is flexible enough to allow new types of elements on assets to be monitored. In this way, it is expected these two areas will continue to evolve, with new intelligence being received driving extensions to the threat intelligence integration capabilities in Tripwire Enterprise, and ultimately to the capabilities of the product as a whole.

Summary

There is good news. Agencies that are just getting started with something as basic as an emailed list of hashes can rapidly assess their situation. At the same time, knowing that there will be more such lists in the future, they understand where the maturity model is going, and can see a clear pathway to fully automating this activity for the future.

Advanced Monitoring

- Standards-based integration
- Industry-specific threat identification
- Automates analysis
- Identifies potentially compromised assets
- Continuously reduces the attack surface

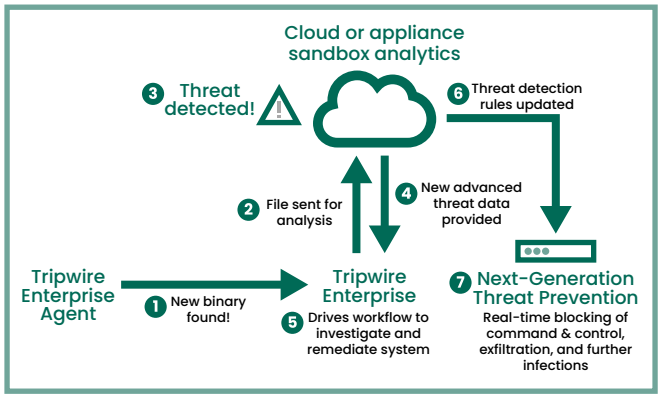
Tripwire Enterprise

1. Automatically downloads Indicators of Compromise (IoC)
2. Employs policies to monitor for IoCs
3. Drives remediation workflow

Applying Malware Analytics to Tripwire Enterprise

Tripwire Enterprise can integrate and connect threat intelligence from both cloud-based and on-premises threat intelligence sources to deliver actionable malware analytics.

When a new or changed binary is identified on a system, Tripwire's integration is intended to answer the question, "Does this binary represent a known or previously unknown advanced threat?" This is complementary to threat intelligence sources that may have knowledge of a specific set of files associated with malicious activity. Figure 2 on the following page simplifies the process, but gives an overview of the basic steps involved in Tripwire's advanced malware identification through threat intelligence integrations.



Step 1

Tripwire Enterprise first detects a new binary on the endpoint and based on its initial analysis deems it a possible threat.

Step 2

Tripwire delivers a file hash to the integrated partner solution for initial identification. The possible outcomes of this are:

1. It's known and benign: not a threat
2. It's not known—unclear if a threat or not: should be investigated
3. It's a known threat

Step 3

If the threat intelligence partner reports that the hash has never been seen before, Tripwire Enterprise will transmit the complete binary for analysis.

Step 4

The partner then analyzes the binary and/or associated files using a variety of techniques (including detonating

it in a sandbox environment). The report back to Tripwire Enterprise includes any suspicious behavior and actions that were observed—along with an analysis of the likelihood of it being a threat to the agency. Further, the threat intelligence partner may contribute the threat to its global threat intelligence community for awareness and rapid identification of this same threat by others.

Step 5

This externally sourced threat intelligence can be used to drive mitigation and remediation actions, using Tripwire Enterprise's automation and integrated workflows.

Step 6

In addition, the network behavior of this threat, such as a command and control (C2) infrastructure being communicated with, may be automatically adapted into threat prevention rules that are delivered in an automated update to next-generation firewall and IPS systems from the partner.

Step 7

The agency can then put into place the appropriate measures to alert, block or take other steps to protect its vulnerable or valuable systems. There are differing views within many agency organizations as to whether threat intelligence programs should include a malware analysis function, or if this should live in a different part of a security organization. Regardless of where it may be housed, this functionality is becoming an essential component of most security programs who seek to meet new and upcoming federal mandates.

Ready to Learn More?

Want to learn more about how Tripwire can help you meet your security needs? Register for a demo at tripwire.com/demo

FORTRA™

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.