Correlating advanced threat information feeds

Jamie Murdock and Suranjan Pramanik
Forward-looking statements

This is a rolling (up to three year) Roadmap and is subject to change without notice.

This document contains forward looking statements regarding future operations, product development, product capabilities and availability dates. This information is subject to substantial uncertainties and is subject to change at any time without prior notification. Statements contained in this document concerning these matters only reflect Hewlett Packard's predictions and / or expectations as of the date of this document and actual results and future plans of Hewlett-Packard may differ significantly as a result of, among other things, changes in product strategy resulting from technological, internal corporate, market and other changes. This is not a commitment to deliver any material, code or functionality and should not be relied upon in making purchasing decisions.
HP confidential information

This is a rolling (up to three year) Roadmap and is subject to change without notice.

This Roadmap contains HP Confidential Information.

If you have a valid Confidential Disclosure Agreement with HP, disclosure of the Roadmap is subject to that CDA. If not, it is subject to the following terms: for a period of 3 years after the date of disclosure, you may use the Roadmap solely for the purpose of evaluating purchase decisions from HP and use a reasonable standard of care to prevent disclosures. You will not disclose the contents of the Roadmap to any third party unless it becomes publically known, rightfully received by you from a third party without duty of confidentiality, or disclosed with HP’s prior written approval.
Utilizing Advanced Threat Intelligence Feeds
BIOS

Jamie Murdock
• CISO at Binary Defense Systems
• 15+ years experience, specializing in security operations, threat intelligence, and incident response
• Created SOC’s and threat intelligence programs for Fortune 500’s
• Assisted in profiling foreign cyber criminals
• Twitter: @b0dach

Suranjan Pramanik
• 8 years of experience in ArcSight R&D
• Extensive knowledge of ESM internals
• Focusing on Security Analytics and Threat Intelligence
• Contact Email: suranjan.pramanik@hp.com
Why incorporating threat intelligence has increased in importance

• The threat landscape has evolved to the point where sophisticated groups, some of which are state sponsored, are becoming more prevalent.
Why incorporating threat intelligence has increased in importance

- Geopolitical issues and social retaliation is now mirrored in the cyber world.
Why incorporating threat intelligence has increased in importance

• By proactively utilizing threat intelligence, you can increase the monitoring capabilities of an organization and decrease response time.
Why incorporating threat intelligence has increased in importance

- Incorporating threat intelligence feeds into ArcSight allows you to create specific content based on threats.
Types of threat intelligence

- Open Source Intelligence (OSINT)
  - Intel gained from available sources; Google, social media, IRC, etc.
  - Good source of “chatter”, you can build your own bad actor profile; types of attacks, methods, types of common targets, etc.
- Commercial feeds
  - Intel that comes from a services that collects threat intelligence, analyzes this information and distributes it to subscribers
  - Typically based on IP addresses/domain names
  - These feeds can usually be fed into ArcSight easily
- Government feeds
  - US-CERT
  - National Vulnerability Database
- Vertical market feeds
  - Information sharing for specific verticals and known malicious IP’s
How to select the right feeds

• Make sure the threat intelligence feed is relevant
• The feeds need to be consumable into ArcSight
• The feeds need to be current
• The feeds need to be actionable
Real world examples

- Threat intelligence from government malicious IP list identified C&C communications to Iran
Real world examples

- Using OSINT, a member of a known bad actor group that targeted business in the region was identified; his known avenues of attack were incorporated into ArcSight to provide increased monitoring of this group.

<table>
<thead>
<tr>
<th>Jan</th>
<th>Feb</th>
<th>Mar</th>
<th>Apr</th>
<th>May</th>
<th>Jun</th>
<th>Jul</th>
<th>Aug</th>
<th>Sep</th>
<th>Oct</th>
<th>Nov</th>
<th>Dec</th>
<th>Jan</th>
<th>Feb</th>
<th>Mar</th>
<th>Apr</th>
</tr>
</thead>
<tbody>
<tr>
<td>CN</td>
<td>CN</td>
<td>CN</td>
<td>CN</td>
<td>CN</td>
<td>CN</td>
<td>CN</td>
<td>CN</td>
<td>CN</td>
<td>CN</td>
<td>CN</td>
<td>CN</td>
<td>CN</td>
<td>CN</td>
<td>CN</td>
<td>CN</td>
</tr>
<tr>
<td>GB</td>
<td>GB</td>
<td>GB</td>
<td>GB</td>
<td>GB</td>
<td>GB</td>
<td>GB</td>
<td>GB</td>
<td>GB</td>
<td>GB</td>
<td>GB</td>
<td>GB</td>
<td>GB</td>
<td>GB</td>
<td>GB</td>
<td>GB</td>
</tr>
<tr>
<td>CA</td>
<td>CA</td>
<td>CA</td>
<td>CA</td>
<td>CA</td>
<td>CA</td>
<td>CA</td>
<td>CA</td>
<td>CA</td>
<td>CA</td>
<td>CA</td>
<td>CA</td>
<td>CA</td>
<td>CA</td>
<td>CA</td>
<td>CA</td>
</tr>
<tr>
<td>IN</td>
<td>IN</td>
<td>IN</td>
<td>IN</td>
<td>IN</td>
<td>IN</td>
<td>IN</td>
<td>IN</td>
<td>IN</td>
<td>IN</td>
<td>IN</td>
<td>IN</td>
<td>IN</td>
<td>IN</td>
<td>IN</td>
<td>IN</td>
</tr>
<tr>
<td>RO</td>
<td>RO</td>
<td>RO</td>
<td>RO</td>
<td>RO</td>
<td>RO</td>
<td>RO</td>
<td>RO</td>
<td>RO</td>
<td>RO</td>
<td>RO</td>
<td>RO</td>
<td>RO</td>
<td>RO</td>
<td>RO</td>
<td>RO</td>
</tr>
<tr>
<td>TR</td>
<td>TR</td>
<td>TR</td>
<td>TR</td>
<td>TR</td>
<td>TR</td>
<td>TR</td>
<td>TR</td>
<td>TR</td>
<td>TR</td>
<td>TR</td>
<td>TR</td>
<td>TR</td>
<td>TR</td>
<td>TR</td>
<td>TR</td>
</tr>
</tbody>
</table>
Real world examples

- Through a commercial feed, C&C IP’s were added to ArcSight and content was created to correlate the C&C traffic and vulnerable hosts. It was discovered that the company was being targeted and attempts were being made to compromise vulnerable hosts.
Real world examples

- Using intelligence from an industry threat intelligence feed, malicious IP's were added to ArcSight and attacks in progress were discovered.
Real world examples

- Using a free feed, P2P traffic was discovered. This led to an investigation that resulted in identifying a gap in security controls.
Walkthrough: Adding Threat Intelligence Feeds into ESM
Overview

Two ways to import threat Intelligence into ESM

**Threat Central**
Threat information feed from HP
- Data Format
- Model Import Connector (MIC) Configuration
- Available ESM Content
- Supports STIX, CSV formats

**Structured Threat Information eXpression – STIX**
Cyber threat information language
- Language syntax
- Flex Connector Configuration (has to be created)
- Author new ESM Content

This is a rolling (up to 3 year) roadmap and is subject to change without notice.
Threat Central
Threat Central

HP’s threat intelligence feed

• Currently available as a Beta program
• Provides automated, collaborative, contextual, and actionable security feeds in a timely manner
• Feeds available from HP Security Research and credible security vendors
• Model Import Connector – transfers information between ESM and Threat Central
Threat Central Portal

All product views are illustrations and might not represent actual product screens.
Threat Central case details

Query

Indicators
- Unknown - IP Whitelist
  - Added by CaptPreto on Feb 10, 2014 0:22
  - Score: 5.00

Trojans - Suspected File Hashes
- Added by CaptPreto on Feb 10, 2014 0:22
  - Score: 4.10

Network layer traffic anomaly - Domain Watchlist
- Added by CaptPreto on Feb 10, 2014 0:22
  - Score: 4.20

Actors
- New Actor
- Add Existing Actor

TTP
- New TTP
- Add Existing TTP

Found a sample
- Added by Randolph on Feb 10, 2014 0:22
  - Actually came across this sample as well – ESET-NOD32 took care of the problem. I guess I just recommend getting one of the AV products capable of detecting this file for quick and easy removal.

DarkComet RAT
- Added by Orler on Feb 10, 2014 0:10
  - DarkComet RAT actually has its own dedicated removal tool. Its creator decided to remove the malware from the company’s server but before creating a DarkComet RAT removal tool, he was unhappy that the infection was being spread by the d&d and other systems with the tool.

Course of Action

- Found a sample
- DarkComet RAT

Observables

This is a rolling (up to 3 year) roadmap and is subject to change without notice.

All product views are illustrations and might not represent actual product screens.
Model Import Connector (MIC)

- Downloads Indicators from TC to ESM
- Uploads Indicators and statistics from ESM to TC
- Configurable upload and download frequency

This is a rolling (up to 3 year) roadmap and is subject to change without notice.
This is a rolling (up to 3 year) roadmap and is subject to change without notice.

ESM Download Active Lists

All product views are illustrations and might not represent actual product screens.
ESM real-time Rule triggers

All product views are illustrations and might not represent actual product screens
ESM Upload Active Lists

This is a rolling (up to 3 year) roadmap and is subject to change without notice.

All product views are illustrations and might not represent actual product screens.
Structured Threat Information eXpression (STIX)

Cyber threat information language

- **Observables** – IP Addresses and File Hashes
- **Adversary tactics, techniques, and procedures**
- **Exploitation targets, Campaigns, and Course of Action**

```xml
<?xml version='1.0' encoding='UTF-8'?>
<cybox:Observables xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:cybox="http://cybox.mitre.org/cybox-2"
  xmlns:cyboxCommon="http://cybox.mitre.org/cybox-common-2"
  xmlns:AddressObj="http://cybox.mitre.org/objects#AddressObject-2"
  xmlns:example="http://example.com/"
  xsi:schemaLocation="http://cybox.mitre.org/cybox-2 ../cybox_core.xsd
                     http://cybox.mitre.org/objects#AddressObject-2 ../objects/Address_Object.xsd"
  cybox_major_version="2" cybox_minor_version="0">
  <cybox:Observable id="example:Observable-0b9af309-0d5a-4c14-bdd7-aea3d99f13b6">
    <cybox:Object id="example:Object-15be6530-c2df-4hf9-8750-3f45ca9e19cf">
      <cybox:Properties xsi:type="AddressObj:AddressObjectType" category='ipv4-addr'>
        <AddressObj:Address_Value>192.168.0.5</AddressObj:Address_Value>
      </cybox:Properties>
    </cybox:Object>
  </cybox:Observable>
</cybox:Observables>
```

[STIX Reference - https://stix.mitre.org/]
Convert STIX files into ESM format

Use Connectors, Rules, and Active Lists

Configure ArcSight Connector

- Create a new XML FlexAgent
- Map the STIX attributes to ESM format (CEF or ActiveList schema)

Create an Active List and Lightweight Rule

- Define an Active List having fields similar to STIX fields
  - E.g., `<IP Address, Domain>`
- Define a lightweight Rule to add data to the ActiveList

Start the STIX Flex Connector

- Send STIX events to the ESM manager
- After processing the files they are renamed to `.processed`

Use Active List in Rules and Reports

- Define a new ESM Rules and Queries to correlate Active Lists with Security Events
Connector configuration for STIX data

- **Agent Type**: sdkxmlfolderfollower
- **Folder where STIX Files are present**: /opt/depot/boxster/feature/
- **Configuration File**: ARCSIGHT_HOME/user/agent/flexagent/
Connector properties for STIX data (IP addresses)

Define namespaces

STIX tokens

CEF Event trigger

STIX to CEF mappings

namespace.count=5
namespace[0].uri=http://www.w3.org/2001/XMLSchema-instance
namespace[0].prefix=xsi
namespace[1].prefix=cybox
namespace[2].prefix=cyboxCommon
namespace[3].uri=http://cybox.mitre.org/objects#AddressObject-2
namespace[3].prefix=AddressObj
namespace[4].uri=http://example.com
namespace[4].prefix=example
-hop.node.count=2
-hop.node[0].name=observables
-hop.node[0].expression=/cybox:Observables
-hop.node[1].name=observable
-hop.node[1].expression=$observables/cybox:Observable
-trigger.node.expression=$observable/cybox:Object/cybox:Properties/AddressObj:Address_Value
token.count=3
token[0].name=sourceAddress
token[0].type=IPAddress
token[0].expression=cybox:Object/cybox:Properties/AddressObj:Address_Value
token[0].node=observable
token[1].name=observableId
token[1].expression=@id
token[1].node=observable
token[2].name=objectId
token[2].expression=cybox:Object/@id
token[2].node=observable
-event.name=observableId
event.message=objectId
event.sourceAddress=sourceAddress
event.deviceVendor=_stringConstant("STIXVendor")
event.deviceProduct=_stringConstant("STIXVendor")
### STIX Data in an Active Channel

#### Example Data

<table>
<thead>
<tr>
<th>End Time</th>
<th>Name</th>
<th>Attacker Address</th>
<th>Device Custom String</th>
<th>Device Custom String2</th>
<th>Device Vendor</th>
<th>Device Product</th>
</tr>
</thead>
<tbody>
<tr>
<td>8/28 18:13:26</td>
<td>example:Observable-0b9af309-...</td>
<td>192.168.0.5</td>
<td>Toobar.dll</td>
<td>C:\Windows\system32</td>
<td>STIXVendor</td>
<td>STIXVendor</td>
</tr>
<tr>
<td>8/28 18:10:12</td>
<td>example:Observable-a727a717-...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8/28 18:01:58</td>
<td>Case Escalation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8/28 17:17:56</td>
<td>Case Escalation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8/28 17:17:56</td>
<td>Case Escalation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8/28 17:17:56</td>
<td>Case Escalation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Key Elements
- **Attacker address**
- **File information**
Analysing STIX data using ESM content

**Rule**

**Rule conditions**
- Category Behavior = /Access
- Category Object = /Host|Resource|File
- Device Product Contains STIX
- Device Vendor Contains STIX
- Device Custom String1 is NOT NULL
- Device Custom String2 is NOT NULL

**Rule actions**
- On First Event
- On Subsequent Events
- On Every Event [ Active ]
  - Add To Active List
    - Field: Device Custom String1
    - Field: Device Custom String2
    - Field: Device Custom String3
    - Field: Device Custom String4
    - Resource: /All Active Lists /Personal/admin’s Active Lists/StixFileInfo

**Active List**

<table>
<thead>
<tr>
<th>File Name</th>
<th>File Path</th>
<th>File Hash</th>
<th>Hash Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>bad_file24.exe</td>
<td>AppData\Mozilla</td>
<td>a7a0390e99406f8975a189...</td>
<td>MD5</td>
</tr>
<tr>
<td>foobar.dll</td>
<td>C:\Windows\system32</td>
<td>6E48C348D742A931EC2CE...</td>
<td>MD5</td>
</tr>
</tbody>
</table>
Conclusion

• Threat Information feeds can be helpful in detecting advanced persistent threats

• HP Threat Central provides automated, collaborative, contextual, and actionable threat intelligence
  – Model Import Connector automatically synchronizes Threat Central server and ESM
  – Threat Central Content provides immediate correlation
  – Allows import and export of STIX documents

• STIX documents can also be imported using Flex Connectors into ESM
  – Requires vetting of the source and context of the documents
  – Need to write new Connectors and Content to use the information
For more information

Attend these sessions
• TB3013, All about HP Threat Central

Visit these demos
• Threat Central Demo

After the event
• Web: hp.com/go/threatcentral
• Blog: hp.com/go/hpsrblog
• Whitepaper: http://hpsw.co/z4L7ZbX

Your feedback is important to us. Please take a few minutes to complete the session survey.
Please give me your feedback

Session TB3169  Speakers Jamie Murdock and Suranjan Pramanik

Use the mobile app
1. Click on Sessions
2. Click on this session
3. Click on Rate Session

Or use the hard copy surveys

Thank you for providing your feedback, which helps us enhance content for future events.
Thank you