IntroSpect Product Update

Viswesh Ananthakrishnan, Senior Director of Product Mgmt.
Agenda
Release Highlights: 2.3, 2.4, and 2.5
Analytics
Analyst Workflow
Integrations
Platform
Act on attacks with a wide range of policy actions

Detect attacks with range of analytics

Visibility through profiling and classification

IT access based on user/device attributes

ARUBA SECURITY
USER/DEVICE
LIFE CYCLE

Aruba 360 Security

Authorize

Respond

Enforce

Aruba 360 Security

IntroSpect

Monitor

Discover

ClearPass Device Insight

ARUBA SECURITY USER/DEVICE LIFE CYCLE

Aruba 360 Security

Authorize

Respond

Enforce

Act on attacks with a wide range of policy actions

Detect attacks with range of analytics

Visibility through profiling and classification

IT access based on user/device attributes
INTROSPECT AT A GLANCE

- **IDENTITY**
  - Consoles / Workflows
  - SIEM
  - SIEM Analyzer
  - ENTITY360
  - ANALYTICS
  - DATA FUSION
  - FORENSICS
  - BIG DATA

- **INFRASTRUCTURE**
  - Office 365
  - SaaS

- **THREAT INTELLIGENCE**
  - Alerts
  - ArcSight

- **NETWORK TRAFFIC**
  - Packet Processor
  - Packets
  - Flows
ACCELERATED INVESTIGATION & RESPONSE

CAMPUS
BRANCH
SaaS
CLOUD

Forensics
Attack Analytics
Behavioral Analytics

ENTITY360

SAM FULLER
3 HOSTS
22 IPs
95 LOGONS
120k SESSIONS

RISK SCORE

25 45 60 80

time

5

@ArubaAPAC/ATM19APAC
Release Highlights from 2.3, 2.4, and 2.5

Analytics
- Chained alerts (2.3)
- Custom AD use cases (2.3)
- Emails to personal accounts (2.3)
- MUTE/Peering with arbitrary LDAP attributes (2.4)
- Service Account Analytics (2.4)
- Office 365 support (2.5)
- Ransomware detection (2.5)

Analyst Workflow
- Intelligent alert clustering (2.4)
- Behavioral baseline visualization (2.4)
- Network visualization (2.5)

Integrations
- Expanded 3rd party alerts (2.4)
- ClearPass granular control (2.4)
ANALYTICS
# Why Chained Alerts?

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Generalizable/ Avoids Overfitting</th>
<th>Easy to apply Business Context</th>
<th>Reduces False Positives</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Rules (1)</strong></td>
<td>![X]</td>
<td>![✓]</td>
<td>![X]</td>
</tr>
<tr>
<td>A user badged in before 5am and badged out after 8pm</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Machine Learning (1)</strong></td>
<td>![✓]</td>
<td>![X]</td>
<td>![X]</td>
</tr>
<tr>
<td>A user accessed anomalously large number of critical servers, compared with history over past 30 days</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Rules (1) + Machine Learning (1)</strong></td>
<td>![✓]</td>
<td>![✓]</td>
<td>![X]</td>
</tr>
<tr>
<td>A user performed anomalously large uploads to Cloud drives and belongs to watchlist “Terminated Employees”</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Chained Alerts - multiple</strong></td>
<td>![✓]</td>
<td>![✓]</td>
<td>![✓]</td>
</tr>
<tr>
<td>A user from watchlist “Terminated Employees” performed anomalously large downloads from critical servers and within the next 8 hours, also had anomalously large print jobs</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
"Temporal Operators" to constrain alerts generated by Rules/ML

1. After

$\text{eventA} : \text{EventA}( \text{this after} \ [1h, 4h] \ \text{eventB} )$

$1h \leq \text{eventA.startTimestamp} - \text{eventB.endTimestamp} \leq 4h$

2. Before
3. Coincides
4. During
5. Finishes
6. Finished by
7. Includes
8. Meets
9. Met by
10. Overlaps
11. Overlapped by
12. Starts
13. Started by
Chained Alert Configuration Example 1
Suspicious Privilege Escalation

Name of this Alert Chain
Suspicious Privilege Escalation

**Alert Chain**

1. ✔️ Create or Enable
2. ✔️ Escalate

**ADD TO SEQUENCE**

**Comment (Optional)**
Suspicious Privilege Escalation
Chained Alert Configuration Example 1
Defining Events Group
# Chained Alert Configuration Example 1

## Defining Events Group

### Name of this Alert Chain

**Suspicous Privilege Escalation**

<table>
<thead>
<tr>
<th>ALERT TYPE</th>
<th>ALERT CATEGORY</th>
<th>ALERT CHAIN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Abnormal Account</td>
<td>Account Activity</td>
<td>1. Create or Enable</td>
</tr>
<tr>
<td>TIME WINDOW</td>
<td>ASSOCIATE BY</td>
<td>2. Escalate</td>
</tr>
<tr>
<td>2 days</td>
<td>User</td>
<td></td>
</tr>
</tbody>
</table>

### Alert Chain

- 1. Create or Enable
- 2. Escalate

### Name of this Group

**Escalate**

**Alert Chain**

- Global Admin Escalation
- Local Admin Escalation
- Universal Admin Escalation

### Add to Group

**Required Alerts**

1 or more

**Comment (Optional)**

Suspicious Privilege Escalation

DONE
Chained Alert – Sample Alert
Suspicious Data Exfiltration

### ALERT CHAIN

<table>
<thead>
<tr>
<th>ALARM NA...</th>
<th>START TIME</th>
<th>END TIME</th>
<th>STAGE</th>
<th>CONFIDENCE</th>
<th>SEVERITY</th>
<th>STATUS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Large Internal SMB Download</td>
<td>Apr 8, 18 8:36 PM</td>
<td>Apr 8, 18 8:53 PM</td>
<td>Internal Activity</td>
<td>100</td>
<td>60</td>
<td>open</td>
</tr>
<tr>
<td>Large Data Upload to External</td>
<td>Apr 9, 18 3:27 AM</td>
<td>Apr 9, 18 3:27 AM</td>
<td>Exfiltration</td>
<td>100</td>
<td>60</td>
<td>open</td>
</tr>
<tr>
<td>Large Dropbox Upload</td>
<td>Apr 9, 18 3:21 AM</td>
<td>Apr 9, 18 3:28 AM</td>
<td>Exfiltration</td>
<td>100</td>
<td>60</td>
<td>open</td>
</tr>
</tbody>
</table>

### SUSPICIOUS DATA EXFILTRATION

User karthik had 9 addresses with 3 suspicious data exfiltration activities on Apr 08, 2018

@ArubaAPAC | #ATM19APAC
New Email Use Cases
Analytics

I. Emails sent to personal accounts
   • At least 4 identical contiguous characters AND sent to a domain which is not trusted

II. Detection of Critical keywords in email subject/attachment name
   • Match configured keywords

<table>
<thead>
<tr>
<th>Log Sources</th>
<th>SMTP Network traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Cisco Email Security logs</td>
</tr>
</tbody>
</table>
I. Configuration Steps for Email sent to personal account

a) Click on **Home > Analytics & Rules** on the Analyzer. Click on **Configuration > Trusted Email Domains** as shown below. Click on **New**, add the domain. Ensure you **Enable** and **Save** it.

b) Alerts are enabled by default in 2.3. You can validate the same under **Home > Analytics & Rules**
Triggered Alert

- Filtered by Alert Type: Email Communication, Suspicious Email Address
- Severity: 20
- Confidence: 20
- Alert Name: Email Sent to Personal Account
- Email account JohnChambers@onyx.com sent 13 emails to personal accounts on Apr 27, 2018
- Personal Email Accounts:
  - JohnPaul@clayton.com
  - JohnSene@clayton.com
b) Go to Configuration Tab on the Analyzer (Home > Configuration). Click on the Analytics tab in the left window pane. Click on New.

c) Alerts are enabled by default in 2.3. You can validate the same under Home > Analytics & Rules.
Triggered Alert

User z_user511 with email Z_user511.user511@onyx.com sent 2 emails containing sensitive keyword exfiltrate to 2 recipients on May 02, 2018.

Emails sent to:
- shyam5.sundar58@clayton.com
- shyam6.sundar6@clayton.com

Keywords: exfiltrate
Custom AD Use Cases
Analytics

Feature Description
• Allow customers to define and configure their own customized use case based on their network environment and preferences
• Useful for customers to fit in their own domain knowledge

Example Use Cases
1. Non-admin role created new user
2. User privilege escalation to join “Guardians of the Galaxy” group
# Custom AD Use Cases – Event ID for Query String Analytics

<table>
<thead>
<tr>
<th>AD Use Case</th>
<th>Event ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>User/Hostname Correlation</td>
<td>4624, 4625</td>
</tr>
<tr>
<td>Account Logon</td>
<td>4767, 4768, 4769, 4770, 4771, 4776</td>
</tr>
<tr>
<td>Account Management</td>
<td>4720, 4722, 4723, 4724, 4725, 4726, 4740</td>
</tr>
<tr>
<td>Group Management</td>
<td>4728, 4732, 4756</td>
</tr>
<tr>
<td>UBA Server</td>
<td>6272, 6273</td>
</tr>
</tbody>
</table>
## Custom AD Use Cases – Field Name for Query String Analytics

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>computer_account_name</td>
<td>service_name</td>
</tr>
<tr>
<td>dest_host_name (*)</td>
<td>src_host_name (*)</td>
</tr>
<tr>
<td>dest_ip</td>
<td>src_ip</td>
</tr>
<tr>
<td>group_domain</td>
<td>status_code</td>
</tr>
<tr>
<td>logon_entity_type</td>
<td>sub_status_code</td>
</tr>
<tr>
<td>logon_guid</td>
<td>subject_account_name (*)</td>
</tr>
<tr>
<td>logon_process_name</td>
<td>subject_account_ou</td>
</tr>
<tr>
<td>logon_type</td>
<td>target_account_name (*)</td>
</tr>
<tr>
<td>process_name</td>
<td>target_account_ou</td>
</tr>
<tr>
<td>sam_account_name (*)</td>
<td></td>
</tr>
</tbody>
</table>

* Denotes fields that can be obfuscated
# Custom AD Use Case #1

## Analytics

### AD-BASED USE CASE NAME

**User privilege escalation to join Guardians of the Galaxy**

<table>
<thead>
<tr>
<th>ALERT TYPE</th>
<th>ALERT CATEGORY</th>
<th>ATTACK STAGE</th>
<th>SEVERITY</th>
<th>CONFIDENCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privilege Escalation</td>
<td>Account Activity</td>
<td>Internal Activity</td>
<td>70</td>
<td>60</td>
</tr>
</tbody>
</table>

### ENTITY

Target Account Name

### QUERY STRING

`event_id:4732 AND group_name:guardians_of_the_galaxy`

### ALERT STRING TEMPLATE

Account `$target_account_name$` was added to group Guardians of the Galaxy by `$subject_account_name$`

### 0 LOCAL MODIFICATIONS FOR THE USE CASE

### USE CASE DESCRIPTION

AD Use Case #3
Custom AD Use Case #2
Analytics

AD-BASED USE CASE NAME
Non-admin role created new user

<table>
<thead>
<tr>
<th>ALERT TYPE</th>
<th>ALERT CATEGORY</th>
<th>ATTACK STAGE</th>
<th>SEVERITY</th>
<th>CONFIDENCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Suspicious Account Activity</td>
<td>Account Activity</td>
<td>Internal Activity</td>
<td>80</td>
<td>60</td>
</tr>
</tbody>
</table>

ENTITY
Subject Account Name

QUERY STRING
event_id:4720 AND NOT subject_account_name:Admin

ACCOUNT STRING/TEMPLATE
$target_account_name$ was created by $subject_account_name$

LOCAL MODIFICATIONS FOR THE USE CASE

USE CASE DESCRIPTION
AD Use Case #2
Modifications (MUTE)

Add/Edit/Delete Modifications from the Analytics Page

Add Modifications before the Alert gets triggered. Reduces False positives
- Known groups or users exporting large amount of data
- Known Vulnerability Assessment scanners
- Known penetration testing systems
- Known applications that trigger Remote Authentications
Peer group support for arbitrary LDAP attributes

Analytics

What were the options in 2.3?
- OU
- Department
- Custom Software changes

What changed?
- Added more LDAP attributes for Peer Groups
- Can select multiple

Who found it useful?
- No consistent Mapping of OU or Department and want to use other LDAP attributes
- Test which Peer based analytics makes the most sense in their environment

NOTE: for HVA server use cases, if the entity type is IP address, the analytics group can only be 'Enterprise' otherwise Peer analytics won't work for those use cases.
Peer group support for arbitrary LDAP attributes

Examples

Abnormal volume of upload from an user to box.net

Peer Groups: Title, Manager

User eflow_canned_2_peer on host eflow_canned_2_peer-pc.niara.com uploaded 9.83 GB to Boxnet on Apr 14, 2018, compared with users having title Sales Director who uploaded an average of 48.88 MB during the same day.

User eflow_canned_2_peer on host eflow_canned_2_peer-pc.niara.com uploaded 9.83 GB to Boxnet on Apr 14, 2018, compared with users reporting to manager Jon Snow who uploaded an average of 48.88 MB during the same day.
Privileged and Service Account Analytics

Analytics

Motivation

Visibility of accounts with higher privileges to monitor misuse

Feature Description

Classification of user accounts based on data ingested from LDAP

- Human
- Nonhuman
- Service (user account that is explicitly created to provide security context for services running on Windows Server)
- Privileged
- Admin
- Executive
Privileged and Service Account Analytics

Feature Description

Classification of user accounts is done based on two methods

- Auto-detection of account types from LDAP attributes using heuristics-based approach
- User configuration using regular expressions to group users based on a pattern
Privileged and Service Account Analytics

Analytics

Account Type Classification

<table>
<thead>
<tr>
<th>Account Type</th>
<th>Matching Values</th>
</tr>
</thead>
</table>
| Executive    | EXEC_TITLE_EMATCH = ['ceo', 'cfo', 'cto', 'c.e.o', 'c.f.o', 'c.t.o', 'vp', 'evp']  
EXEC_TITLE_PMATCH = ['president', 'chairman', 'officer', 'founder', 'director'] |
| Service      | ou has 'service accounts' or 'system accounts' |
| Privileged   | belongs to one of the following:  
PRIVILEGED_GROUPS = ['cn=remote desktop users', 'cn=event log readers',  
'cn=performance log users',  
'cn=performance monitor users'] |
| Admin        | ou has 'admin accounts' or 'administrator'  
begins to one of the default Admin Groups |
Privileged and Service Account Analytics

Analytics

User Configured Account Types

Note:
Pattern uses python REGEX

```
admin\..*
```

NOT
```
admin..*
```

- . = matches any single character
- \_ = matches the character ‘_’ (period)
- .* = matches 0 or more character
- \d* = matches 0 or more digits [0-9]*
- -* = matches 0 or more ‘-’ (dash)

Python regex reference: https://docs.python.org/2/library/re.html
VPN Logon using privileged account

Analytics

**USE CASE NAME**
VPN Logon using privileged account

<table>
<thead>
<tr>
<th>ALERT TYPE</th>
<th>ALERT CATEGORY</th>
<th>ATTACK STAGE</th>
<th>SEVERITY</th>
<th>CONFIDENCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Abnormal User Log...</td>
<td>Remote Access</td>
<td>Internal Activity</td>
<td>60</td>
<td>80</td>
</tr>
</tbody>
</table>

**ENTITY**
User Name

**QUERY STRING**
user_account_type:admin_account OR user_account_type:service_account OR user_account_type:privileged_account

**ALERT STRING TEMPLATE**
Privileged account $user_name$ logged into via VPN

**0 ACTIVE MODIFICATIONS EXIST FOR THE USE CASE**

**USE CASE DESCRIPTION**
VPN Logon using privileged account

SAVE  CANCEL

* Indicates mandatory fields
Office 365 support
Analytics

Background and Motivation
Many customers (small and large) have adopted cloud based applications and O365 is very prevalent
• Off-premise activity monitoring
Granular reporting (individual file-access)
Requested by existing and potential customers
Most competitors have some kind of Office 365 'connector' (Splunk, Exabeam, Securonix, Darktrace)

Feature Description – Phase I Focus
Log Ingestion: Splunk and Native Cloud API
Basic built-in use-cases
• Behavioral
Custom Use cases
Office 365 support
Applications Supported

- Sharepoint
- AzureActiveDirectory
- OneDrive
- Exchange
- DataCenterSecurity
- Compliance
- Sway
- Yammer
- SecurityComplianceCenter
- PowerBI
- MicrosoftTeams
- MicrosoftFlow

Some of the Audit activities we parse.
Exchange: Admin activity
OneDrive: Admin activities, file activity
SharePoint: File activity, sharing activity
Security and Compliance Center: User and Admin activity, alerts
Azure AD: O365 logins, directory activities
Power BI: Admin activities
Office 365 Support
Use Cases

Peer Baseline
- Excessive Number of Files Accessed from Cloud
- Excessive Number of Files Downloaded from Cloud

Historical Baseline
- Excessive Number of Files Accessed from Cloud
- Excessive Number of Files Downloaded from Cloud
- Remote Cloud Access from New Location
- Remote Cloud Access with Land Speed Violation
Office 365 Support
Custom Use Case

Useful Attributes

**operation**:       **file_name**
- FileAccessed       -
- FileDownloaded     -
- FileModified       -
- FileDeleted        -
- FileUploaded       -
-FileSyncDownloadedFull
-FileSyncUploadedFull

(path: app_subtype: file_type: remote_country)

(operation:FileAccessed or operation:FileDownloaded or operation:FileModified or operation:FileDeleted or operation:FileSyncDownloaded) AND file_name:*Classified*
Ransomware Detection
Analytics

Background and Motivation
Top Malware threat for Enterprise
Multiple customers’ feature request
Competition

Feature Description
Ransomware detection in < 5 mins
Machine Learning Models

**Supervised**
(Real Time Analytics)

Global: Actions are irrefutably malicious and apply to all

- Faster detection
- Lower false positive rate

**Unsupervised**
(Behavioral Analytics)

Local: Baseline normal behaviours and identify anomalies

- Learning period
- Requires feedback/tuning
Detection details

- Based on an ML-based model that detects suspicious file operations in the SMB network traffic
- Sub 5-minute detection since the commencement of disk encryption activity
- Can be combined with C&C and lateral movement alerts as a chained alert to raise the severity and confidence of the ransomware event
- Alert remediation via CPPM integration
- 20+ SMB related features used in the ML model to detect ransomware activity
  - Reads
  - Writes
  - # of files seeks
  - Total commands
  - Duration
  - Log[bytes]
  - # of renames
  - # of deletes
  - Known ransomware file extensions
  - Rename loop detection
  - Significant % files with the same extension
  …
Ransomware Detection with IntroSpect

**Infection**
- IOC-STIX
- Ransomware Tracker
- Suspicious Email Attachment
- Suspicious Email Domain

**Command and Control**
- DNS DGA
- DNS Tunneling

**Lateral Spread**
- Host scan
- Port scan
- Abnormal host access
- Excessive host activity
- Failed auths
- New logons

**Encryption**
- Unusual file activity
- Detect network share encryption

**Supervised ML**
- Beaconing Activity
- New Country Access

**Unsupervised ML**
Ransomware
A Simple illustration of a Ransomware Attack

Your not-so-friendly neighborhood Ransomware

Email / Lateral spread

Encrypt

Drives
C:/Local
D:/Network
E:/Network

Encrypt

Encrypt

Encrypt

Encrypt

Bulk operations within a short period of time

Single TCP session
SMB Read/Write/Rename/Delete
Ransomware
Aruba Threat Lab Research

Ransomware

Wannacry
Dharma
Gandcab
Hermes
Matrix
Scarab
GlobeImposter
Trickbot
Cryptomix
Jigsaw
Keypass
CryptoShield
Sage
Revenge
Alphacrypt
BigBobRoss
BlackRouter

Juicylemon
Outsider
Phobos
Ryuk
Saturn
Seon
Teslacrypt
Shade
Ryuk
LockerGoga

and more .....
Ransomware Beaconing

The event is triggered by frequent communication between a vulnerable/infected host and a rare domain which is indicative of a C2 domain. Beaconing is a *low and slow method* of communicating with a malware C2 domain. After a malware infects a vulnerable host, it initiates a channel back to the command and control site. After it establishes a connection, the infected host will communicate at *regular time intervals*.

- Source IP Address
- Destination DNS name
- Protocol (HTTP/HTTPS/DNS)
- Frequency
- Outbound Traffic payload
- Inbound Traffic payload

Requires visibility into North – South traffic sent via SPAN to the Packet Processor.

**Limitation**: Minimum period detectable is 3 seconds and Maximum is 74 seconds.
Ransomware
Suspicious SMB Share Encryption

This event is triggered when a host accesses a SMB network share and performs a large number of file operations such as writes/renames/delete leading to encrypting the files in a short period of time. This event is an indicator of Ransomware trying to encrypt files on the users device and also remote SMB shares.

- Source IP
- Destination IP
- Distinct Shares
- SMB Operations
- Time since activity started

Requires visibility into East – West traffic sent via SPAN to the Packet Processor
ANALYST WORKFLOW
Alert clustering using frequent pattern mining
Analyst Workflow

Background and Motivation
Investigating large number of (first-order) alerts one by one is time-consuming
Usually a ‘pattern’ or commonality in the alerts of the same type (per use-case)
Finding the ‘pattern’ for visualization and applying MUTE
Set a time limit for MUTE (don’t want to set the exception indefinitely all the time)

Feature Description
Use Frequent Pattern Mining techniques to cluster alerts
Visualize alert clusters and apply MUTE
Set time-limit for MUTE
Alert clustering using frequent pattern mining
Clustering UI → Alerts → Clusters
Alert clustering using frequent pattern mining
Clusters UI → Card
Alert clustering using frequent pattern mining
Clusters UI \rightarrow Card
Behavioral Baseline Visualization
Analyst Workflow

Background and Motivation
Provide insights on an entity’s baseline behavior and why an alert was triggered (or not)

Feature Description
Introduced in 2.4 release in Conversations > Visual > Use Case Visualization
Applies to behavioral use cases (historical or peer) based on conversations (eflows) only
In 2.5 release, there is new Getting started screen to select use case and associated entity
Behavioral Baseline Visualization
Analyst Workflow

Select the desired use case to visualize
Select one or more entities to be included in visualization
Behavioral Baseline Visualization
Analyst Workflow

Each bar in chart is clickable to get further details

Only conversations that meet these conditions are included in visualization of use case
Behavioral Baseline Visualization
Analyst Workflow

Details

- **Apr 29**
  - Unique Dest. IP Subnets: 2
  - Unique Dest. IPs: 23

**Dest. IP subnet distribution**
- 2 Dest. IP subnets
  - 10.49.0.0/24
  - 10.44.1.0/24

**Time distribution**
- Count
  - 0:00 am - 1:00 am: 150
  - 3:00 am - 4:00 am: 100
  - 5:00 am - 6:00 am: 50

**Applications**
- 1 Application
  - unknown-123

**Protocols**
- Protocol
  - 10

---

@ArubaAPAC | #ATM19APAC
Network Visualization
Analyst Workflow

Background and Motivation
Visualization provides the first step in operational and security insights for the monitored environment
• Big picture view before investigation of machine-learning-based and rules-based analytics

Feature Description
In 2.5 release, the visualizations are organized into new dashboards from the main landing page
• Risk Posture: original dashboard from previous releases’ landing page (no change)
• Security Data: new dashboard for visualization (descriptions in following slides)
• Traffic Data: new dashboard for visualization (descriptions in following slides)
Network Visualization
Security Data Dashboard
Network Visualization
Security Data Dashboard

Distribution of conversations by policy violation, defined as Bitcoin, BitTorrent, OpenVPN, P2P, and TOR activity.

This is internally defined in the system and is not user-configurable.

List of custom rules-based use cases that have recently triggered.

List of users that display admin-like behavior where they are not classified as admins.

Behavior is based on apps used such as ssh, rdp, wmi.
Network Visualization
Security Data Dashboard

- Scatter plot of Source IPs vs Conversations for HTTP(S) Domains, User-Agents, and ASN Destination Accessed
- Rare is defined as < 10 sources
- Data in the lower right quadrant of the chart would be considered suspicious activity
- All conversations data is included in the charts, it is not dependent on the date range as specified by symbol on top left of the chart
Network Visualization
Traffic Data Dashboard
Network Visualization
Traffic Data Dashboard

Displays destination countries of the conversations for the given date range.

Color coded according to scale at bottom left of the chart.

Can toggle between Bytes, Users, and Number of Conversations

Displays Source/Destination pair traffic according to Zones that are configured by the end user.

Zones is configured by CSV file which is a list of subnets and corresponding name of zone.

Displays volume of traffic for the given date range.

Can toggle between Bytes, Users, and Number of Conversations
Network Visualization
Traffic Data Dashboard

Scatter plot of App categories by Number of Users vs. Volume of Conversations for the given date range

App categories include Social Media, File Sharing, Email, Photo-Video, General-Business, Infrastructure

Distribution of Applications traffic for the given date range
Can toggle between Bytes, Users, and Number of Conversations

Heat map of total Conversations traffic for the given date range
Can toggle between Bytes, Users, and Number of Conversations
Expanded 3rd party alerts
Data Diversity

Motivation
• Alerts from 3rd party sources can influence an entity’s risk score
• 3rd party alerts can be coupled with other native IntroSpect alerts to investigate an entity

Description
• Add a Log parser
• Add a new use-case
• Affects the risk score based on Severity and confidence of the alert triggered

Splunk Notable events
• Available by default from 2.4
ClearPass integration Phase 2
Data Diversity

Motivation
• Automated actions
• Provide more context to ClearPass

Description
• Send Syslog for
  • Entities
  • Security Alerts
• Parse them on ClearPass using Ingress Event Engine
• Take policy decisions or automated actions
ClearPass integration Phase 2
Pictorial View
Questions?
Thank You