a Hewlett Packard
Enterprise company

SOLUTION OVERVIEW

ALERT PRIORITIZATION AND INCIDENT INVESTIGATION WITH INTROSPECT UEBA

EXECUTIVE SUMMARY

Aruba IntroSpect User and Entity Behavior Analytics (UEBA) enables security teams to efficiently prioritize alerts from multiple systems and effectively investigate and triage incidents through analytics-driven visibility. IntroSpect builds comprehensive risk profiles for each user and entity (i.e., anything with an IP address) by applying AI-based machine learning and behavioral analytics techniques on data from both network and security infrastructure. These Entity360 profiles include continuous risk scoring and granular enriched security information which significantly reduces the time and effort to discover, understand and respond to threats.

OVERVIEW

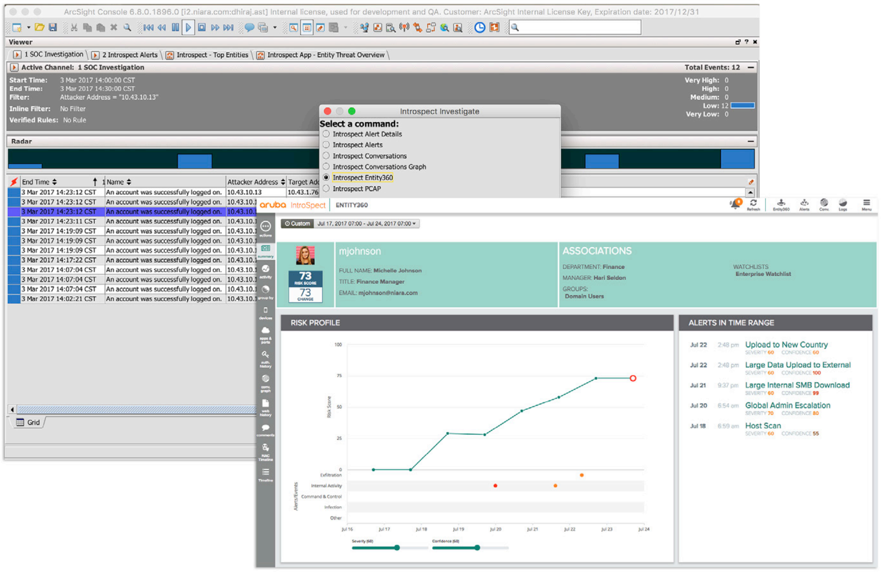
Security incidents continue to happen, yet focusing on and investigating the threats that really matter is very challenging. Security analysts spend much of their time searching, finding, organizing and analyzing information from multiple siloed systems – gathering important insights, but unable to adequately prioritize and investigate all the alerts they receive. Most enterprises simply don't have the resources, solutions, staff or time to investigate the hundreds of alerts they see every day.

THE INTROSPECT APPROACH

IntroSpect UEBA helps analysts more efficiently recognize pending attacks and more quickly investigate incidents in their environment. IntroSpect is the only solution that leverages diverse network and security data sources – i.e., packets, flows, logs, alerts, endpoint, cloud, and threat feeds – for machine learning-based analytics, providing unmatched visibility. The IntroSpect platform can help in the following manner:

1. Diverse supervised and unsupervised machine learning techniques deliver comprehensive, high-fidelity Entity360 profiles not just for users, but also for hosts and devices—anything with an IP address. These analytics results are statefully tracked over time and contribute to an entity's overall risk score. These risk scores serve as a reliable and holistic way to focus the analyst on the threats that matter.

   For example, IntroSpect's analytics can plug into existing SIEM or log management systems to help prioritize the rule-based alerts based on the user. In Figure 1, an ArcSight rule fire is dynamically mapped to the user in question by IntroSpect and the risk profile for the affected user is presented back to ArcSight to help the analyst determine its relative priority.



ArcSight Console 6.8.0.1896.0 [i2.niara.com:dhiraj.ast] Internal license, used for development and QA. Customer: ArcSight Internal License Key, Expiration date: 2017/12/31

Viewer

1 SOC Investigation \ 2 Introspect Alerts \ Introspect - Top Entities \ Introspect App - Entity Threat Overview

Active Channel: 1 SOC Investigation — Total Events: 12

Start Time: 3 Mar 2017 14:00:00 CST
End Time: 3 Mar 2017 14:30:00 CST
Filter: Attacker Address = "10.43.10.13"
Inline Filter: No Filter
Verified Rules: No Rule

Very High: 0
High: 0
Medium: 0
Low: 12
Very Low: 0

Radar

End Time	Name	Attacker Address	Target Add
3 Mar 2017 14:23:12 CST	An account was successfully logged on.	10.43.10.13	10.43.1.76
3 Mar 2017 14:23:12 CST	An account was successfully logged on.	10.43.10.1	
3 Mar 2017 14:23:12 CST	An account was successfully logged on.	10.43.10.1	
3 Mar 2017 14:23:11 CST	An account was successfully logged on.	10.43.10.1	
3 Mar 2017 14:19:09 CST	An account was successfully logged on.	10.43.10.1	
3 Mar 2017 14:19:09 CST	An account was successfully logged on.	10.43.10.1	
3 Mar 2017 14:19:09 CST	An account was successfully logged on.	10.43.10.1	
3 Mar 2017 14:17:22 CST	An account was successfully logged on.	10.43.10.1	
3 Mar 2017 14:07:04 CST	An account was successfully logged on.	10.43.10.1	
3 Mar 2017 14:07:04 CST	An account was successfully logged on.	10.43.10.1	
3 Mar 2017 14:07:04 CST	An account was successfully logged on.	10.43.10.1	
3 Mar 2017 14:02:21 CST	An account was successfully logged on.	10.43.10.1	

Grid

Introspect Investigate

Select a command:
○ Introspect Alert Details
○ Introspect Alerts
○ Introspect Conversations
○ Introspect Conversations Graph
● Introspect Entity360
○ Introspect PCAP

aruba IntroSpect | ENTITY360

Custom Jul 17, 2017 07:00 - Jul 24, 2017 07:00

73 RISK SCORE
73 CHANGE

mjohnson
FULL NAME: Michelle Johnson
TITLE: Finance Manager
EMAIL: mjohnson@niara.com

ASSOCIATIONS
DEPARTMENT: Finance
MANAGER: Hari Seldon
GROUPS: Domain Users
WATCHLISTS: Enterprise Watchlist

RISK PROFILE

ALERTS IN TIME RANGE

Jul 22 2:48 pm Upload to New Country
SEVERITY 60 CONFIDENCE 60

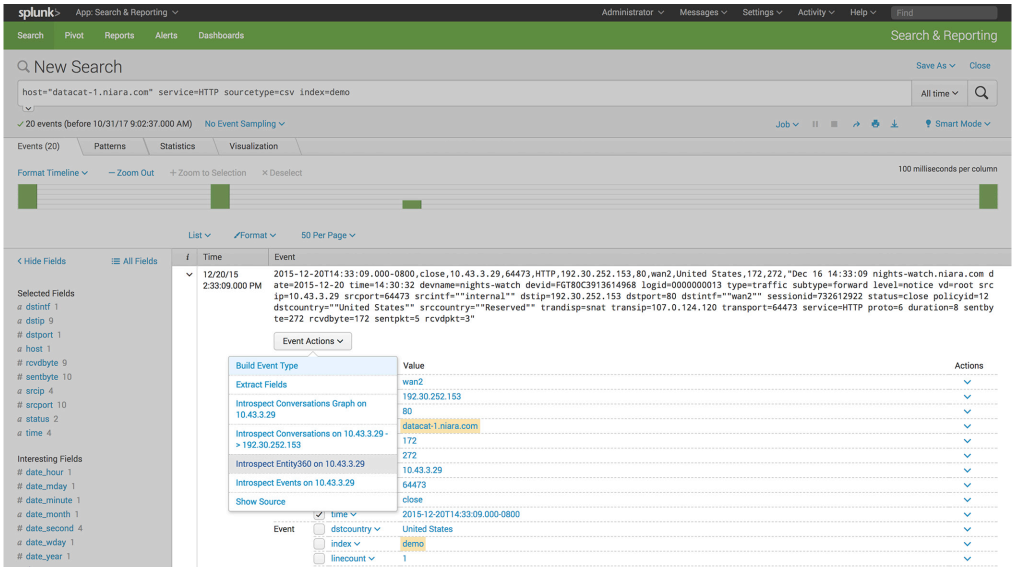
Jul 22 2:48 pm Large Data Upload to External
SEVERITY 60 CONFIDENCE 100

Jul 21 9:37 pm Large Internal SMB Download
SEVERITY 60 CONFIDENCE 99

Jul 20 6:54 am Global Admin Escalation
SEVERITY 70 CONFIDENCE 80

Jul 18 6:59 am Host Scan
SEVERITY 60 CONFIDENCE 55

Figure 1: IntroSpect Entity360 can be easily accessed from ArcSight



```
host="datacat-1.niara.com" service=HTTP sourcetype=csv index=demo
```

✓ 20 events (before 10/31/17 9:02:37.000 AM)

Selected Fields
- a dstintf 1
- a dstip 9
- # dstport 1
- a host 1
- # rcvdbyte 9
- # sentbyte 10
- a srcip 4
- # srcport 10
- a status 2
- a time 4

Interesting Fields
- # date_hour 1
- # date_mday 1
- # date_minute 1
- a date_month 1
- # date_second 4
- a date_wday 1
- # date_year 1

i	Time	Event
	12/20/15 2:33:09.000 PM	2015-12-20T14:33:09.000-0800,close,10.43.3.29,64473,HTTP,192.30.252.153,80,wan2,United States,172,272,"Dec 16 14:33:09 nights-watch.niara.com date=2015-12-20 time=14:30:32 devname=nights-watch devid=FGT80C3913614968 logid=0000000013 type=traffic subtype=forward level=notice vd=root srcip=10.43.3.29 srcport=64473 srcintf=""internal"" dstip=192.30.252.153 dstport=80 dstintf=""wan2"" sessionid=732612922 status=close policyid=12 dstcountry=""United States"" srccountry=""Reserved"" trandisp=snat transip=107.0.124.120 transport=64473 service=HTTP proto=6 duration=8 sentbyte=272 rcvdbyte=172 sentpkt=5 rcvdpkt=3"

Event Actions:
- Build Event Type
- Extract Fields
- Introspect Conversations Graph on 10.43.3.29
- Introspect Conversations on 10.43.3.29 -> 192.30.252.153
- Introspect Entity360 on 10.43.3.29
- Introspect Events on 10.43.3.29
- Show Source

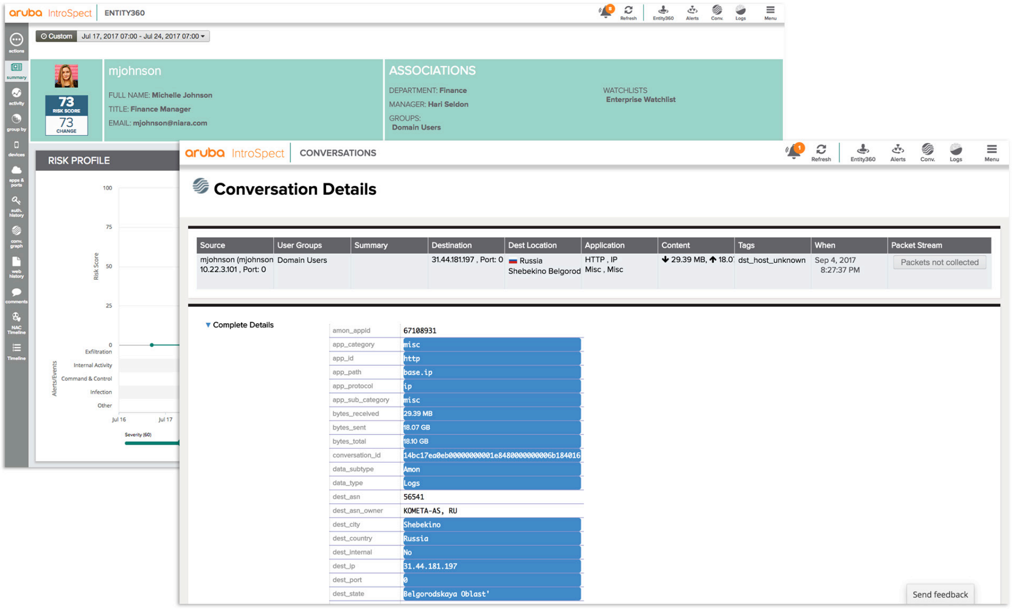
	Field	Value
		wan2
		192.30.252.153
		80
		datacat-1.niara.com
		172
		272
		10.43.3.29
		64473
		close
	☑ time	2015-12-20T14:33:09.000-0800
Event	☐ dstcountry	United States
	☐ index	demo
	☐ linecount	1

Figure 2: IntroSpect Entity360 can be easily accessed from Splunk

2. Once the alert has been deemed as high priority and worthy of investigation, IntroSpect helps the analyst investigate the affected user and alert in a comprehensive manner. Layered forensics, ranging from rich metadata to raw log and network data, support investigating a user, system or device with a high risk score. With IntroSpect, security analysts get one-click access to the information they need to investigate and triage the incident. And a big data-based architecture enables IntroSpect to scale easily, economically extending the investigation window to months and years if needed.

3. IntroSpect automates vast chunks of an analyst's incident investigation workflow by instantly providing answers to questions every analyst asks when faced with potential attack. For example, when an analyst has to investigate an alert, they need to be able to answer:

- Who or what did this happen to
- What exactly happened
- Who else or what else did it happen to



mjohnson

FULL NAME: Michelle Johnson
TITLE: Finance Manager
EMAIL: mjohnson@niara.com

ASSOCIATIONS

DEPARTMENT: Finance
MANAGER: Hari Seldon
GROUPS:
Domain Users

WATCHLISTS
Enterprise Watchlist

Conversation Details

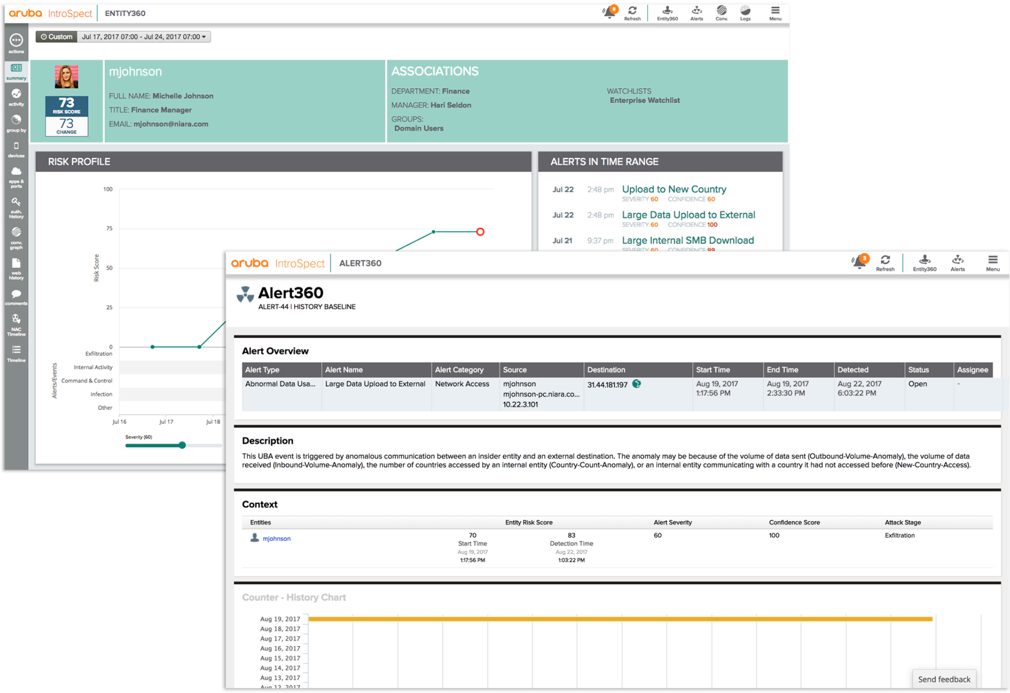
Source	User Groups	Summary	Destination	Dest Location	Application	Content	Tags	When	Packet Stream
mjohnson (mjohnson 10.22.3.101 , Port: 0	Domain Users		31.44.181.197 , Port: 0	Russia Shebekino Belgorod	HTTP , IP Misc , Misc	↓ 29.39 MB, ↑ 18.0	dst_host_unknown	Sep 4, 2017 8:27:37 PM	Packets not collected

▼ Complete Details

amon_appid	67108931
app_category	misc
app_id	http
app_path	base.ip
app_protocol	ip
app_sub_category	misc
bytes_received	29.39 MB
bytes_sent	18.07 GB
bytes_total	18.10 GB
conversation_id	14bc17ea0eb00000000001e8480000000006b184016
data_subtype	Amon
data_type	Logs
dest_asn	56541
dest_asn_owner	KOMETA-AS, RU
dest_city	Shebekino
dest_country	Russia
dest_internal	No
dest_ip	31.44.181.197
dest_port	0
dest_state	Belgorodskaya Oblast'

Figure 3: IntroSpect Entity360 provides analysts with 1-click access to the information needed for investigations such as the details of network conversations.

The final question is just as important because anytime remediation actions have to be initiated, the analyst has to be certain that the threat has been fully contained. In the screenshot below, IntroSpect has consumed a FireEye alert and has not only identified the user in question and detailed exactly what happened, but has also extracted the IOC (Indicators of Compromise) in question to identify other users who might have also been to the same, potentially infected, site but evaded detection.



Jul 17, 2017 07:00 - Jul 24, 2017 07:00

mjohnson

FULL NAME: Michelle Johnson
TITLE: Finance Manager
EMAIL: mjohnson@niara.com

ASSOCIATIONS

DEPARTMENT: Finance
MANAGER: Hari Seldon
GROUPS:
Domain Users

WATCHLISTS
Enterprise Watchlist

ALERTS IN TIME RANGE

Jul 22 2:48 pm Upload to New Country
SEVERITY 60 CONFIDENCE 60

Jul 22 2:48 pm Large Data Upload to External
SEVERITY 60 CONFIDENCE 100

Jul 21 9:37 pm Large Internal SMB Download
SEVERITY 60 CONFIDENCE 99

Alert360
ALERT-44 I HISTORY BASELINE

Alert Overview

Alert Type	Alert Name	Alert Category	Source	Destination	Start Time	End Time	Detected	Status	Assignee
Abnormal Data Usa...	Large Data Upload to External	Network Access	mjohnson mjohnson-pc.niara.co... 10.22.3.101	31.44.181.197	Aug 19, 2017 1:17:56 PM	Aug 19, 2017 2:33:30 PM	Aug 22, 2017 6:03:22 PM	Open	-

Description

This UBA event is triggered by anomalous communication between an insider entity and an external destination. The anomaly may be because of the volume of data sent (Outbound-Volume-Anomaly), the volume of data received (Inbound-Volume-Anomaly), the number of countries accessed by an internal entity (Country-Count-Anomaly), or an internal entity communicating with a country it had not accessed before (New-Country-Access).

Context

Entities	Entity Risk Score		Alert Severity	Confidence Score	Attack Stage
mjohnson	70 Start Time Aug 19, 2017 1:17:56 PM	83 Detection Time Aug 22, 2017 1:03:22 PM	60	100	Exfiltration

Figure 4: IntroSpect Entity360 makes it easy for analysts to get answers to key questions when faced with potential attacks

IntroSpect UEBA helps analysts of all experience levels more efficiently achieve the goal of any incident investigation and response program, which is to find and respond to gestating attacks before they do damage and consequently minimize the risk to their organization.

SUMMARY

IntroSpect supercharges security teams' alert prioritization and incident investigation capabilities, allowing them to easily confront the challenge of alert volumes and focus on the attacks that truly matter.

IntroSpect does this by applying advanced analytics to a broad range of data sources (i.e., packets, flows, logs, files, alerts, endpoint, cloud, and threat feeds) and building high-fidelity Entity360 risk profiles. Alert prioritization is easily addressed by using risk scores in Entity360 to set the priority of investigation. Attacks can be instantly traced to the affected user/host/device and in depth investigation is easy with one-click access to detailed, correlated views into all the relevant activity.

ABOUT ARUBA, A HEWLETT PACKARD ENTERPRISE COMPANY

Aruba, a Hewlett Packard Enterprise company, is a leading provider of next-generation networking solutions for enterprises of all sizes worldwide. The company delivers IT solutions that empower organizations to serve the latest generation of mobile-savvy users who rely on cloud-based business apps for every aspect of their work and personal lives. For more information visit www.arubanetworks.com. For real-time news updates follow Aruba on Twitter and Facebook, and for the latest technical discussions on mobility and Aruba products visit Airheads Community at http://community.arubanetworks.com.

For more information, go to http://www.arubanetworks.com/products/security/ueba/

aruba
a Hewlett Packard
Enterprise company

www.arubanetworks.com

3333 SCOTT BLVD | SANTA CLARA, CA 95054
1.844.473.2782 | T: 1.408.227.4500 | FAX: 1.408.227.4550 | INFO@ARUBANETWORKS.COM