aruba
a Hewlett Packard Enterprise company

SOLUTION OVERVIEW

UEBA USE CASE: INSIDER ATTACK IDENTIFICATION WITH INTROSPECT

EXECUTIVE SUMMARY

Aruba IntroSpect's User and Entity Behavioral Analytics (UEBA) automates the detection of insider threats from malicious insiders and negligent employees that are hard to detect by traditional means. Security teams can accelerate their investigations and hunt for such incidents through analytics-driven visibility. IntroSpect builds risk profiles for users and hosts by applying behavioral analytics techniques, including supervised and unsupervised machine learning, on data collected from the network and security infrastructure from packets, flows, logs, and alerts. IntroSpect's combines machine learning with layered forensics for rich context, and delivers a differentiated solution that enables attack detection and incident investigation without relying on rules, configuration and signatures.

OVERVIEW

The insider threat is well recognized as a significant enterprise security risk. The Verizon 2017 Data Breach Investigations Report[1] classifies this threat as insider and privilege misuse, which includes non-sanctioned or malicious use of an organization's resources. These incidents involve users behind your firewall, acting carelessly or with malice alone or in collusion with outsiders. These users have easy access to an organization's data and are comfortable exfiltrating data out in the open on the corporate LAN.

Only 28% of these insiders are in leadership roles (i.e., executive or other management) or roles with elevated access (e.g., system administrators or developers. Almost one third are end users who have access to sensitive data as a requirement of their role. The takeaway is that organizations need to worry less about job titles and more about the level of access that each user has as well as the ability to monitor them. Almost 60% of the incidents are motivated by financial gain or espionage purposes, but there are also healthy occurrences of employees negligently mishandling data or misusing email, web and USB devices to place an organization's data and sensitive assets at risk.

Insider incidents are the hardest (and take the longest) to detect. According to the Verizon report, an overwhelming majority of these insider misuse cases take months or years to discover. Insiders are people within who know about the organizations' security practices, data and IT systems – e.g., employees, contractors, and business partners. Motivations can vary, ranging from anger to greed to politics. For example, employees get a whiff of an upcoming reduction in force and start downloading commercially valuable information from the corporate server prior to the layoff. Or a disgruntled executive assistant is secretly emailing out sensitive board meeting minutes to an interested 3rd party. But attributing purposeful threats (e.g., fraud, sabotage, theft of confidential information) back to malcontents is tough. After all, as trusted insiders, they have broad privileges to freely move about their company's internal networks.

THE ARUBA INTROSPECT DIFFERENCE

IntroSpect can help analysts detect and investigate insider threats posed by negligent and malicious insiders. It uniquely does this by observing users over long time periods, gleaning security insights by applying machine learning-based analytics, and correlating all activity back to the users.

1. Different from other UEBA solutions, IntroSpect's analytics uses diverse data sources (i.e., packets, flows, logs, files, 3rd-party alerts and threat feeds), to observe users and data. IntroSpect applies true machine learning on all the aforementioned data sources across a whole range of dimensions – authentication, remote access, peer-to-peer activity, internal access to high value server, internet usage, DNS activity, cloud application usage – to paint a composite picture of every user and host. Disparate events for a user are statefully tracked over time to flag employees whose behavior may be indicative of risky or rogue behavior.

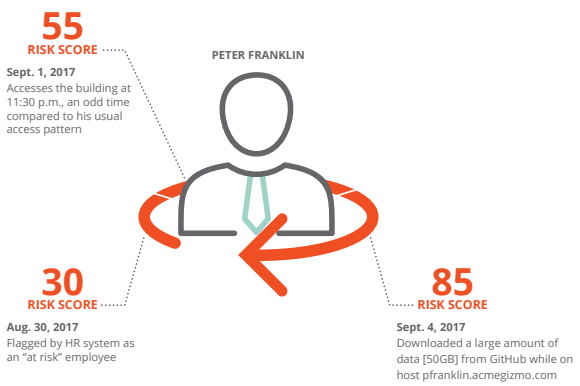

Figure 1: IntroSpect provides contextually-weighted risk scores to account for the severity, sequencing, distribution and temporal significance of events.

[1] 2017 Data Breach Investigations Report, Verizon

2. Because IntroSpect looks at diverse data sources that may provide clues around user behavior, IntroSpect can spot anomalies on many dimensions:
   - **Abnormal behavior on internal resources:** Users who abuse their privileges to download more information or access resources at an odd time or spending a lot of time on a high value server
   - **Physical access:** Tying digital activity to physical activity such as building access at odd times or tailgating
   - **Business context:** Tying into HR systems or analyst input around at-risk employees or high value assets

3. The combination of the comprehensive analytics applied to the diverse data sources means that the detection vectors supported by IntroSpect include:
   - **Privileged account abuse** – inappropriate use of access permissions to abuse access to sensitive data
   - **Abnormal access to high value resource**s – abuse of access permissions to download internal sensitive information for e.g. source code or PII information
   - **Unusual activity** – remotely accessing high privileged assets, and unusual login duration, time or location
   - **Password sharing** – inappropriate sharing of passwords by users leading to violation of corporate security policies
   - **Exfiltration, including cloud application-based exfiltration** – using cloud applications or external sites to exfiltrate data

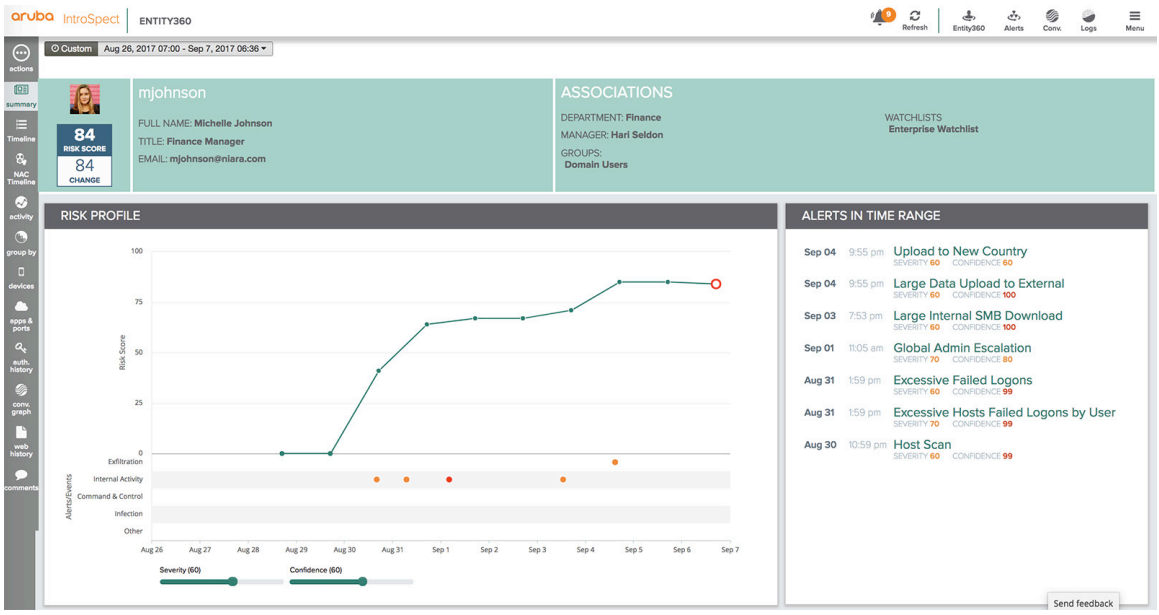

Figure 2: IntroSpect Entity360 makes it easy to spot anomalies, such as excessive failed logins, noted above.

4. Investigation is just as important. While detecting insider activity that could potentially place your information at risk, it is just as important to provide enough context to help truly understand what happened. This is important for 2 reasons:

A. First, let's say that we detect that a user uploaded a lot of sensitive information to Dropbox. The security analyst has to then be able to investigate the user around the event, sometimes going back months to truly understand:
   - Every asset that the user had access to
   - What did they end up gaining access to?
   - What other data may be at risk for exfiltration?

B. Sometimes, systems cannot always detect the insider activity, which means having the information to be able to investigate the user ex-post is extremely important.

Since IntroSpect correlates all the data at a user or host level, and not just at investigation time, this makes investigating an incident for an "insider" extremely easy. The analyst can go from a behavioral anomaly alert to a detailed investigation of the user extremely easily.

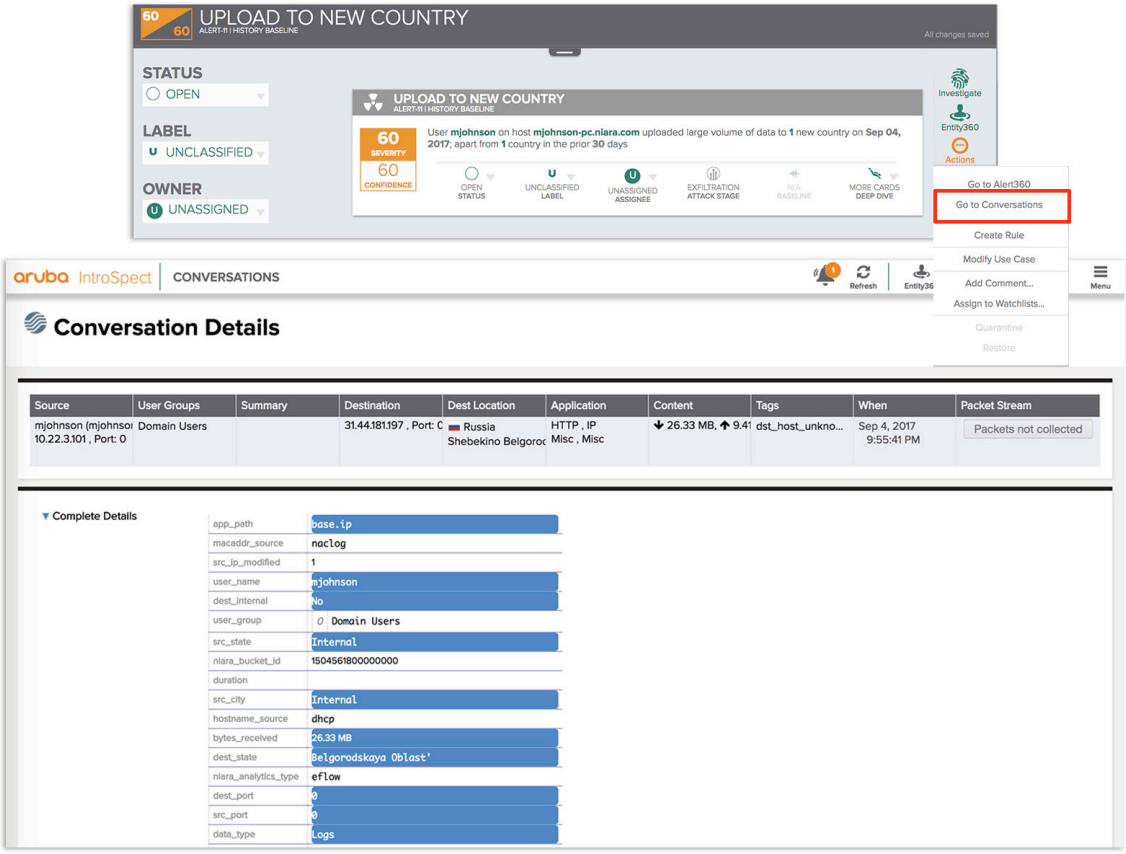

Figure 3: IntroSpect makes it easy to pivot from an alert to the contextual evidence, all in a single system.

IntroSpect also makes it easy to investigate any user very easily. For example, a query such as "Show me all the internal activity for user 'mjohnson' where he downloaded more than 10MB over the last 6 months" is extremely easy, producing the results shown in the figure below.

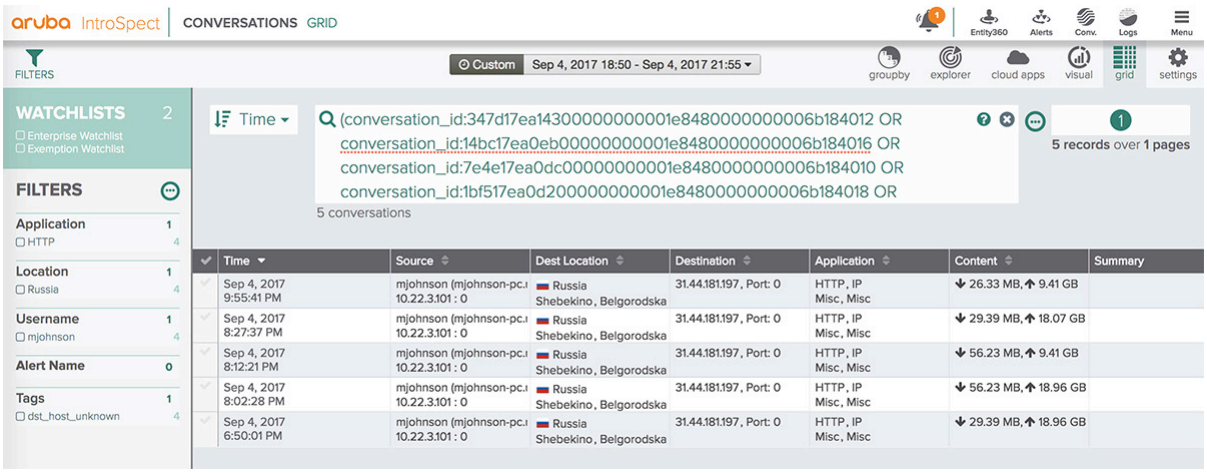

Figure 4: IntroSpect makes it easy to run complex queries.

The analyst can drill down into each of the entries for additional detail, with full context forensics.

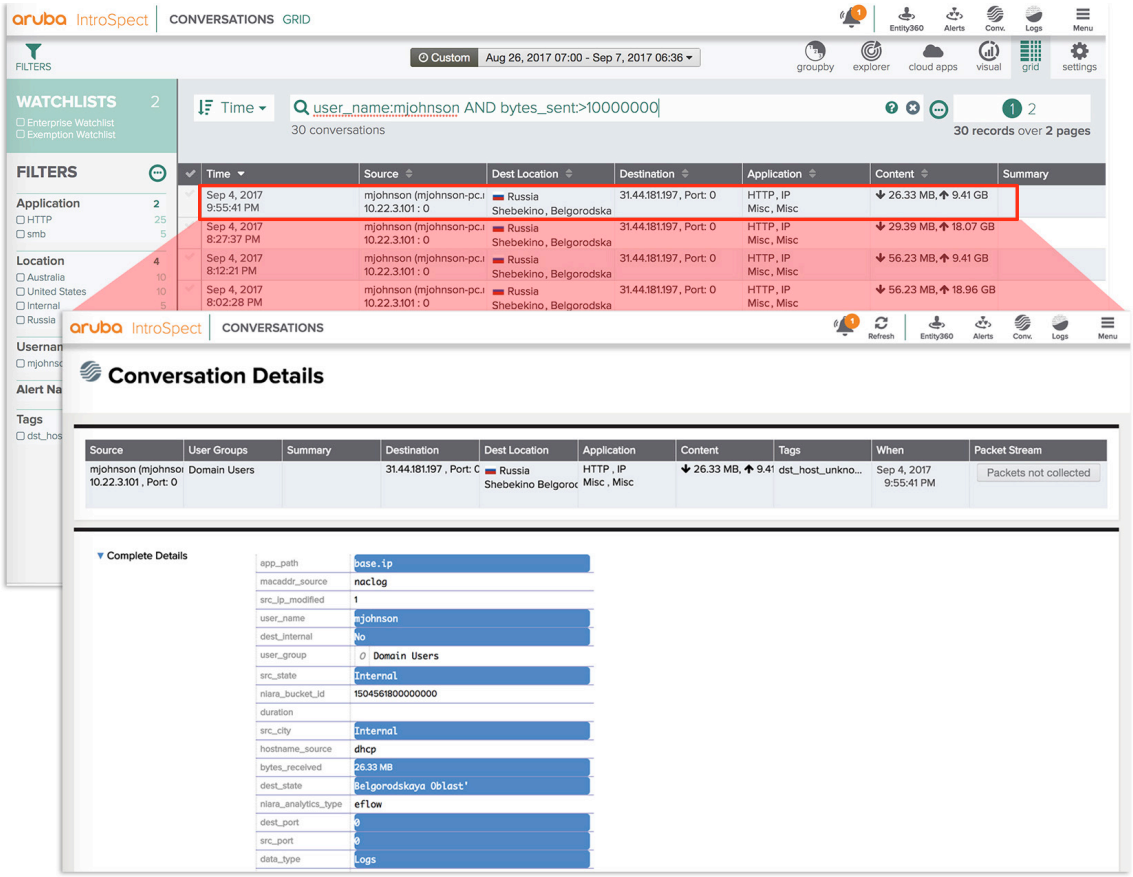

Figure 5: Integrated forensics makes it for analysts to get the full context needed for investigations from within IntroSpect. Shown above are the network conversation details for the highlighted download that exceeded 10MB.

IN SUMMARY

To detect insider threats, IntroSpect can ingest the following data sources:

Required data sources:

- Active Directory (AD) logs
- Firewall logs or network traffic for internal activity to servers/datacenter
- Ingress/egress firewall logs or web proxy logs or network traffic

Optional data sources:

- DNS Logs
- VPN logs
- Endpoint logs
- Internal Network flows
- DLP logs

BENEFITS OF USING INTROSPECT

1. Build high fidelity entity risk profiles by applying supervised and unsupervised machine learning that go well beyond statistical techniques.
2. Maximize your chances of detecting insider activity – both negligent and malicious variety – by applying machine learning techniques that go well beyond statistical techniques and also beyond the just a few logs.
3. Don't just shrink the time to detect; Shrink the time to detect and investigate with analytics that is combined with "user" context forensics that make it easy to investigate any incident or a user for extended periods of time.

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

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

www.arubanetworks.com