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.

Figure 1: IntroSpect Entity360 can be easily accessed from ArcSight
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

Figure 2: IntroSpect Entity360 can be easily accessed from Splunk

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.

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/