aruba
a Hewlett Packard Enterprise company

UEBA USE CASE

COMPROMISED USER AND HOST DETECTION USING BEHAVIORAL ANALYTICS

EXECUTIVE SUMMARY

Attacks involving compromised users and hosts are notoriously difficult to detect because cyber criminals can evade perimeter defenses by using legitimate credentials to access corporate resources. Aruba IntroSpect's User and Entity Behavior Analytics (UEBA) automates the detection of these attacks with analytics-driven visibility. Advanced techniques, including supervised and unsupervised machine learning, are applied to data from the network and security infrastructure (e.g., packets, flows, logs, alerts). This information is then used to create Entity360 risk profiles for all users and hosts where seemingly disparate security events are observed and correlated over time. By measuring the changes and/or the anomalies associated with each entity, IntroSpect surfaces advanced attacks, which might appear to be a legitimate user's activity, but in reality more likely an attacker masquerading as a legitimate employee. In addition, these anomalies can only be detected by intelligently correlating "weak" signals over long periods of time. IntroSpect also provides analysts with one-click access to integrated layered forensic evidence, which can go back months or more, as context is often needed to investigate attacks. By combining machine learning with layered forensics, IntroSpect delivers a differentiated analytics solution that automates attack detection and incident investigation without rules, configuration and signatures.

OVERVIEW

For cyber criminals, credentials that provide access to corporate networks are invaluable. Phishing scams, social engineering and malware are just a few of the popular techniques by which these criminals acquire employee corporate credentials. These techniques are effective – Verizon reports that over 80% of advanced attacks are due to external actors.[1] Once attackers have these credentials, they can pose as users with legitimate access, scour internal networks for valuable data (e.g., emails, intellectual property, financial information, etc.) and steal it with impunity over extended periods of time without raising any alarms. In fact, over 75% of attacks take weeks or more to be detected.[2] Traditional rule based systems such as IDS/IPS or SIEM are good at detecting the "known bad" attacks, but are ill-equipped to detect such credential-based attacks that fall in the realm of the "unknown bad".

Credential-based attacks are typically multi-stage, involving many of the activities shown in the first row of Figure 1.

Accurately detecting such attacks is challenging because raising an alert based on detection of only one activity will generate excessive false positives. What's needed to learn what may truly be happening to the entity is a macro profile that provides visibility across different attack stages. Detecting as many of these stages as possible will best position your organization to thwart attacks. However, this is challenging because the data needed (shown in the 2nd row of Figure 1) is available from differing sources in a multitude of forms.

ATTACK STAGE	Initial Infection	Command & Control	Internal Recon	Privilege Escalation	Lateral Movement	Abnormal Access	Data Exfiltration
DATA SOURCE	Email activity Web activity	DNS records Network activity	Network activity	AD logs Network activity	Network activity	Network activity	Endpoint logs Network activity

Figure 1: Diagram showing the stages between infection and data loss as well as the data sources needed for analytics to accurately detect the attack stage.

DRAWBACKS WITH COMMON APPROACHES

In-market solutions use a variety of approaches in an attempt to detect advanced attacks. Most suffer from significant drawbacks.

Statistical techniques

Many solutions use statistical techniques – like the first time a user accessed a server or a sudden spike in the amount of data uploaded or downloaded by a user – to detect advanced attacks. However, this is not sufficient to yield meaningful results. Consider a hypothetical user "Bob" who atypically downloaded a large amount of sensitive data from an internal server. The abnormality of this action alone may not warrant an alert, as Bob may have been preparing for an important meeting and simply needed access to this information. User behavior is extremely variable, and analysis using statistical techniques alone yields poor results – generating excessive false positives that add to the alert white noise problem faced by most organizations.

Limited data sources

Some solutions claim to offer meaningful results by only looking at limited data sources like Active Directory or VPN logs, then adding 3rd party alerts and business context. This approach is ineffective against many modern attacks and threats. For example, once an attacker gains access to an employee's device, many of the attacker's actions would not get logged by the domain controller. As a result, Active Directory logs will have no record of the attacker's activities inside the network. The attack involved multiple stages, many of which could have been detected by analyzing email traffic, internal activity and network activity. Analysis of Active Directory logs alone was insufficient to detect this attack.

Data-driven approach

Solutions that are bolted on to a log management/SIEM will attempt to derive insights from the data already logged in SIEM alone. While this sounds easy to deploy and appears to be a great idea, this approach is a failing value proposition. It often ignores extremely useful sources of security insights already present in an organization's network (e.g., high volume log sources such as DNS records, network activity information) that is perhaps not being collected and stored due to cost.

THE INTROSPECT DIFFERENCE

Behavioral analytics, or UEBA (user and entity behavior analytics) is an approach that has shown promise in accurately detecting advanced attacks. However, it's tough to differentiate between solutions as all vendors make similar-sounding claims. Double-clicking into their technology reveals how dramatically dissimilar they really are, which makes a huge difference in what they can actually detect.

IntroSpect's approach is fundamentally different. As a result of several critical design choices, IntroSpect's user and entity behavior analytics best positions organization against these attacks and ensures your security analysts are focusing on the threats that matter.

Multi-dimensional analytics

Unlike UBA solutions that use only statistical techniques, IntroSpect combines unsupervised, supervised, and adaptive machine learning with statistical techniques to build entity risk profiles that more reliably link anomalies with malicious intent. IntroSpect applies all analytics in parallel, on all data (no sub-sampling like many UBA solutions do), and for all entities (i.e., users, hosts, devices). IntroSpect's machine learning modules use global behavioral patterns, entity specific patterns around historical normal behavior and peer-based pattern analysis to determine the risk score of an entity. As a result, IntroSpect detects a broader range of anomalies than other UBA solutions and with greater accuracy.

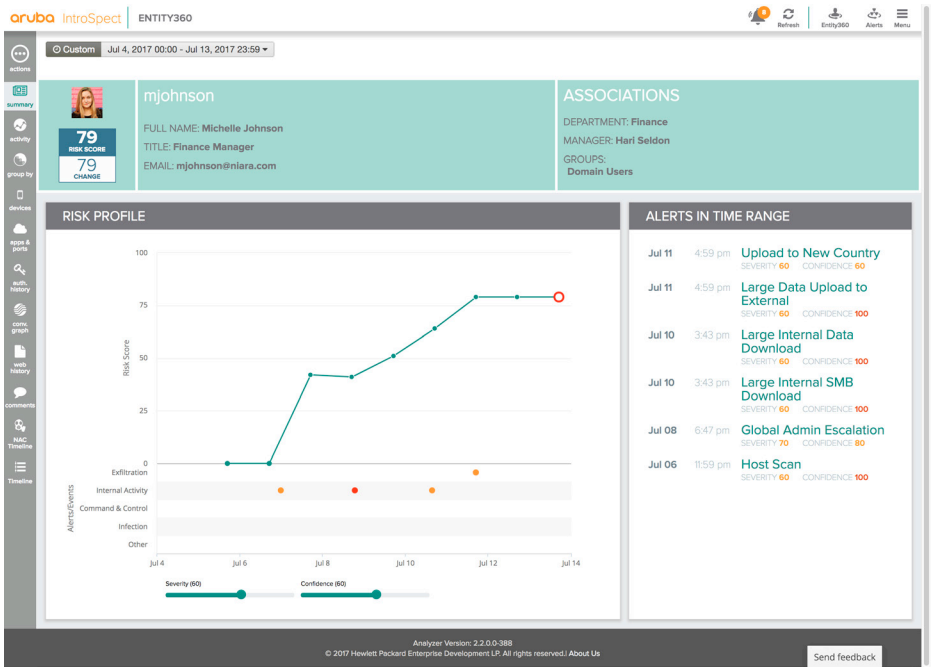

Figure 2: Multi-dimensional analytics enable creation of high-fidelity entity risk profiles and shrink the time to detect attacks.

Adaptive learning enables analysts to label warnings as either true anomalies or authorized exceptions and continuously incorporates that feedback into IntroSpect's machine learning models. Superior detection results, as unsupervised models are transformed into context-driven supervised ones.

IntroSpect's behavioral analytics framework is the industry's most flexible. It can ingest any data source, including customer-specific ones, and determine the best machine-learning model to apply based on analyst-chosen feature sets. Analysts can also extend IntroSpect to alert on their own custom analytics use cases.

Diverse data sources

Different from other behavioral analytics, IntroSpect uses diverse data sources out of the box (i.e., packets, flows, logs, files, 3rd-party alerts and threat feeds), finding more anomalies and more importantly, chaining them together to deliver accurate insights about entities. In addition, IntroSpect doesn't use simplistic statistical techniques to detect anomalies on a single dimension such as authentication (e.g., alerting when a user's login rate exceeds an arbitrarily chosen number of deviations from the norm). This contributes to alert noise. Instead, IntroSpect applies machine learning on all data sources across a range of dimensions (i.e., authentication, remote access, peer to peer activity, internal high value server access, internet usage, DNS activity, cloud application usage) to paint a composite picture of every user and host.

Disparate events such as command and control activity, suspicious modification of account privileges, communication to an external website, unusual access to internal servers, large file transfers, etc., while individually not rising to the level of an alert, are statefully correlated for a user or host over an extended period of time – hours or days or weeks – and contribute to a composite risk score. A high-risk score may constitute a sign of a user or host that is compromised and under attack.

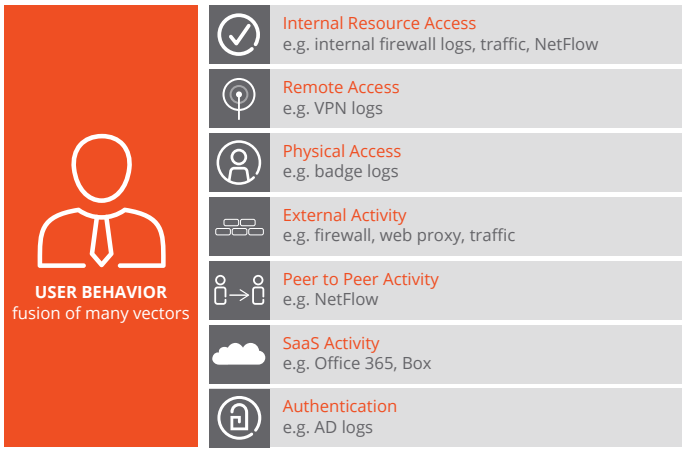

Figure 3: IntroSpect leverages a comprehensive set of data sources to build a risk profile for each entity.

This results in higher fidelity entity risk profiles, enabling more accurate attack detection with fewer false positives and false negatives. IntroSpect results are more credible, as it can analyze all data sources, including packet data. For example, to find command and control (C&C) activity, many UBA solutions analyze only DNS logs for signs of algorithmically generated activity, but that alone yields many false positives. IntroSpect analyzes DNS logs and correlates the results with the return responses seen in DNS traffic, filtering out false positives and surfacing only anomalies that analysts can confidently assume are in fact real.

To detect compromised users/hosts, IntroSpect can ingest the following data sources for analysis

Required data sources

- Active Directory (AD) logs
- Ingress/egress firewall logs or web proxy logs or network traffic

Optional data sources

- DNS Logs
- VPN logs
- Firewall logs or network traffic for internal activity to servers/datacenter
- Endpoint logs
- Internal network flows
- DLP logs
- FireEye or WildFire alerts

INTROSPECT USES DIVERSE DATA SOURCES IN A VARIETY OF DETECTION VECTORS IN ORDER TO DETECT THE DIFFERENT ATTACK STAGES.

Type	Examples	Detection Vectors
Network activity	Firewall logs IDS/IPS logs Web Proxy logs Email logs Network traffic Network flows	Lateral movement Abnormal resource access Browser exploits Malware activity Suspicious file downloads Command and control activity Beaconing
Remote access activity	VPN logs	Credential theft, password sharing
Identity	AD logs DHCP logs	Credential violations Account takeover Privilege escalations
Infrastructure	DNS logs	Command and control activity Tunneling Exfiltration
3rd party alerts	FireEye alerts WildFire alerts	Incorporate alerts into user risk profiles
Threat intelligence feeds	Commercial & STIX feeds	Perform historical impact assessment
Endpoint logs	DLP logs File integrity monitoring logs	Suspicious file activity USB, cloud based file exfiltration

Integrated forensics

It's not sufficient to produce an alert, especially one driven by machine learning, which is probabilistic in nature. Analysts can't be expected to investigate and close out alerts generated by UEBA solutions, however good, unless they have confidence in the solution's results. IntroSpect is the only UEBA solution that integrates analytics with high-fidelity forensics. This provides analysts with detailed supporting evidence, potentially going back months. Forensics help analysts determine exactly what happened, when it happened, who else was affected, making it very easy for them to work their way from detection to investigation to closure of alerts.

The figure below is an example of what IntroSpect makes available to aid investigations. In this situation, IntroSpect has detected a suspicious file download. Analysts can see details about the alerts raised by IntroSpect's multi-dimensional analytics. Analysts also get access to all the forensic information needed to investigate the alert. In addition to the alert details, the figure also shows great detail about the network interactions associated with the download of this suspicious file.

DETECTING COMPROMISED USERS AND HOSTS

With IntroSpect, analysts get analytics-driven visibility into every stage of the attack chain. Multi-dimensional analytics, diverse data sources and integrated forensics ensure that attackers using compromised users and hosts have no place to hide within the organization. Detection vectors supported by Aruba IntroSpect include:

A. Advanced low and slow multi-stage attacks
B. Privileged account abuse (i.e., inappropriate usage of access permissions)
C. Abnormal resource access (i.e., abuse of access permissions to download internal sensitive information
D. Privilege escalation (i.e., transformation of identity and access credentials)
E. Unusual internal activity (i.e., accessing external domains, remotely accessing high privileged assets, and unusual login duration, time or location)
F. Credential compromise (i.e., stealthy takeover of accounts for malicious purposes)
G. Password sharing (i.e., inappropriate sharing of passwords by users)
H. Account Takeover (ATO) (i.e., compromise of privileged and regular accounts by external, malicious entities)

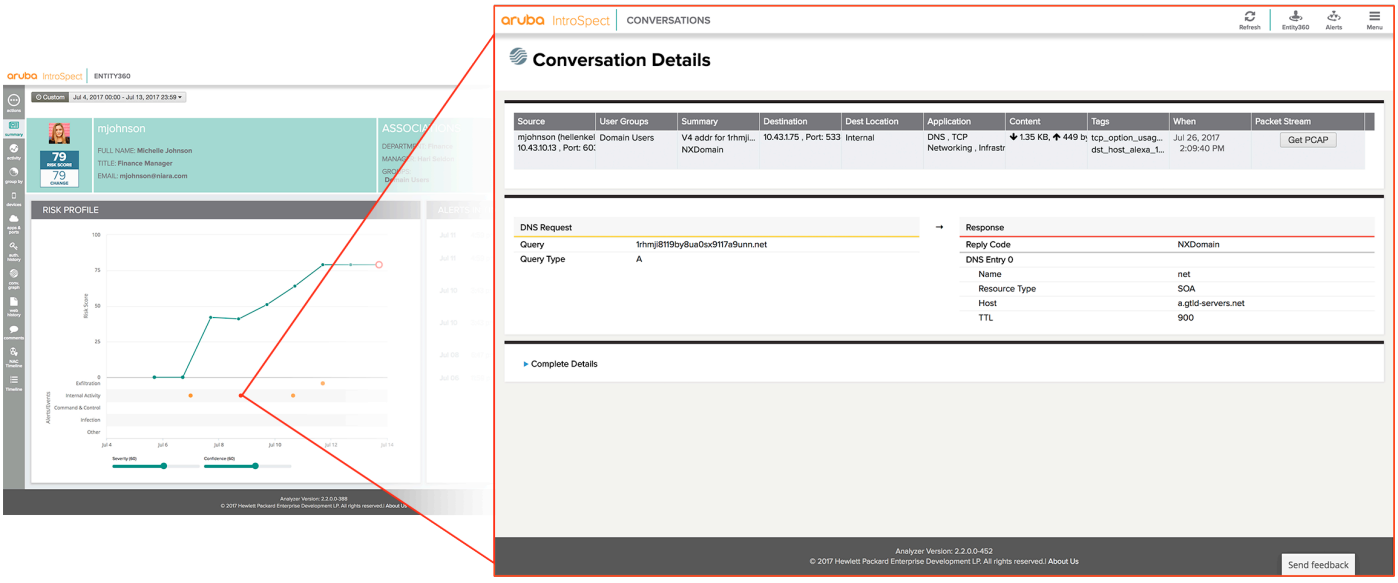

Figure 4: IntroSpect provides multiple layers of easy-to-access forensics that help shrink the time for incident investigations.

I. Internal reconnaissance (i.e., probes to identify and exploit vulnerable assets)
J. Lateral movement (i.e., navigation of malware or attackers within a network)
K. Command and Control (C&C) activity (i.e., communication activity with C&C infrastructure such as abnormal DNS or beaconing)
L. Browser exploits and malware activity (i.e., infection discovery of polymorphic attacks and advanced persistent threats (APTs) via email or web)
M. Data exfiltration (i.e., the act of stealing private, confidential and sensitive data within an organization by malware or an attacker)
N. Cloud application-based exfiltration (i.e., using cloud applications to exfiltrate data)

To get a perspective into the power of Aruba IntroSpect, consider the following example involving a hypothetical user "Michelle" who has become compromised and is unknowingly being used in an attack.

Michelle downloaded a suspicious file at home and got infected. Now the attacker has gained access to her machine. Days later at work, suspicious C&C activity is detected originating from Michelle's laptop. A week later, the attacker uses Michelle's credentials to escalate her privileges. A few days after that, the attacker uses her improved privileges and credentials to download a treasure trove of sensitive information. A few days after that the attacker manages to exfiltrate the data to a server in Belize.

The diagram above shows the various detection vectors used by IntroSpect's multi-dimensional analytics to automatically detect the attack. The diagram also shows, the data used in the analytics and a real-time risk score that reflects the increasing risk that Michelle poses to the organization as the attack progresses. In this example, IntroSpect leveraged data from existing repositories (e.g., Active Directory logs from a SIEM) and tapped into additional ones that were not in any existing repositories (e.g., packets, flows and high-volume logs). Solutions that rely on a single behavioral analytics model based solely on a few logs would not have been able to provide the visibility into the attack that IntroSpect made possible.

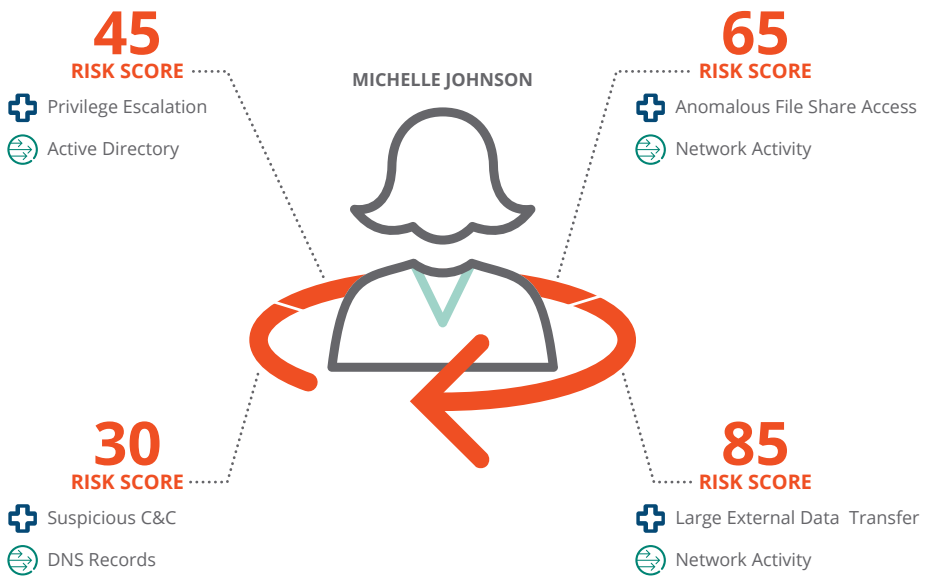

Figure 5: Compromised User Detection with IntroSpect

BENEFITS OF USING ARUBA INTROSPECT

Traditional systems such as IDS/IPS or SIEM are ill equipped to detect credential-based advanced attacks. While behavioral analytics shows promise, not all UEBA solutions are created equal as solution architecture has a tremendous impact on what is actually detected. IntroSpect's choice of combining multi-dimensional analytics, diverse data sources, and integrated forensics provide analysts with benefits unachievable via other UEBA solutions.

1. Detect attacks faster. Supervised, unsupervised and adaptive learning techniques automatically generate high-fidelity entity risk profiles, well beyond what's possible with statistical techniques alone and shrink the time to detect attacks.
2. Comprehensive visibility: IntroSpect can analyze diverse data sources, finding more anomalies and providing a more complete view into criminal activity and risk behaviors within your organization.
3. Shrink investigation time. Analytics integrated with forensics amplifies your analysts' investigative capabilities and shortens the time needed to resolve incident investigations. Both are important given the acute shortage of security professionals.

To learn more about Aruba IntroSpect and User and Entity Behavior Analytics, go to www.arubanetworks.com/IntroSpect

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.

[1] 2017 Data Breach Investigations Report, Verizon
[2] 2017 Data Breach Investigation Report, Verizon
[3] M-Trends 2016: Special Report, Mandiant – A FireEye Company, February 2016

aruba
a Hewlett Packard Enterprise company

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

www.arubanetworks.com