RSA

RSA NETWITNESS® UEBA USE CASES

POWERFUL DETECTION FOR USER-BASED THREATS

RSA NetWitness UEBA is a purpose-built, big-data driven, user and entity behavior analytics solution integrated as a central part of the RSA NetWitness Platform. By leveraging unsupervised statistical anomaly detection and machine learning, RSA NetWitness UEBA provides comprehensive, behavior-based detection of unknown threats to address a wide range of use cases. RSA NetWitness UEBA augments your existing security team to provide rapid detection and actionable insights at every step of the attack lifecycle.

When evaluating user and entity behavior analytics (UEBA) solutions, look for the following critical features and capabilities:

- Fully-automated and continuous threat detection and monitoring
- Visibility into the full attack lifecycle leveraging data collection, detection, investigation and response
- Natural language indicators aligned with the MITRE ATT&CK™ framework
- Unsupervised machine learning with a zero touch, turn-key data science model that requires no tuning
- An endpoint agent that's core to the platform and pairs log collection with endpoint detection and response

CORE CAPABILITIES OF ENTERPRISE-GRADE UEBA

NATIVE DATA COLLECTION

A significant challenge for many SOC teams is managing the collection, storage and analysis of all the logs produced in different formats by their company's vast portfolios of on-premises and cloud-based systems. RSA NetWitness UEBA addresses this challenge by collecting raw log data from these systems, dynamically parsing activities generated by people and processes from a wide range of sources, and interpreting relevant security information from these data sources.

FIND OUT MORE

Visit RSA.com/DoMore or Schedule a demo

UNIFIED METADATA TAXONOMY

For a UEBA solution to perform optimally, the log, network traffic and endpoint data feeding it should be parsed, normalized and transformed at capture time into a unified, consistent metadata taxonomy. Because RSA NetWitness UEBA is a central component of the RSA NetWitness Platform evolved SIEM, this happens automatically.

DETECTION AT MACHINE-LEARNING SPEED

Too often, threat indicators from point security solutions can't reliably or consistently be used to identify an attack because the majority of time these activities, in isolation, are not part of an attack and alerting on them would quickly drown analysts in a sea of dead-end alerts. RSA NetWitness UEBA yields much more focused, actionable alerts than point security solutions because it looks at patterns of activity and behavior over time, uses machine learning to identify deviations in baseline behaviors and learns from past alerts marked as false positives.

WHY HAS UEBA BECOME A CORE SECURITY REQUIREMENT?

- 28% of reported breaches stem from internal actors; UEBA makes it easier to detect these kinds of threats
- Top internal actors causing reported breaches are system admins and end-users
- 68% of breaches took two months or longer to discover; UEBA helps security teams detect threats faster
- Top actions of reported breaches are stolen credentials and privilege abuse/misuse; activities UEBA is designed to alert on

Verizon Data Breach Investigations Report 2018, Verizon.

RSA

6 USE CASES RSA NETWITNESS UEBA IS DESIGNED TO DETECT

ABNORMAL ACTIONS/ CHANGES

If an attacker gains privileged access to an Active Directory (AD) domain or a domain controller, the attacker can leverage that access to control or even destroy the entire AD forest. If he compromises even a single domain controller, any modifications to that controller can be replicated to every other system. RSA NetWitness UEBA helps analysts detect these types of scenarios by identifying spikes in the volume of user actions against an AD domain that may indicate an account is compromised and/or being used to corrupt or destroy critical directory data.

ABNORMAL PRIVILEGED USER ACCESS

RSA NetWitness UEBA helps you identify when a privileged user may pose an insider threat. For instance, if a help desk technician begins straying from their "normal" routines and established security policies, and starts configuring new users' passwords to never expire, RSA NetWitness UEBA would pick up on that.

SNOOPING

Snooping refers to unauthorized access to another person's or company's data. This could entail an internal user or external attacker attempting to browse servers and folder locations they're not entitled to access, typically in an effort to locate and obtain valuable corporate information. Sophisticated snooping leverages custom programs that remotely monitor activity on a computer or perform automated file discovery.

RSA NetWitness UEBA can detect snooping in a number of ways: It captures users' failed and successful attempts to access data they don't have legitimate access to. When the solution identifies an abnormally high number of successful and unsuccessful file access attempts in a short timeframe to a new location, it triggers an alert.

BRUTE FORCE AUTHENTICATION

Sophisticated UEBA solutions can distinguish a true brute-force attack from a benign authentication failure by looking at failed authentications in the context of other abnormal user activity. RSA NetWitness UEBA only triggers alerts when it detects other suspicious behavior patterns alongside repeated authentication failures. This helps to eliminate false-positives associated with faulty network configurations or users' finger-fumbling their passwords.

MACHINE-OPERATED ACTIVITIES

RSA NetWitness UEBA can detect when a malicious program is trying to access restricted corporate resources using compromised credentials. User profiling may reveal signs of a brute force attack, while entity profiling may pick up on a significant spike in suspicious entity behavior, such as an excessive number of activities to hundreds of accounts from a single device or IP address, or a massive amount of file renames across multiple computers that are all perpetrated from a single machine where the malicious program is installed.

ELEVATED PRIVILEGES

Attackers will try to leverage the organization's regular users, more often the easier target, than grant themselves with elevated privileges for further network exploits. Closely monitoring privileged user activities, access granted, sensitive groups, and more is critical to combatting compromised credentials. But because privileged users don't always follow a set pattern of "normal" behavior, false positives are inevitable. Therefore, identifying, collecting and parsing an accumulation of indicators is critical to pinpoint those that are malicious.

Therefore, for the case of elevated privileges with an actor logging on from an atypical location after multiple failed authentication attempts, followed by creating new user accounts with elevated privileges, will result in high risk within top alerts list.

Before you add another point solution (in this case UEBA) to your security stack, ask yourself if it will truly add value or just create more noise. The benefit of RSA NetWitness UEBA is that it detects critical user-based anomalies alongside traditional threats, all within a single platform.