SOLUTION BRIEF

Enhanced Attack Detection and Accelerated Investigations with UEBA

In an era of headline-making attacks, enterprise security teams need detection and response solutions that complement and enhance their existing security infrastructure. Niara's machine learning-based user and entity behavior analytics (UEBA) are designed for early attack detection and accelerated incident investigation by associating high-risk activities to a user. The solution delivers precision attack alerts and supporting forensic data directly to the McAfee® Enterprise Security Manager console, enabling security teams to detect and investigate malicious, compromised, or negligent users so they can be remediated within the McAfee Enterprise Security Manager workflow before they damage the operations or reputation of the organization.

McAfee Compatible Solution

- Niara Behavorial Analytics with McAfee Enterprise Security Manager

The Business Problem

Enterprises have tuned their security operations centers (SOCs) to be the focal point of attack detection and incident investigation and response. However, attacks are now targeted based on specific knowledge of an organization, as well as a keen understanding of typical defenses. Given this advanced threat environment, how does the security team leverage their investment in SOC training, technology, and processes while introducing new types of detection and decision-making support to meet these new challenges?

McAfee and Niara Joint Solution

Increasingly, enterprises are turning to machine learning-based attack detection provided by products like UEBA to supplement their defenses. SIEM and UEBA are natural companions. Niara has been designed to deliver maximum value to the SOC by accessing McAfee® Enterprise Security Manager's comprehensive data aggregation to feed its analytics and to return value back to McAfee Enterprise Security Manager by providing a second dimension of analytics that can surface hard-to-find attacks on the inside. This reduces the number of alerts an analyst must process while providing instant availability for the forensic information needed to shrink investigation and response from hours and days to minutes.

Machine Learning Models for Detecting Attacks on the Inside

Attacks on the inside can be caused by compromised users who may have clicked on email-borne malware and unleashed ransomware on the organization, negligent users who share credentials, and malicious users who see an opportunity to financially benefit from extracted patient records or credit cards. Niara's more than 100 machine learning models build baselines of "normal" behavior for users, hosts, applications, and partners based on each entity's activity, as well as within an entity's peer group. Deviations from the norm are captured, tracked over time, and put into context with other security-relevant events so that Niara can raise accurate and highly relevant alerts that the security team can respond to before damage is done.

Packets to Logs to Alerts: Full Visibility and Easy McAfee Enterprise Security Manager Integration

Unlike solutions reliant on one type of data, Niara provides complete visibility across logs, flows, packets, files, alerts, and external threat intelligence to feed supervised and unsupervised algorithms designed to identify telltale attack signals that evade other security products. Niara alerts and forensic information are integrated with the McAfee Enterprise Security Manager SOC and incident-response workflow so that the entire security team can leverage Niara's attack discovery and comprehensive decision support.

Entity360: Instant Investigation and Response with Powerful Threat Hunting

Niara Entity360 security dossiers contain risk profiles for users, servers, and applications that score and summarize small changes in behavior and present alerts by stages in the kill chain (infection, spread, command and control, and more) ranked by potential impact on the organization. Via Entity360, the analyst also has one-click access to forensics data that would otherwise take hours or days of searching through months and years of IT activity, down to the packet level. Proactive threat hunting is easily accomplished with a powerful query interface, without requiring searching and summarizing across isolated data stores.

About Niara

Niara's behavioral analytics platform automates the detection of attacks and risky behaviors inside an organization and dramatically reduces the time and skill needed to investigate and respond to security events. Unlike other UEBA solutions that only see a part of the IT ecosystem, Niara applies machine learning algorithms to data from the network, logs, and alerts to detect compromised users, entities, and negligent or malicious insiders, reduces the time for incident investigation and response, and speeds threat hunting efforts by focusing security teams on the threats that matter.

About McAfee Enterprise Security Manager

McAfee Enterprise Security Manager—the foundation of the security information and event management (SIEM) solution family from McAfee—delivers the performance, actionable intelligence, and real-time situational awareness at the speed and scale required for security organizations to identify, understand, and respond to stealthy threats, while the embedded compliance framework simplifies compliance.

McAfee™
Together is power.

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com