MICRO FOCUS

Data Sheet
Security

ArcSight User Behavior Analytics

Micro Focus® Security ArcSight User Behavior Analytics (UBA) enables security analysts to minimize the risk and impact of cyberattacks in real time.

Product Highlights

Instead of solely focusing on events and log data, ArcSight UBA detects unknown threats through purpose-built security analytics by creating a baseline of normal user and entity behavior and identifying anomalies as they occur. By aggregating activities and multiple indicators of compromise, ArcSight UBA delivers insight into the highest risk users and entities—even when credentials are legitimate.

As the security landscape expands and evolves, enterprise security professionals continue to be challenged by threats that are more severe and complex. Insider threats, in particular, are a growing concern. Because it is difficult to detect malicious users or entities that have legitimate credentials, rogue or compromised accounts can install malware that can go undetected for months as it steals sensitive information and devastates critical assets. To effectively reduce breach impact, security teams must detect, investigate, and respond to those threats with speed and accuracy. However, enterprises today are increasingly finding that traditional security solutions are no longer adequate for combatting advanced persistent threats.

While rule-based tools such as security information and event management (SIEM) platforms still serve a purpose, they often fail against modern threats. According to a recent Verizon security study, 82 percent of all breaches investigated showed that evidence of the attacker activity was available and contained in security log files.1 Traditional tools alert enterprises to suspicious activities, but by the time security teams are made aware of the breach, investigate the event, assess its validity, and respond with a context-relevant solution, the adversaries have inflicted serious damage. Even more, security professionals must comb through these vast quantities of log data all while meeting changing regulatory requirements and controlling costs.

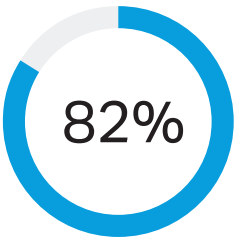

Figure 1. 82 percent of all breaches investigated showed that evidence of the attacker activity was available and contained in security log files.

ArcSight UBA enables detection of advanced user- and entity-based threats, and when used in conjunction with the installation of Micro Focus Security ArcSight SIEM, can leverage the same operational teams, data feeds, and

Quick View

- Delivers enhanced visibility into attacks, with real-time alerts on suspicious activities and behaviors
- Displays an intuitive workbench that delivers immediate insight into security risks, streamlines investigations, and increases productivity
- Prioritizes the most suspicious and abnormal activities across users and entities to present risk-ranked threats
- Detects cyberattacks and insider threats, even if legitimate credentials are being used, thereby spotting adversaries faster and before significant damage occurs

incident response processes already in place. This in turn drives investigation efficiency and operational savings.

Key Benefits

See Fig. 2

- Delivers enhanced visibility into attacks with real-time alerts on suspicious user and entity activities and behaviors
- Displays an intuitive workbench that delivers immediate insight into security risks, streamlines investigations, and increases productivity
- Prioritizes the most suspicious and abnormal activities across users and entities to present risk-ranked threats
- Detects cyberattacks and insider threats, even if legitimate credentials are being used, thereby spotting adversaries faster and before significant damage occurs
- Provides hundreds of supported use cases to target intelligence activities to various threat situations

Key Features

Better Advanced Threat Detection Through User Behavior and Entity Analysis

By coupling the latest advances in machine-learning and advanced anomaly detection techniques and algorithms, ArcSight UBA rapidly detects known and unknown threats—without solely relying on signatures, policies, or rules. ArcSight UBA performs peer group analysis to identify unusual behaviors and unprecedented events. By comparing groups of users and entities, ArcSight UBA can compare behaviors and spot activities that are out of baselines, even if they occur only once. By correlating anomalous user and entity behaviors with context-rich intelligence, ArcSight UBA can reduce false positives, enabling security teams to concentrate on real, high-risk threats to the organization—including network-related scenarios such as malware beaconing detection, and abnormal volumes and counts of traffic to suspicious sites. ArcSight UBA can help organizations identify high-risk data exfiltration, misuse of privileged and service accounts, and detection of advanced, persistent threats.

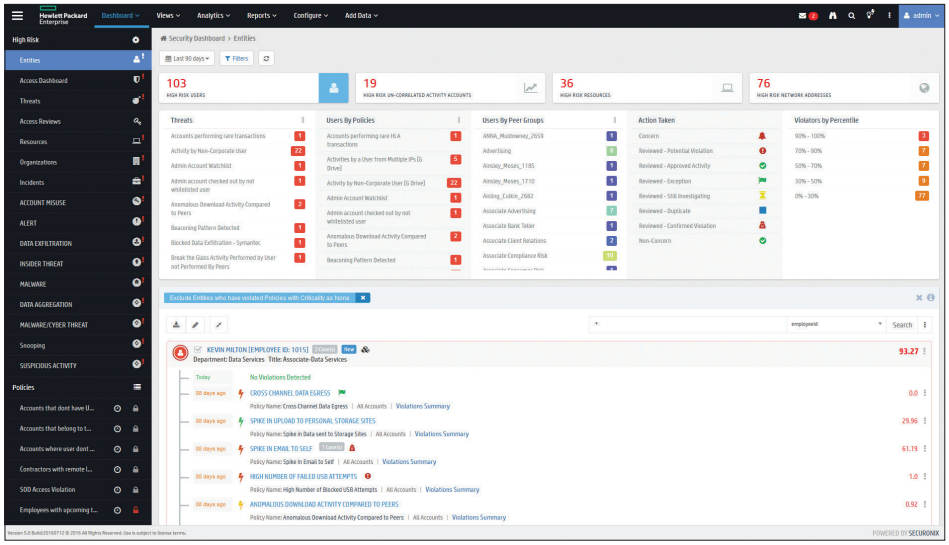

Figure 2. ArcSight UBA enables detection of advanced user- and entity-based threats in real time.

More Proactive Adversary Hunting to Reduce Breach Impact

By combining user identity management and access information with database, file, and user-centric activity, ArcSight UBA can actively monitor the actions of privileged users for risky or unusual activity, lowering the risk and impact of cyberattacks by detecting unusual behavior sooner. It includes advanced and targeted attack identification, identity correlation, insider threat identification and investigation, and privileged account misuse. This information is visualized in a useful way for the organization to find the bad guys faster.

Faster, More Accurate Investigation and Decision-Making

The streamlined user interface enables more efficient investigation and effective decision-making. A multi-entity investigation workbench enables distillation of massive amounts of data collected from disparate sources and prioritization of security information in a business-relevant context. Dashboards, violation timelines, point-and-click filtering, and search capabilities enable analysts to immediately refine data and logs down to the most relevant information, such as host name, IP address, and risk scores, and identify real threats. Risk boosting and dashboard actions ensure cyber defense centers maintain a human element.

Greater Situational Awareness to Respond to Threats More Intelligently

ArcSight UBA Threat Library gives organizations access to hundreds of sophisticated use cases that can be configured to meet individual enterprise needs. ArcSight UBA Threat Library enables cyber defense centers to target their activities to various threat situations, including user and entity behavior analytics,

data loss prevention, enterprise and cloud applications, and cyber threats against devices. Hundreds of supported use cases translate to more accurate threat identification and not just anomaly identification or false positives.

Efficient and Effective Event Resolution

Achieve faster event resolution with purpose-built security analytics and intelligence that mines, enriches, and transforms your SIEM information to produce actionable intelligence on known and unknown threats against the entire IT environment by providing detailed visibility into users and entities, mitigating threats before they occur.

Move from IP Address to User Mapping

Many logs for important systems such as proxies do not record user behavior information, but instead only record IP addresses. Investigating user activity on those systems requires knowing which IP address the user had at a given time. UBA solves this problem by using identity correlation, a process that correlates data between addressing systems to attribute unauthenticated activity to individual users.

Learn More At
www.microfocus.com/arcsightesm

Contact us at:
www.microfocus.com