Splunk® User Behavior Analytics
Detect Cyber Attacks and Insider Threats – Powered by Caspida

**Key Use Cases**

- Cyber Attack Detection
- Insider Threats
- On-line Account Takeovers

**Data Sources**

- **Identity and Privileged User Activity**: entity ID and authentication events (Active Directory, single sign-on, VPN, etc.), and privileged account management applications
- **Activity**: HTTP transactions, intra-network activities (firewall, web gateway, VMs, proxy, DPL, etc.)
- **SIEM**: existing SIEM and log management products (HP/ArcSight, LogRhythm, IBM/QRadar, etc.)
- **Hadoop Ecosystem**: existing Hadoop data repositories (Cloudera, HortonWorks, etc.)
- **Malware Detection**: existing sandbox or dynamic analysis products (FireEye, Palo Alto Wildfire, etc.)
- **External Threat Feeds**: external threat feeds (FS-ISAC, Google CIF, etc.)
- **Cloud, Mobile**: mobile device events, remote application logs, AWS CloudTrail, Box, etc.
- **Endpoint**: application and security logs from laptops, desktops and servers
- **Custom Apps**: live event streaming via JavaScript, Java, REST, Syslog

**New Layer of Cyber Defense**

Splunk User Behavior Analytics helps organizations find known, unknown and hidden threats using machine learning, behavior baseline, peer group analytics, and advanced correlation to find lurking APTs, malware infections, and insider threats. It addresses security analysts and hunter workflows, requires minimal administration, and integrates with existing infrastructure to locate hidden threats.

**Behavior-Based Threat Detection**

- Multi-entity behavior profiling and peer group analytics – users, devices, service accounts and applications
- Threat and anomaly detection with sophisticated kill-chain visualization
- Machine learning – no signatures, no human analysis

**HIGHLIGHTS**

- Improve detection of known, unknown and hidden cyber attacks and insider threats.
- Increase security analyst effectiveness by prioritizing threats and reduced false positives.
- Easy to use for SOC analysts and incident responders.
Architecture

Splunk User Behavior Analytics is built as a platform that includes Hadoop ecosystem for scalable, cost-efficient and open data persistence. The platform is designed for real-time and large-scale event analysis, includes time-series databases and graph databases for processing and representing security connections within the network. The platform provides RESTful APIs for integrating with third-party products to ingest data automatically, as well as to drive action for remediation and prevention. The product is proven to scale over hundreds of TBs and billions of events.

Deployment Options

- On-premise VM or software
- WS and vCloud Air public cloud

Why Behavioral Analytics from Splunk?

Machine learning, statistical profiling and other anomaly detection techniques need a foundation. A massively scalable and readily available data platform is required to support advanced analytics, one that provides users accessibility, quality and data coverage from a range of security and enterprise systems. The entire lifecycle of security operations: prevention, detection, response, mitigation, to the ongoing feedback loop, must be unified by continuous monitoring and advanced analytics to provide context-aware intelligence. The threat detection capabilities in Behavioral Analytics extend the search/pattern/expression (rule) based approaches currently in Splunk and Splunk Enterprise Security for detecting threats.

Splunk can provide the data platform as well as the security analytics capabilities needed to allow organizations to monitor, alert, analyze, investigate, respond, share, and detect known and unknown threats regardless of organizational size or skillset.

Learn more about Splunk User Behavioral Analytics by contacting ubainfo@splunk.com.