User and Entity Behavior Analytics (UEBA) through FireEye Helix

Manage risk with entity-based alert correlation

Monitoring user and account behavior is a staple of today's security programs. Malicious insiders use privileged access to steal data, while external attackers harvest stolen credentials to gain a foothold in your environment. To detect such threats organizations need a SIEM that uses machine learning to build detections customized to user behavior within their environment.

FireEye Helix offers alert to fix capabilities that use robust analytics and a deep understanding of user and attacker behavior. A native security detection and analytics module within the Helix platform, entity-based alert correlation uses machine learning to identify normal behavior and alert on risky deviations that suggest insider threats, lateral movement or attacks at the end stages of the cyber kill chain.

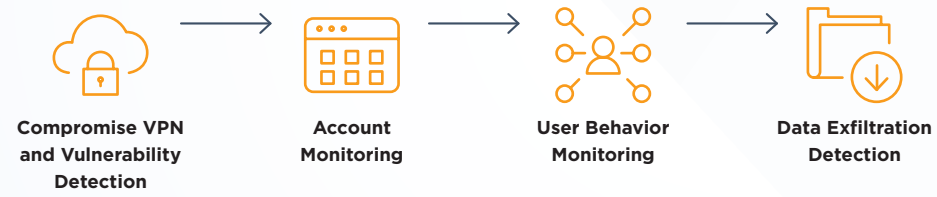

Figure 1. Operational interface for immediate situational awareness.

BENEFITS

- **Prevent Data Loss and Insider Threats:** Monitor user data access and prevent sensitive data from leaving your organization
- **Investigate faster:** Triage alerts with agregated risk scores that are calculated per entity and based on alerts from rules, intel and analytics.
- **Detect late stage attacks:** Find the most critical threats by monitoring connected device behaviors

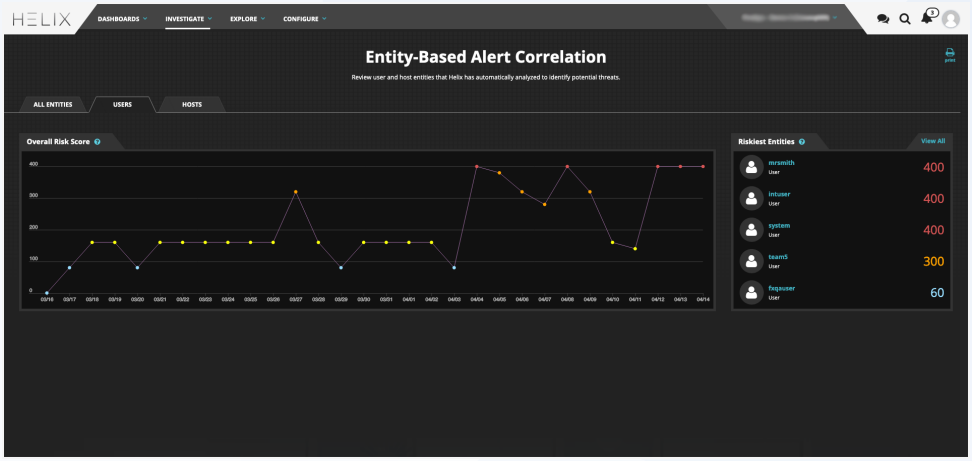

Figure 2. Entity dashboards present a prioritized table of entities and risk scores, and allow you to view entity profiles to identify the highest risk user and host entities so security teams can identify and remediate potential issues.

HOW TO GET THE FIREEYE HELIX PLATFORM

FireEye Helix is available standalone or with the purchase of FireEye's subscription-based solutions. It works across all FireEye technologies and helps integrate your installed base of non-FireEye security products. As your organization grows and changes, FireEye solutions can be reconfigured, added or upgraded without disrupting organizational operations.

ADDITIONAL CAPABILITIES

Data Theft Detection

Detect late stage attacks by identifying when data is being exfiltrated to suspicious destinations using advanced machine learning and statistical anomaly detection.

Compromised VPN Account Detection

Detect compromised behavior using models of login times and locations as well as login hostnames for users within a network.

User Behavior Monitoring

Detect insider threats and automatically generate reports to meet data compliance standards including PCI and HIPAA.

Entity Analytics and IoT Monitoring

Monitor all devices across your network. Use behavioral baselining to detect unusual data flow destinations and login behaviors.

Credential Abuse

Identify abnormal user account creations, privilege escalations and geographically infeasible logins which may indicative of account abuse.

Misconfiguration Detection

Automatically notify your analysts when security devices go silent. Detect third party cloud misconfigurations that can be exploited by attackers.

To learn more about FireEye Helix, visit: **www.FireEye.com/helix**