Brochure

Behavioral Analytics

Hewlett Packard
Enterprise

Identify malicious insiders

HPE Security Products

Malicious insiders are extremely difficult to identify because they are authorized users within your system. They know what tripwires are in place to monitor for security breaches. What is HPE's approach for identifying these malicious insiders?

Why are malicious insiders so difficult to detect?

Traditional security systems are set up to protect the perimeter. They monitor firewall and network activity and deploy systems such as intrusion detection and prevention sensors. These systems are very effective at blocking external threats and malware but ineffective if the attacker is inside your perimeter.

Security systems can utilize insider threat solutions with the goal of detecting abuses and anomalies in the behavior of high-risk, high-profile, or high-privilege users. These systems are set up with "tripwires" that alert to threatening events on internal systems. These systems are configured with signatures to match a user's attempt to access data beyond their permission level or misuse a system in a predefined way. These signatures are easy to setup but the fact that they are predefined means that they are predictable and therefore easy for knowledgeable insiders to circumvent.

Behavioral analytics

HPE has developed and implemented a Behavioral Analytics Security Intelligence Cell (BASIC) solution that is a programmatic approach to countering insider threat and fraudulent activity across an enterprise. The BASIC solution applies a purposefully developed monitoring framework built upon technical and non-technical analytic methodologies for identifying and monitoring insider threats.

> "The intelligent insider knows what attack signatures we monitor for and can avoid triggering them."
>
> – David Beabout, Managing Principal, HPE Security Products Global Services

Technology + HUMINT

The technical aspects are built upon HPE Security Products. The non-technical aspects are based upon offensive and defensive Human Intelligence (HUMINT) operations as well as best practices and subject matter expertise around information security and all-source intelligence analysis. BASIC combines the people, processes, and technologies from both disciplines to enable organizations to identify patterns, indicators, and warnings of a malicious insider as well as ongoing monitoring and response.

Create user baselines

User-based anomaly detection establishes a baseline frequency for each user against all objects he or she touches. The baselines of behavior for individual users can be created with HPE Security ArcSight ESM.

Behavioral alerts

These digital behavior patterns evolve over time and once established, HPE Security ArcSight ESM can trigger alerts upon the detection of any statistically significant deviations from each individual user's activity. If the behavior crosses a specified threshold, then the user's activities warrant further investigation.

Utilize existing technology

The initial BASIC implementation requires HPE Security ArcSight ESM. This allows for baseline creation and alerting. HPE Security ArcSight IdentityView can be added for further identity recognition. For unstructured data monitoring and baselines, you can also incorporate HPE Autonomy IDOL.

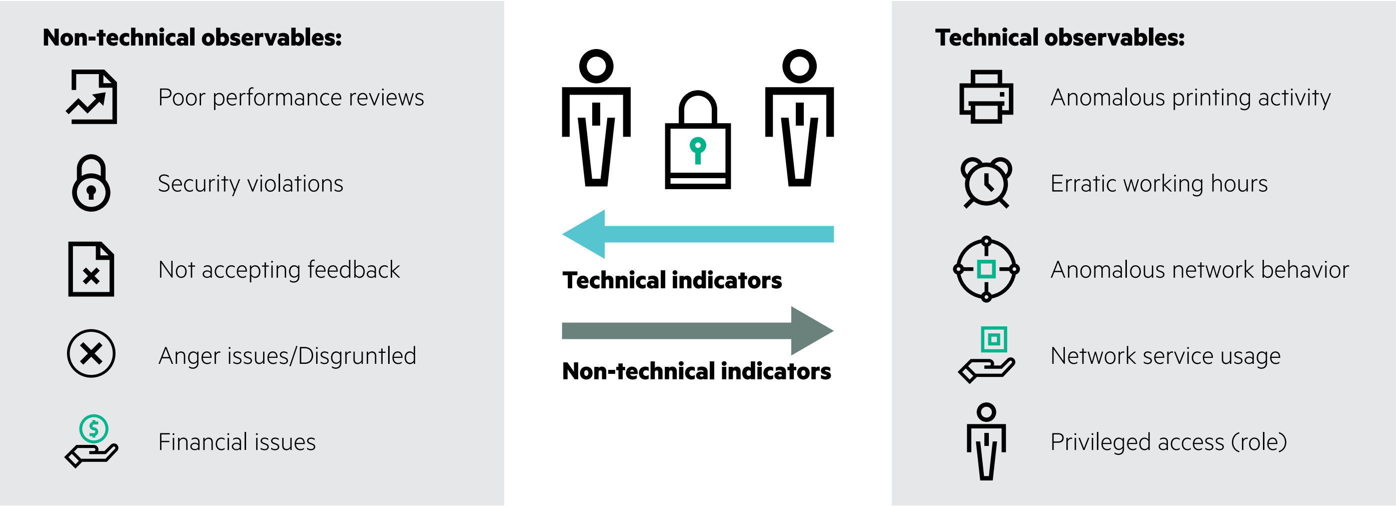

Figure 1: Non-technical observables are combined with technology observables for maximum effectiveness

BASIC solution

HPE Behavioral Analytics Security Intelligence Cell (BASIC) solution includes the implementation of user baselines and anomalous behavior triggers as well as:

- **Graduated response plan:** Tailored to your organization based on individual and organizational traits and patterns of activity leading to measured and appropriate responses to anomalous behavior.
- **Program dashboard and reports:** Provide regular updates and immediate alerts to program management, security officers, and department managers as directed by your organization.
- **Process documentation:** The BASIC solution documents the roles and responsibilities for each person involved, and documents the process around your behavioral analytics implementation. This facilitates the transition of personnel, progress monitoring, and coordination of efforts across your organization.

Why BASIC?

Hewlett Packard Enterprise has experience implementing BASIC at numerous large enterprises and government agencies. Benefits of having HPE Security Products Global Services implement this solution in your organization include:

- Integrates foundations of Human Intelligence (HUMINT)/Law Enforcement investigative functions that help inform better reporting and analysis
- Enhanced monitoring capability filter out anomalous behavior that could be hiding in the normal “noise” of daily network activity
- Greater return on dollars already spent on existing HPE Security ArcSight technology
- Integration and refinement process that is self-learning and provides better fidelity over time

HPE Security Products Global Services

HPE Security Products Global Services can help you achieve your insider threat monitoring goals. We use a combination of operational expertise—yours and ours—and proven methodologies to deliver fast, effective results, and demonstrate ROI. Our proven, use-case driven solutions combine market-leading technology together with sustainable business and technical process executed by trained and organized people. We have delivered security services to thousands of enterprises like yours and can help you build and mature your cyber security and response solutions and capabilities that support the cyber threat management and regulatory compliance.

Learn more at
hpe.com/software/espservices

Sign up for updates

★ Rate this document

Hewlett Packard
Enterprise