SOLUTION BRIEF

Detect and Respond To Insider Threats: Fortinet FortiSIEM With User and Entity Behavior Analytics

Executive Summary

Identifying and responding to threats from negligent and malicious insiders remains a complex challenge that enterprises cannot afford to ignore. Risk from users within an organization can be a serious blind spot in terms of cybersecurity as well as compliance. The transition to cloud-based applications and rapid shift to telework as a result of COVID-19 have reduced visibility and dimished the effectiveness of traditional security controls to flag inappropriate employee activity.

"The global average cost of an insider threat is $11.45 million. The frequency of insider incidents has tripled since 2016."[1]

Fortinet FortiSIEM addresses these challenges in the security operations center (SOC). Our security information and event management (SIEM) platform delivers real-time threat visibility across the entire IT ecosystem. Further, FortiSIEM's user and entity behavior analytics (UEBA) includes unique data security and threat-detection capabilities that provide advanced threat hunting. With endpoint monitoring and behavior analytics capabilities, organizations can detect, respond to, and manage risky user behaviors that put business-critical data at risk.

Gain Visibility

Organizations face a range of challenges to achieving visibility into activity on end-user workstations and identifying undesirable user behavior. FortiSIEM UEBA, based on mature and proven FortiInsight technology, addresses these visibility challenges in an effective, yet nonintrusive manner.

FortiSIEM UEBA is easy to use and works with the traditional SIEM functionality of FortiSIEM to provide monitoring of end-to-end activity, from endpoints, to on-premises servers and network activity, to cloud services. FortiSIEM incorporates real-time, actionable insights into anomalous user behavior regarding business-critical data. This enables comprehensive profiles of users, applications, peer groups, files, endpoints, and networks. Core capabilities include:

- **Endpoint visibility.** Gain complete visibility of data flow (both on- and off-network) via a lightweight stream of user and endpoint behaviors, across platforms and form factors.
- **Federated security.** Assign multiple usernames and passwords to different team members for alerts and incident response tasks.
- **Compliance reporting.** Dedicated reporting capabilities help maintain regulatory compliance such as the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA).
- **Visualization and dashboards.** See key data about the user, processes, endpoint, type of resource (file, database, application), and behavior.
- **Detailed forensics trail.** See a complete record of all user and endpoint activities supporting rapid responses to potential or actual breaches. This is essential for effective incident response, casebuilding, and compliance obligations (for example, the GDPR's 72-hour disclosure rule).

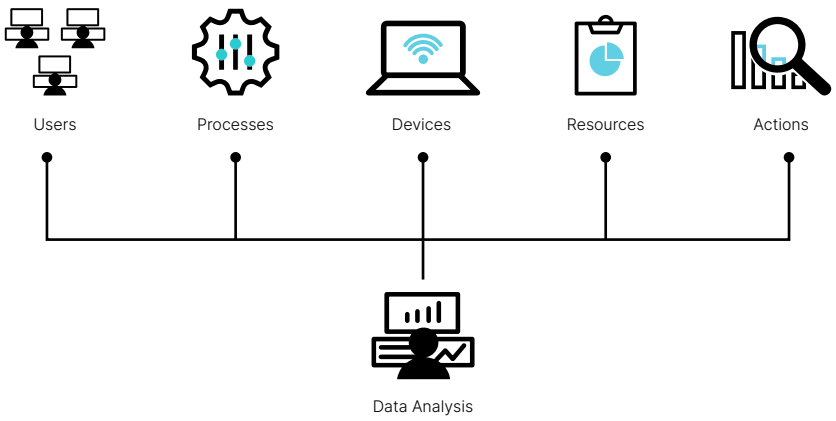
Detect Known and Unknown Threats

FortiSIEM UEBA detects known and unknown threats, ranging from user error, to policy violation, to malicious insider activity, to compromised accounts or account takeover by malicious outsiders. It combines powerful and flexible machine learning with detailed forensics on user actions. This provides full visibility into activities affecting an organization's data (the who, what, where, and when) by monitoring user behavior and data movement—both on and off the network.

FortiSIEM examines user behavior related to data flow to spot unusual activity (such as users accessing files they do not normally seek out) or changes in work patterns, compromised accounts, or unusual peer-group actions. When anomalous behaviors are identified, real-time alerts are sent to relevant stakeholders for immediate investigation.

Key Benefits of FortiSIEM UEBA include:

- Real-time, actionable insights
- Rapid incident response
- Centralized intelligence
- False-positive elimination
- Comprehensive protection



How It Works

The FortiSIEM UEBA engine runs on the FortiSIEM Supervisor node and gathers data from end-user machines via the FortiSIEM UEBA agent. The UEBA agent directly gathers high-fidelity logs, ensuring that accurate data is provided and minimizing overhead on the client device. An agent-based solution also provides visibility into USB-drive activity and can gather logs even when a client is not connected to the corporate network (off-net). Off-net activity can either be cached locally on the client for later analysis, or a FortiSIEM collector can be deployed in a DMZ for off-net agents to upload to when they have internet connectivity.

As demonstrated in the image below, FortiSIEM's lightweight UEBA agent captures high-fidelity data, on- and off-network, by leveraging a five-factor telemetry model. To understand the behavior of users, it uses information from the following:

- Users
- Processes
- Devices
- Resources
- Actions

Maintain Employee Privacy While Monitoring

FortiSIEM UEBA is not an intrusive employee-monitoring solution. It does not perform keystroke logging, screen recording, or detailed web activity logging, which may be a concern for some organizations. The agent logs the interaction of users with resources (files) on the machine, providing the ability to:

- Monitor user, process, and file access activity on laptops to assist with activities such as investigating user activity and performing threat hunting
- Help identify potential insider-threat activity
- Log data exfiltration to USB drives
- Monitor or identify the use of specific applications on endpoints
- Monitor or identify specific filenames or types, for example:
  - Filenames that could suggest confidential data (CustomerData.csv)
  - Filenames that could suggest undesirable media (mp3, avi, mpg)
  - Filenames that could suggest a security risk (passwords.txt)
- Alert when anomalous user behavior is detected

Secure The Network—Inside and Out

FortiSIEM UEBA protects organizations from insider threats by continuously monitoring users and endpoints with automated detection and response capabilities. It automatically identifies noncompliant, suspicious, or anomalous behaviors (on- or off-network) and then rapidly sends alerts. By leveraging machine learning and advanced analytics, our proactive approach to threat detection delivers additional protection and visibility across the entire enterprise network.

[1] Larry Ponemon, "Gaining Insight Into the Ponemon Institute's 2020 Cost of Insider Threats Report," Security Intelligence, January 27, 2020.

September 8, 2021 4:04 AM
779872-A-0-EN