Lumen℠ Managed Security Behavioral Analytics

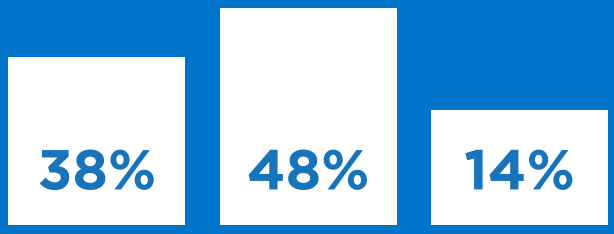
Detect and identify suspicious behavior before incidents become breaches

Cyberthreats inside your organization—especially from malicious individuals, disgruntled employees or compromised accounts—can possibly go unnoticed for months, or even years. Lumen Managed Security Behavioral Analytics gives you advanced visibility into potential threats via a targeted managed security service that profiles, monitors and analyzes risky insider activities.

Benefits

- Detect and deter insider cybersecurity breaches
- Monitor for signs of credential theft, hijacked accounts and login anomalies
- Seek out malicious activities at the operating system, application and database levels
- Detect signs of early breach and minimize dwell time

"While all attack sources pose threats, organizations are significantly more concerned about attacks originating from inside the organization."



Source: CenturyLink Cybersecurity Insiders, Insider Threat Report, September 2019

Features

- **Intelligent analytics**
  Automated threat-hunting algorithm reviews both user and network activities to identify potential indicator of compromise (IOC) risks based on customer use cases, security outcomes, risks and priorities.
- **Embedded detection**
  Lightweight sensor/agent runs on servers hosting critical assets, data and applications.
- **Privileged account monitoring**
  Monitor privileged operations that are security relevant for anomalies and unusual operations such as abuse of data access, unauthorized transactions and excess privileges.
- **Behavioral baseline**
  Gathers insights into individual user personas to establish a pattern of normal behavior in which to identify anomalies and provide fast detection.
- **Real-time discovery**
  24/7 monitoring via integration into the Lumen Security Operations Center (SOC).
- **Platform agnostic**
  Supports multiple operating systems.

Why choose Lumen?

Lumen believes it is essential to see more of the entire network/user activities, to help enterprises stop more cybersecurity threats, including insider attacks. Layered on top of our massive global IP infrastructure backbone with embedded security, Lumen Managed Security Behavioral Analytics analyzes network and user behavior by leveraging advanced cyberthreat detection sensors monitored from our 24/7 SOC facilities. This comprehensive ongoing monitoring and assessment of your environment provides fast detection to insider-initiated breaches, minimizes dwell times and protects your most critical assets, data and applications.

LUMEN®

Detecting anomalies through user behavior monitoring

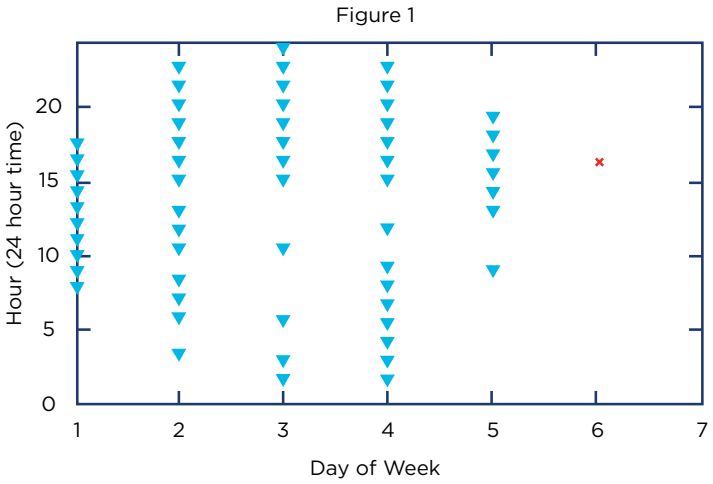


Figure 1

Each user login attempt is profiled, tracked and recorded. The system learns normal behavior consistent with past activity for this person ("green heart"). Unusual privileged user account activities carry a higher risk score and are flagged to Lumen SOC when identified. Ordinary user account activities are analyzed against their baseline profiles and if the anomaly falls outside of the baseline or in volumetric activity, such as data transfer or file access, and deviates more than three standard deviations, the anomaly will be flagged to Lumen SOC.

Recent logins (Stacked) ▼
Anomaly Login ×

Managed security behavioral analytics service

Multi-tenanted Deployment Model

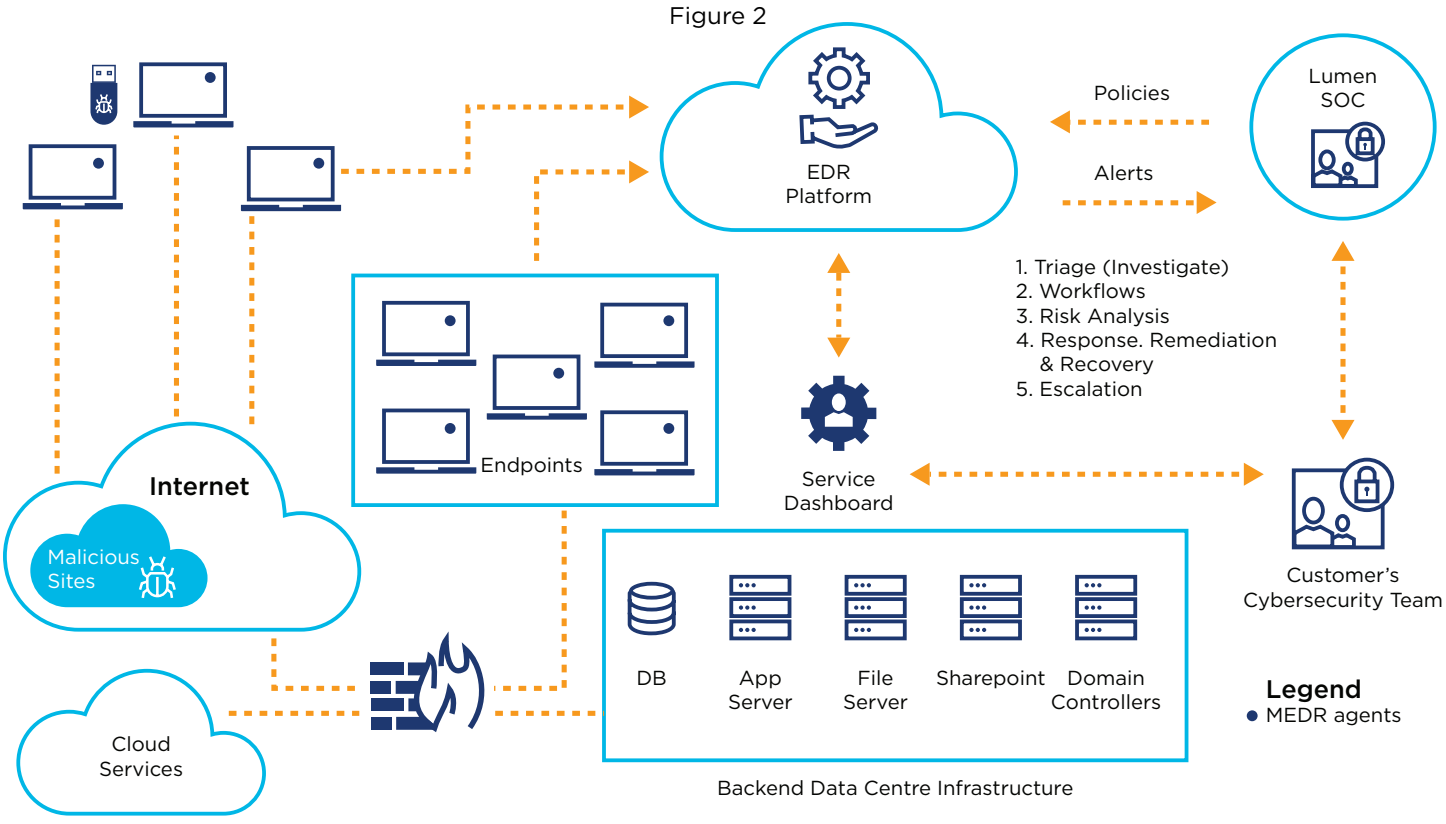


Figure 2

The typical architecture of a customer's enterprise network, servers and where Lumen Service and SOC teams fit into the model, illustrating how we monitor the customer's environment and respond to cyber threats.