opentext™ | Cybersecurity

Case Study

Large Government Agency

ArcSight suite provides full visibility for faster threat response through User and Entity Behavior Analytics.

Introducing UEBA Baselines with ArcSight Intelligence

This organization reviewed their security requirements and looked for a platform to incorporate running advanced and customized correlations on their security events. The security team already leveraged ArcSight ESM by OpenText and ArcSight Logger by OpenText to analyze over 15,000 events per second (EPS). They added additional features to this solid program foundation as custom use cases were uncovered. The Security Analyst explains: "We have a wide variety of data sources: active directory, VPNs, firewalls, web proxies, IPS, Windows data, etc. Visibility into our user and entity behaviors is key for us. We also wanted to connect this directly with our incident response processes so that clear action can be taken as soon as an issue is identified."

> "We plan to further expand and build our SecOps program with ArcSight to mature our threat hunting abilities."
>
> **Security Analyst**
> Large Government Agency

Building baselines in User and Entity Behavior Analytics (UEBA) establishes current user behavior and assigns a risk score to any deviations to determine if they are within an acceptable range. Having enjoyed the benefits of ArcSight, the team was excited to be introduced to ArcSight Intelligence by OpenText, designed to differentiate between unusual behavior and real threats by using mathematical probability and unsupervised machine learning to more accurately identify the most suspicious entities.

Increased Visibility and MITRE ATT&CK Alignment

Introducing the ArcSight suite solution gives the organization the granularity required. It also enables them to ingest Incidences of Concern (IoC) data from all relevant data sources and has aligned them to the MITRE ATT&CK framework. This knowledge base is used as a foundation for the development of specific threat models and methodologies.

At a Glance

Industry

Government

Location

North America

Challenge

Add UEBA capabilities to bolster an already solid security program to gain more visibility into individual user behaviors

Products and Services

ArcSight Enterprise Security Manager (ESM)
ArcSight Logger
ArcSight Intelligence

Critical Success Factors

- Faster threat response with fully incorporated incident response processes and procedures
- Alignment with MITRE ATT&CK framework matures threat hunting ability
- Ingest IoC data from all relevant data sources

768-000028-002 | O | 08/23 | © 2023 Open Text