opentext™ | Cybersecurity

Product Flyer

ArcSight Intelligence—Behavioral Analytics Starting with Azure AD

Swiftly reveal hidden and unknown threats, including insiders and advanced persistent threats (APTs) when pairing ArcSight Intelligence's advanced behavioral analytics with Microsoft Azure data.

ArcSight Intelligence—Behavioral Analytics Starting with Azure AD at a Glance

- Advanced insider threat, novel attack, and APT detection
- Detection that evolves with your constantly changing attack surface
- Distill billions of events into a handful of actionable leads
- Risk aggregation enabling low and slow attack detection
- Do more with your Azure AD data

The Power of Behavioral Analytics

Defending an organization from attacks is expensive, time consuming, and exhausting. While the attacker need only be right once, defenders need to be right 24/7. Because of this, defenders must have the right tools in place to catch threats before damage can be done. User Entity Behavior Analytics (UEBA) is one of these tools.

ArcSight Intelligence by OpenText™, a UEBA solution, uses machine learning to identify "normal" behavior for entities (users, servers, endpoints, etc.) in an organization, finding and alerting threat hunters when anomalies are detected. Where rules, thresholds, and pattern matching techniques of traditional security tools are adept at catching known threats, ArcSight Intelligence is adept at catching unknown threats.

ArcSight Intelligence provides context rich leads allowing threat hunters to focus less on hypotheses-based hunting and more on detecting and preventing attacks in progress. Not only does ArcSight Intelligence improve your threat hunters' effectiveness, it also improves your overall SOC efficiency. Unlike other tools that require frequent updating of rules and thresholds to remain relevant and reduce false positives, ArcSight Intelligence continually adapts and evolves with your changing organization, automatically.

Improving Effectiveness

During the COVID-19 pandemic many security teams were inundated with false positives as companies adopted work-from-home policies. While ArcSight Intelligence did show higher than normal risk scores during the transition, ArcSight Intelligence automatically adjusted to the new normal within days without any intervention. This allowed overworked security teams to remain focused on current threats rather than updating their detection tools.

Leverage Your Azure Active Directory

To effectively detect insider threats, novel attacks, and APTs, ArcSight Intelligence relies on rich data sources such as Azure Active Directory. With Azure AD data alone, ArcSight Intelligence can detect attack scenarios such as:

- Account misuse
- Compromised accounts
- Internal recon
- Lateral movement

By monitoring your Azure Active Directory logs for anomalies and flagging the riskiest entities for further investigation, ArcSight Intelligence adds greater security value to data already being collected by your organization and reduces the effort required to analyze the data coming in.

Cloud first organizations using Azure AD realize the importance of detecting threats before an attacker can gain a foot hold in an active directory. ArcSight Intelligence shines a light on threats poking and prodding your active directory, Office365, and SharePoint services to gain access while revealing attempts to exfiltrate data to external locations such as Google Drive, Dropbox, or writable device.

With Azure AD alone ArcSight Intelligence has detected and helped stop real attacks including:

- Watering hole attack against employees
- SIM swapping attack against C-Suite Executives
- Two Factor spamming attack
- Password guessing
- Sensitive file access/modification

Employee Compromised Account Used in a Copy Shop

Using Azure Active Directory data with ArcSight Intelligence a customer of ours was able to detect a unique attack in near real time. During a daily threat hunt in ArcSight Intelligence, a large healthcare provider noticed an unusually high risk score for a single entity. The entity in question was an account for an employee who worked on the east coast of the U.S. Just seven minutes after logging into their account, Azure AD recorded a second login from a location more than an hour and a half away, raising the entities risk score.

While impossible travel is anomalous on its own, ArcSight Intelligence then picked up that the entity accessed an unusual volume of applications as well as accessing SharePoint and exchange online, applications they had rarely/never used. When aggregated these anomalous events raised the users risk score to a concerning level prompting an immediate investigation. ArcSight Intelligence's contextual insights and correlated findings help threat hunters identify that the attack originated after hours from a print and copy shop.

Do More with Azure AD + EDR

As amazing as Azure AD data is for behavioral analytics, it is not the only source of data security teams are collecting. ArcSight Intelligence has a proven track record of detecting hidden threats using endpoint detection and response (EDR) data as well.

While Azure AD data provides insights into authentication and application access data, EDR unlocks user and entity level telemetry valuable for detecting unique attack vectors. From unusual network connections, to data staging and exfiltration on off-cloud devices, to detecting lateral movement across devices, ArcSight Intelligence with EDR and AD data provides an impressive coverage of the MITRE ATT&CK tactics and techniques giving security teams tools to detect attacks in areas previously undetectable.

Learn more at
www.microfocus.com/en-us/cyberres/

Connect with Us
www.CyberRes.com

opentext™ | Cybersecurity

OpenText Cybersecurity provides comprehensive security solutions for companies and partners of all sizes. From prevention, detection and response to recovery, investigation and compliance, our unified end-to-end platform helps customers build cyber resilience via a holistic security portfolio. Powered by actionable insights from our real-time and contextual threat intelligence, OpenText Cybersecurity customers benefit from high efficacy products, a compliant experience and simplified security to help manage business risk.