opentext™ | Cybersecurity

Service Flyer

ArcSight Intelligence with Microsoft Defender for Endpoint

Swiftly reveal hidden and unknown threats, including insiders and advanced persistent threats (APTs) when pairing ArcSight Intelligence's advanced behavioral analytics with rich Microsoft Defender for Endpoint telemetry.

ArcSight Intelligence with Microsoft Defender for Endpoint 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 Microsoft Defender for Endpoint 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, Intelligence is adept at catching *unknown* threats.

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, 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 Intelligence did show higher than normal risk scores during the transition, 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.

Essential to Advancing Defender's Security

Microsoft Defender for Endpoint

ArcSight Intelligence effectively detects insider threats, novel attacks, and APTs by repurposing the rich telemetry that is already being produced by the Microsoft Defender endpoints in your enterprise.

Microsoft Defender for Endpoint telemetry is especially powerful when used for behavioral analytics since it records events that take place on individual endpoints and across all endpoints in an organization. With Microsoft Defender telemetry, ArcSight Intelligence can detect attack scenarios such as:

- Data staging/exfiltration
- Unusual uploads/downloads
- Account compromise and misuse
- High risk IP/data access
- Unusual traffic and connections
- And more

With just the Microsoft Defender data, Intelligence is not only able to detect these attack scenarios but provide contextual and relevant insights to threat hunters to quickly determine the best way to stop a threat from becoming a major security incident.

Intelligence with EDR solutions like Microsoft Defender has detected and helped stop real attacks including:

- 3rd party supply chain attacks
- Nation state attacks
- Advanced reconnaissance
- Sensitive file accesses/exfiltration
- Password guessing on C-Suite accounts (and more)

Preventing Layoff Data Exfiltration
During a round of layoffs an ArcSight Intelligence customer wanted to ensure outgoing employees were not walking off with company secrets. Using Intelligence with EDR data, the customer detected an employee logging in outside of their normal working hours and attempting to transfer 4,000 plus files to a removable device.

When confronted about the files, the employee assured the security team that he wasn't doing anything shady and promised not to transfer files again. Less than a week later the employee increased their risk score by running an application that had never been run by anyone in the company and then attempting to move over 800 GB of data to a removeable drive in a single transfer prompting the security team to take further action.

Despite a change in attack vectors and an attempt to hide their real intent, ArcSight Intelligence was able to detect the employee's anomalous behavior, raise their risk score, and provide the contextual evidence needed to prevent further damage.

Microsoft Defender + Microsoft Entra ID with Intelligence

While ArcSight Intelligence is effective at using Microsoft Defender for Endpoint data to detect threats originating from company-controlled endpoints, an organization's digital footprint and attack surface extends beyond physical hardware and devices. Microsoft Entra ID (Formerly Azure Active Directory) data is an excellent source of telemetry for Intelligence that gives security teams powerful insights into unusual user authentication attempts, cloud, or web application access, and more.

When paired together, Microsoft Defender telemetry and Microsoft Entra data complement each other and expand your visibility of relationships between endpoint and cloud entities. Combining endpoint, active directory, and cloud application (Office365 and SharePoint) data, Intelligence can follow threats as they move between endpoint and cloud, highlighting potentially risky entities faster than with endpoint data alone.

Learn more at
www.arcsight.com/intelligence

Connect with Us
www.opentext.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.

761-000115-002 | O | 10/23 | © 2023 Open Text