Flyer
Analytics and Big Data
Security

User and Entity Behavioral Analytics for Financial Services

ArcSight Intelligence behavioral analytics gives financial services organizations a new lens through which to detect, investigate, and respond to unknown threats—before your data is stolen.

Financial services organizations find managing cyber risk increasingly important as they work hard to protect sensitive customer data in the face of more frequent and more targeted attacks. In fact, financial services firms suffer from cyber attacks 300 times more than businesses in other industries (Identity Theft Resource Center, 2018). Three-quarters of financial services executives agree that cybersecurity is one of the top three risks that will be of increasing importance over the next two years, but only half of these executives feel their institutions have the issue under control (Deloitte, Global Risk Management Survey, 2019). At the core of these organizations' fight against cybercrime is a difficult-to-solve challenge: limited human and financial resources.

ArcSight Intelligence behavioral analytics helps financial services security teams maximize their existing resources and gives them a new lens through which to detect, investigate, and respond to threats—before data is stolen. Using machine learning, ArcSight Intelligence distills billions of events into a prioritized list of high-quality security leads to focus and accelerate the efforts of your security operations center (SOC). ArcSight Intelligence's machine learning models, combined with an intuitive user interface (UI), accelerate threat detection and investigation from weeks to minutes.

Why ArcSight Intelligence

Financial services organizations have important assets to protect, whether it is customer information, intellectual property, or both. Unfortunately, existing approaches to protecting these assets continuously fall short, leaving security teams to contend with rigid, rules-based analytics, fragmented security ecosystems, and a never-ending barrage of alerts—most of which are false alarms. Meanwhile, these teams are expected to flawlessly protect against critical threats like data exfiltration and unauthorized network access.

ArcSight Intelligence is uniquely positioned to find the threats that matter for enterprises with valuable data to protect, limited security resources, and significant surface area to monitor—characteristics common among financial institutions. Unlike other solutions, ArcSight

Detect. Investigate. Respond.

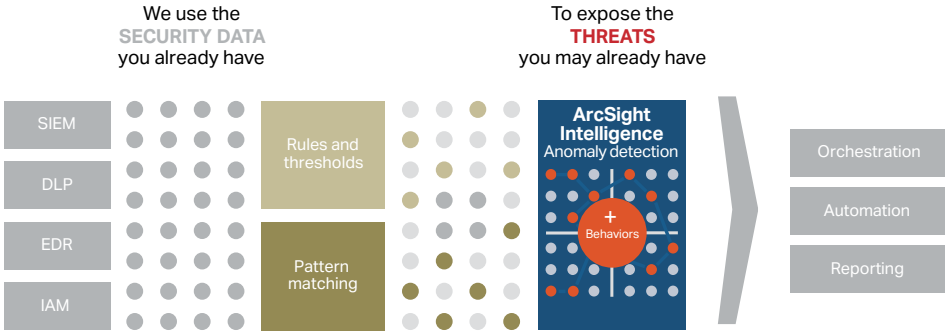


Figure 1. ArcSight Intelligence views your existing security data through a new lens in order to identify hidden threats by looking for anomalous behavior. This produces high-quality threat leads, allowing your security teams to respond and remediate quickly and effectively.

Threat Detection Use Cases

Insider Threat
- At-Risk employee
- High-Risk Employees
- Account Misuse
- Privilege Account Misuse
- Terminated Employee Activity

Data Breach
- Data Staging
- Data Exfiltration
- Email Exfiltration
- Print Exfiltration
- USB Exfiltration
- Unusual data access
- Unusual uploads

Advanced Threat
- Compromised Account
- Internal Recon
- Unusual Traffic
- Abnormal Processes
- Unusual Applications
- Infected Host
- Malicious Tunneling
- Bot Detection

IP Theft
- Mooching
- Snooping
- Interactions with dormant resources/files
- High Risk IP/Data Access
- Lateral Movement

Figure 2. ArcSight Intelligence uses advanced mathematical algorithms to constantly mine billions of data points and reveal indicators of insider threats, data breaches, advanced persistent threats (APT), IP theft, and more.

Intelligence bypasses rules and thresholds and instead assesses the potential risk of a user or entity in your enterprise based on mathematical probability and unsupervised machine learning models. This approach, combined with ArcSight Intelligence's native big-data architecture, allows your security team to detect difficultto-find threats with speed and at scale

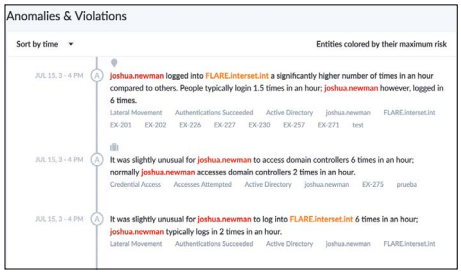
Using supervised machine learning—a type of artificial intelligence (AI) that doesn't need labels—ArcSight Intelligence's algorithms extract available entities (users, machines, IP addresses, servers, printers, etc.) from within log files and observe events that involve these entities to determine expected behavior—a measurement we call "unique normal." As new information comes through the analytics process, events are evaluated against previously observed behavior to assess potential risk.

With this process of baselining and scoring, ArcSight Intelligence boosts the efficiency and speed at which security teams detect, triage, investigate, and respond to threats. ArcSight Intelligence's output risk assessments can be used to initiate actions via automation, orchestration, and alerting solutions to execute faster-than-human actions as risks are found. ArcSight Intelligence also provides downloadable reports summarizing immediate organizational risks.

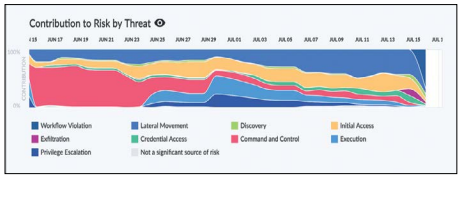
Viewing Risky Entities

As a security practitioner, your primary mechanism for interacting with ArcSight Intelligence is the intuitive, web-based dashboard. ArcSight Intelligence's dashboard allows users to quickly and easily determine which entities represent the greatest potential risk. As entities are identified, the dashboard allows you to drill down into results so that the potential risk can be understood in the context of the generated alerts and, if desired, the raw events that produced them. The screenshots below show a drilldown from the list of riskiest users down to the raw events:

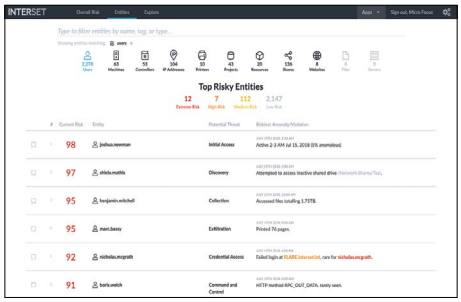
1. View all entities within the enterprise with analytics to display, grouped by entity type. The screenshot shows a list of users, with a presentation that displays them in order of risk score from highest to lowest.



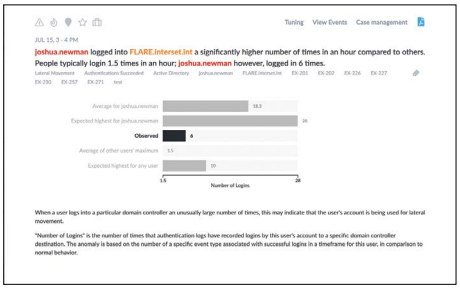
2. When any entity is viewed, its risk score over time is displayed in a timeline view. This perspective shows not only the change in risk score, but also broadly characterizes the types of behavior that drove it.



3. When viewing an entity, a display of the alerts associated with the entity can be seen below the timeline view. They can be filtered by associated entities and types of risk and, because they display in chronological order linked to the timeline view, it is simple to see a narrative of the unfolding behavior in the context of other events.



4. Clicking on any of the alerts allows for examination that shows the event in context of the user's baseline and other relevant entities in the enterprise. The risk associated with the alert is displayed, and the model that triggered the alert is described in detail. Note that the user's baseline is compared to both itself, as well as to other similar entities. These similar entities are identified through statistically determined peer groups.



5. The raw events that triggered an alert are only one click away. In addition to seeing the actual contents of the log file responsible for the analytics, users have the ability to enter additional queries using this interface.

Table 1. Screenshots of the ArcSight Intelligence dashboard showing navigation through the analytical results.