ArcSight Investigate

Micro Focus® ArcSight Investigate enables organizations to proactively respond to and decrease the impact of security incidents.

Product Highlights
Despite the advent of machine learning and advanced analytics, every step of security investigation relies heavily on security analysts’ experience and ability to identify threats and make appropriate decisions. While the demand for skilled talent is constantly increasing, more than 285,000 cybersecurity positions were unfilled in 2018 in the United States alone, and unfilled cybersecurity positions are expected to reach 3.5 million worldwide by 2021.

To address the ongoing skills and talent shortages, leading organizations are looking beyond traditional security tools and investing in new technologies to increase speed, simplicity, and analytical capabilities across the entire process of security operations.

ArcSight Investigate is a next-generation hunt and investigation solution built on a new advanced analytics platform to serve the evolving needs of security teams. It helps hunt and defeat unknown threats by processing large volumes of data almost instantly. Security analysts are empowered with an intuitive solution to investigate higher-priority threats quickly and accurately. With the ability to leverage data lakes, ArcSight Investigate provides insights from Big Data to drive real value.

Features and Benefits

**Act Faster by Identifying Threats Instantly**
ArcSight Investigate now helps you hunt for unknown threats faster by providing you deeper insights into host behavior through the Host Profiler dashboard. The ‘findwho’ function helps find which users were impacted by a security event, without the need to write a query.

1. **Host Profiler dashboard provides fast valuable insights into host behavior**
2. **Build queries from Day One with guided suggestions**
3. **Pre-defined visualizations + custom charts and dashboards optimized for security investigation**
4. **Easy integration with Hadoop expands data visibility for analysis**

**Key Benefits**

- Hunt and defeat unknown threats faster
- Improve analysts’ productivity to address talent shortages
- Decrease the impact of security incidents by reducing response time
- Lower risks with a complete view of security events

---

1. HuntSource—The Top 4 Cyber Security Jobs of 2018
Powered by Vertica, a high performance analytics platform, it brings unprecedented analytical power to the investigative process. Vertica’s columnar database responds to queries much faster than traditional row-oriented databases and handles analytics at exabyte scale. By embedding this new technology, ArcSight Investigate can execute lightning-fast searches, returning results in seconds even for months or years of data. With proven ingestion rates in the hundreds of thousands of events per second (EPS), the ability to ask questions at scale unlocks the opportunity for security analysts to explore data without limiting the time span or result size of their searches.

**Work Smarter with Guided Experience**

ArcSight Investigate provides an intuitive search interface that understands search terms in security context and dynamically suggests relevant queries. Users can easily build or modify a query by choosing from suggestions or clicking a drop-down menu. ArcSight Investigate Version 3.0 offers pre-defined visualizations that provide analysts with comprehensive out-of-box visual insights with the ability to edit and rettool as needed. Through direct integration with ArcSight Enterprise Security Manager (ESM), ArcSight Investigate populates an automatic query from ArcSight Enterprise Service Manager, allowing an immediate launch of investigation. On day one, junior security analysts can create queries without learning a complex query language or proprietary schema. Advanced users benefit from saving time to script complex queries through smart suggestions.

Once search results are retrieved, sifting through the millions of events for investigation is another complex and time-consuming challenge. ArcSight Investigate provides easy data interaction allowing users to navigate, aggregate, and visualize data without running queries or exporting data to another analytics tool. Pre-defined chart types help quickly visualize data to identify patterns, anomalies, and relationships between events. By simply saving charts or adding visuals, a customized dashboard is created for a security analyst to view key metrics at a glance, and continuously monitor in-progress investigations.
Reach Further to Uncover Hidden, Unknown Threats

Disparate, unstructured data storage delays the investigation process and limits the ability to connect repeated patterns or multi-stage attacks. Through integration with ArcSight Data Platform, normalizing and categorizing security data from various sources, ArcSight Investigate empowers security teams to build a single, structured data lake for data exploration. Powerful analytics built in to ArcSight Investigate derive meaningful insights from Big Data to uncover hidden threats.

In many organizations, long-term data stored in Hadoop are rarely fully utilized for security investigation due to the time consuming user experience. ArcSight Investigate’s integrated user interface accessing historical events stored in Hadoop removes any friction and provides a seamless view to search and analyze data of any timeframe.

Increase Speed, Simplicity and Effectiveness of Your Security Operations

By delivering blazing fast search results, ArcSight Investigate reduces response time to security incidents and allows security analysts to follow their hunches with numerous experiments to hunt unknown threats. Having all structured data in one place ready for analysis accelerates investigation and improves the quality of information gained from the data. Most importantly, ArcSight Investigate streamlines manual tasks with its intuitive search interface and built-in analytics. It minimizes requirements for expertise and training for security analysts, helps prioritize their time, and improves the efficiency of their jobs.

Learn more at www.microfocus.com/arcsightinvestigate