opentext™ | Cybersecurity

Case Study

Major Healthcare Provider

ArcSight supports efficient patient care through transparent risk monitoring with relevant statistics, improving resolution times.

Overview

This healthcare provider is ranked among the best hospitals in the country and delivers comprehensive, integrated, family-focused care in more than 100 medical specialties.

Challenge

With over 25,000 users, 22,000 desktops, and 3,000 servers to maintain and keep secure, the healthcare provider realized a Security Information and Event Management (SIEM) solution would be vital to securing their networks. With ever-changing healthcare regulations, the organization is regularly audited, both internally and externally, and structuring the data to provide easy access became more difficult as the IT infrastructure grew. A Security Information Analyst for the organization explains the challenge further: "When we first started exploring a SIEM, we knew that we needed to track our critical IT systems better, but we really weren't quite sure how to do this or what to track. We worried about cyber threats and the increasing associated risks. Although implementing a SIEM seemed almost like a trend at the time, we felt sure this would help improve the control on our security situation for the long term."

> "I liken ArcSight to a Ferrari. It takes you a little while to get to know all its abilities, but once you do, it is the most powerful security solution you will find."
>
> **Security Information Analyst**
> Major Healthcare Provider

Solution

The organization conducted extensive market research to find the right solution, as the customer comments: "We investigated IBM QRadar and Nitro (now marketed as McAfee Enterprise Security Manager). However, ArcSight (by OpenText™) has the reputation of being the best solution. I had worked with ArcSight in a previous position and knew that it could deliver the security and control we were looking for."

ArcSight Enterprise Security Manager (ESM) by OpenText collects data and correlates events in real-time to escalate threats that violate the internal rules within the platform. ArcSight Logger by OpenText was deployed to support this large, multi-location ArcSight implementation. It delivers a cost-effective universal log management solution that unifies searching, reporting, alerting, and analysis across any type of

At a Glance

Industry

Healthcare

Location

New England, USA

Challenge

Combat cyber security threats, provide comprehensive audit feedback, and run a secure IT environment for 25,000 users in a highly regulated healthcare environment

Products and Services

ArcSight Enterprise Security Manager (ESM)
ArcSight Logger

Critical Success Factors

- Identify and address security incidents within 10–15 minutes
- Respond efficiently and timely to audit requests
- Track privileged users to quickly act upon compromised credentials
- Future-ready SIEM to manage IoT medical devices

> **“The Internet of Things is an area where ArcSight can really come into its own. It is a huge challenge but with our sophisticated ArcSight SIEM in place we feel ready to meet it head on.”**
>
> **Security Information Analyst**
> Major Healthcare Provider

Connect with Us
www.opentext.com

enterprise machine data. The data is used for compliance, regulations, security, IT operations, and log analytics.

The customer provides his point of view from years of experience as a security expert: “I liken ArcSight to a Ferrari. It takes you a little while to get to know all its abilities, but once you do, it is the most powerful security solution you will find. Nowadays, auditors love us. We easily meet all of their parameters and collecting security logs takes minutes now. We work closely with our internal infrastructure auditing team for analysis and reporting on any new proposed tooling. For us, it is key that we understand what ‘normal’ looks like, so that any deviations from it are easily and quickly identified. Every day we encounter millions of potential security events in our infrastructure. With ArcSight, we can easily distinguish the false positives from the true positives and take decisive action accordingly.”

ArcSight collects information from many systems, including end-point security solutions. This way the organization keeps track of all users with escalated privileges. Compromised credentials in this group could mean serious harm to the organization. A list of these users is dynamically updated through their directory and ArcSight notifies the security team of any unusual activity here so that swift action can be taken.

Emerging cyber threats can attack a network and migrate from server to server with specific malware. For example, EternalBlue was linked to several serious cyber-attacks. EternalBlue was developed by the U.S. National Security Agency according to testimony by former NSA employees. It exploits a vulnerability in Microsoft’s implementation of the Server Message Block (SMB) protocol. With the different systems reporting into ArcSight, any intrusions, including EternalBlue attempts, are immediately identified and reported to system analysts, enabling them to quickly address the breach and limit its impact. This experienced ArcSight analyst further explains: “We particularly like the quick and easy after-action analysis ArcSight gives us. No more endless scrolling through security logs; within 10–15 minutes we have worked out what happened and taken corrective action.”

Results

The Internet of Things (IoT) looms large in this healthcare provider’s security strategy. A clinical engineering team is engaged in internet-connecting many devices, such as infusion pumps and blood pressure monitors, so that valuable patient data is collected and interpreted in real-time. The customer contact explains: “The Internet of Things is an area where ArcSight can really come into its own. It is a huge challenge but with our sophisticated ArcSight SIEM in place we feel ready to meet it head on.”

He concludes: “Our doctors are very tech-savvy and it is of vital importance that we give them the tools to look after our patients most efficiently. With ArcSight we provide controlled system access to those who need it, while keeping security incidents to an absolute minimum. We have been very encouraged by the Micro Focus (now part of OpenText) development and support of the ArcSight portfolio.”

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.