Hewlett Packard Enterprise

Case Study

Lake Health

Objective
Improve overall system performance through the rapid mitigation of anomalies

Approach
Implement an effective security information and event management (SIEM) system in order to reduce multiple dashboards to a single version of the truth across the enterprise

IT Matters
- Implemented a solution that supports a proactive approach to identifying and mitigating anomalies in Lake Health's networks and systems
- Gained the ability to process several thousand events per second through HPE ArcSight
- Greatly simplified the process of obtaining information, with HPE ArcSight pulling information from multiple sources and aggregating it together
- Increased the number of anomalies that are investigated and resolved by a factor of 10, from 30 per year to around 300

Business Matters
- Automated situational awareness across the entire network to enable timely response to security threats and system malfunctions
- Streamlined compliance with a broad range of healthcare requirements, including PCI and HIPAA
- Enhanced Lake Health's ability to prevent disruptions that might impact patient safety and care
- Integrated HPE ArcSight with existing and new technology to maximize the organization's technology investment
- Freed resources for use elsewhere at Lake Health, because HPE ArcSight can be managed with a very small staff

Lake Health enhances patient experience with HPE ArcSight

Healthcare provider

"HPE ArcSight allowed us to go from a reactive to a much more proactive approach to information security. Without HPE ArcSight, there is no way that we could aggregate these types of events and get the visibility that we have."

– Keith Duemling, Information Security Officer, Lake Health

A proactive approach to security

Lake Health—a private, not-for-profit leader in community healthcare in Northeast Ohio—aims to be the first choice for superior care close to home. Its vision is to coordinate a lifetime of health, which patients and families experience as warm, responsive, and state-of-the-art. Achieving this vision requires modern facilities, advanced services, and a superlative clinical staff. It also requires a secure and reliable IT infrastructure that supports efficient operations and the highest patient care quality. Today, Lake Health has this kind of infrastructure, thanks in large part to the event management capabilities of HPE ArcSight.

Lake Health experienced several minor information security events which helped the organization with the decision to deploy an event management solution. Self-replicating applications entered the environment via remote connections and impacted a very small number of the organization's non-critical workstations. They did not access any system that contained patient data or critical financial data, but they were able to disrupt certain operations. And it took a while for the Lake Health information security team to identify all the places the applications had reached and to repair the damage.

It was a wake-up call. "One thing we learned was that we could not easily say, 'Something unexpected has entered the organization, and we need to respond to it,'" recalls Information Security Officer Keith Duemling. "We were unable to pull all those different event sources together, and we found out about the events through our end-users calling the help desk to report abnormal behavior."

Lake Health went looking for a tool that would support a proactive approach to identifying and mitigating anomalies in its networks and systems. Based on extensive research and a comprehensive proof of concept, HPE ArcSight was the right answer.

Heavy lifting

Lake Health's challenges are like those of most healthcare environments. In addition to myriad compliance-related requirements, including PCI and HIPAA, it is critical to understand what is going on across the network at all times. "This is not just related to privacy and security, but also to system uptime," explains Duemling. "The aim is to prevent disruptions that may impact patient safety and patient care."

Before implementing HPE ArcSight, Duemling had to log into a virtually endless set of different dashboards and applications to obtain information; for some systems, he even had to develop scripts or applications to look for a specific event. "We specifically implemented HPE ArcSight to get away from that, so we could allow a proven technology to do the heavy lifting for us," he says. "All we had to do was build a dashboard and put in queries, and then HPE ArcSight could pull the information from multiple sources and aggregate it together for us."

Events of interest can take many forms. A common one is unexpected account lockouts, whether for a service account or an actual named user. An account lockout can be a clue that someone is trying to maliciously compromise the password associated with that account. Or, it can indicate a denial of service attempt; if the account can be locked out for an extended period of time, then anything that relies on that account will malfunction. Account lockouts can also be used as a means of reconnaissance, with the intent to hack user directories and probe for weaknesses.

Before deploying HPE ArcSight, rooting out such problems was cumbersome and time-consuming. Now, Duemling immediately homes in on the source of a given event. "Basically, we can take our thousands of systems and shrink that number down to just the two or three systems where we are seeing the anomaly occur," he says. "Rather than islands of data, we have one continent of data that we can run all the queries against and say, 'This is the threat, this is what it's impacting, and here's how we contain it.'"

Right-sized solution

Lake Health exercised due diligence in seeking the best event management system, conducting extensive research and evaluating both on-premise and managed services options. "In the end, we felt that HPE ArcSight was the best solution to drop into our infrastructure, knowing that we had limited resources within our department to manage the technology," says Duemling. "The proof of concept convinced us that HPE ArcSight could readily absorb the information and aggregate it in a way that we could act on."

The proof of concept (POC) did more than demonstrate superior performance and functionality; it also provided immediate and empirical evidence that HPE ArcSight was easy to implement and use. "The setup time for the POC was only three days," recalls Duemling. "By the end of the second day, we were already pulling events into HPE ArcSight—and by the end of the third day, we were starting to build our own connectors into different applications in our environment that would generate events. This showed us that we could manage the technology on a day-to-day basis very cost-effectively, with existing staff."

Duemling adds that the solution was right-sized for Lake Health. "The appliances came preinstalled with the software, and all we had to do was apply some minor version upgrades. It was pretty close to 'plug-and-play.' We dropped the appliances in, spent a couple hours getting them configured on the network, did some knowledge transfer, and then we were able to move right into the proof of concept. That really spoke to the ease of implementation of the technology."

Exponential increase

Lake Health does not have a large information security staff, but HPE ArcSight acts as a manpower multiplier, and staff have dashboards with HPE ArcSight running 24x7 on big screens. They leverage HPE ArcSight to show on a minute-by-minute basis what the landscape looks like and how it is changing, using customized case studies, reports, and similar methods to aggregate specific pieces of knowledge to the surface.

This improved situational awareness translates directly into faster response time. Explains Duemling: "I have a much better answer when the CIO comes into my office and says, 'This issue has been reported to me. What do we know?' Instead of 'Come back tomorrow,' I can say 'Well, let's take a look.' We pull up the dashboard and start doing searches in real time."

Lake Health also uses HPE ArcSight as an event triaging tool. If Duemling sees something abnormal, he creates a case and starts aggregating information from the different event sources. Then he marries that data up with the organization's internal case tracking software system, so he can back up the observations based on the technical information from HPE ArcSight.

In addition to identifying and addressing specific security threats, HPE ArcSight has helped identify some anomalies that involve system malfunction. "When we fix them, typically the performance improves," says Duemling. "So we have had a number of positive outcomes, from the security standpoint as well as performance improvement."

The ability to track and respond to anomalies has increased exponentially with HPE ArcSight. By the end of this year, Lake Health will have investigated several hundred specific anomalies; prior to implementing the solution, it was just a few dozen per year. Several thousand events per second are being processed through the HPE ArcSight technology, and there is an initiative in the works to increase the volume by broadening the classification of events.

Information assurance

At Lake Health, HPE ArcSight is central to keeping the IT infrastructure secure and operational. "Without HPE ArcSight, there would be no way to aggregate all these events and get the visibility we have," says Duemling. "There is just too much volume occurring 24x7 for any one person or group of people to effectively process that stream of information. It would be like trying to drink water from a fire hose." With HPE ArcSight, Duemling no longer has to rely on end-users calling the help desk. "HPE ArcSight helps us be proactive rather than reactive. We are already aware of the issue, we are tracking it, we are working to resolve it—and, in many instances, we notify our end-users long before they see any type of disruption."

IT security and operational efficiency are key to Lake Health's success, but Duemling is not stopping there. His personal vision encompasses the much broader concept of information assurance—making sure the data on which clinical decisions are made is always available and unquestionably trustworthy—and here again, HPE ArcSight will play an important role. For example, Duemling plans to pull deeper pieces of information from the various applications, such as record modification anomalies in the electronic medical record system, to help ensure the integrity of the data. This will provide an additional check, helping to ensure that life-critical data such as patient blood type is always correctly shown in the system.

Worth the money

Staying ahead of the hackers, whether recreational or state-sponsored, is an exploding challenge. In addition to account lockouts, Lake Health uses HPE ArcSight to monitor hits against the organization's antivirus systems, looking for things like worms, viruses, and Trojans. Duemling is also starting to look for anomalies when it comes to account activity, especially accounts that are not used for long periods of time and then suddenly become active.

Case study
Lake Health

Industry
Healthcare

Customer at a glance

Software
- HPE ArcSight Express
- HPE ArcSight Logger

HPE Services
- HPE ArcSight professional services

Integrating HPE ArcSight with the electronic medical records (EMRs) is another exciting development. "This will make it possible to identify the accounts that accessed a given record across all the different applications between Friday and Monday, making it a proactive HIPAA auditing tool," says Duemling. "Our network monitoring systems aggregate events and forward them into HPE ArcSight, so we are able to pair up what happens from a logical standpoint with what's happening in the physical world." Lake Health also plans to integrate HPE ArcSight with the badge systems, such that if there is ever an incident, it can be shown definitively who entered the building and accessed the account.

It's hard to put a figure on this kind of security power, but Duemling states unequivocally that HPE ArcSight's total cost of ownership more than justifies the purchase price. "I think if you do an analysis, as we did, there are many compelling advantages to this solution," he says. "The ease of deployment, the technical proficiency of HPE ArcSight, its ability to expand and grow with the environment, the ability to manage the solution without hiring dedicated staff—these factors convinced us that this best-of-breed technology delivers the most for the money we spent."

In terms of enabling the business, HPE ArcSight's ease of use frees up resources for use elsewhere at Lake Health. "It basically prevents us from having to say, 'In order to perform our compliance-related tasks, we will need three more full-time equivalents, or FTEs, at a certain price point," says Duemling. "It allows that budget to be used for more nurses and doctors on the floor. Even with a very small staff, we can keep the systems up and providing the highest quality of data to those clinicians, so Lake Health patients get the best care possible."

HPE ArcSight also helps Lake Health maximize its investment in existing technology. Continues Duemling: "We integrate HPE ArcSight into existing and new technology, including other competing and complementary products that feed events and information into the solution. HPE ArcSight is our one true source for situational awareness.

We let all the other technologies do what they are best at, and then we let HPE ArcSight do what it is best at, which is bringing everything together and displaying it in an actionable format."

Focus on patient experience

Lake Health uses HPE ArcSight not just to detect security events, but also to improve performance. Says Duemling: "The visibility we gain with HPE ArcSight helps us fix things that we don't even know are broken—except our patients know that they're broken, because they might be getting substandard service as an indirect result, or they are trying to use a wireless access point that is malfunctioning. This type of event is flagged as an anomaly in the HPE ArcSight system, so we can investigate it immediately. HPE ArcSight makes an important contribution to improving the experience of our patients."

On the rare occasions when he has a few minutes to relax, Duemling likes to have fun with HPE ArcSight. "It's the non-management part of me, the old technical person coming back out," he says. "There are times when I'll pull up an HPE ArcSight dashboard and learn things about our network that I never knew existed, just by going off on a tangent. For example, I've learned that if you don't configure iPads correctly, they will authenticate a large number of times to your email server. That would never show up on a security report, so it's something I didn't know until I actually was digging through the dashboard one day."

Fun aside, the overriding benefit of HPE ArcSight at Lake Health comes from its powerful monitoring capability. Concludes Duemling: "It's the ability to see what would be impossible to see if you didn't have HPE ArcSight—the millions of events per year that you would be inundated with if you had to go through them manually. Before implementing this solution, I could not identify and address anomalies in a timely manner. Now I can provide answers virtually in real time, and also use the tool to proactively improve security and performance."

Learn more at
hpenterprisesecurity.com/

Sign up for updates

Hewlett Packard Enterprise

4AA4-4995ENW, July 2016, Rev. 1