CASE STUDY

# InfoTeK and Splunk Deliver Security Intelligence Platform for Public Sector Customer

## Executive summary

Many organizations depend on security information and event management (SIEM) software to monitor, investigate and respond to security threats. But at one U.S. government agency its mission was hampered when its legacy SIEM software from HP ArcSight failed to live up to expectations. The agency turned to InfoTeK, a leading cybersecurity, software and systems engineering firm, to replace its SIEM tool. Since deploying the Splunk platform, the customer has seen benefits including:

- Deploying in one weekend and stopping an attack the next day
- Achieving a 75 percent cost reduction to support its SIEM
- Reducing number of tools required, including log aggregators and endpoint solutions

## Why Splunk

“At InfoTeK, we live by the motto ‘imagine, inspire and innovate,’” says Jonathan Fair, senior incident handler and security engineer at InfoTeK. “Our goal is to provide imagination for customers, give them the inspiration they need to push forward, and then innovate to come up with a solution that will not just meet the need, but will go above and beyond to truly transform their environment.”

That was certainly the case with this agency. Despite using ArcSight, as well as several other tools, it was difficult to glean actionable intelligence about threats. Identifying anomalies that could indicate vulnerabilities or an attack in progress required seasoned security engineering skills—and even for them, it was a time-consuming puzzle.

Gaining insight wasn’t the only issue: as the volumes of data that needed to be searched and analyzed grew considerably, its legacy SIEM simply couldn’t keep pace. Scaling performance meant more hardware and more expense.

## Delivers immediate value

With Splunk Enterprise and Splunk Enterprise Security (ES), the agency has an analytics-driven SIEM that provides the IT team with actionable security intelligence at an affordable cost. InfoTeK deployed Splunk software over one weekend for the customer. Starting the very next day, the software proved its value. The IT team was able to search security events and immediately thwarted an attack vector.

### Industry

- Public sector
- Technology services

### Splunk Use Cases

- Security
- IT operations

### Challenges

- Monitoring threats and responding to incidents was time-consuming and difficult
- Massive data sets impacted performance
- Needed to increase the efficiency and effectiveness of security operations
- Required many resources including costly hardware and engineering support

### Business Impact

- Analyzing massive data volumes to identify attacks in real time and respond rapidly to incidents
- Deploying in one weekend and stopping an attack the next day
- Achieving a 75 percent cost reduction to support the SIEM
- Reduced number of resources to manage ArcSight from two to one-half-time engineer

### Splunk Products

- Splunk Enterprise
- Splunk Enterprise Security
- Splunk IT Service Intelligence

"Something that used to take hours, days or even weeks with other products or jumping between multiple tools can be done in seconds, minutes or hours with Splunk," says Fair. "We were able to provide a ROI before the product was even fully purchased because the customer successfully stopped a threat that would have required a complete rebuild of the network."

## Scale without sweat

With Splunk, the agency has a security intelligence platform that can process massive amounts of machine data to reveal insights. "Splunk is the only product that we have found that has been able to truly take any data source and go to scale," says Fair. "We're talking anywhere from low volume—gigabytes a day—to high volume—terabytes a day—and provide a cost model that's less expensive."

The Splunk platform can ingest security data from the network layer, all the way down the endpoint. Administrators use a single pane-of-glass console that eliminates time wasted jumping between different tools. InfoTeK is also in early talks with the agency and other customers about how Splunk solutions can help transform IT monitoring and analytics.

"Splunk truly stretches across all data, and you can search across any data set at any time," says Fair. "An expanded view is necessary to truly look at an event, either in real time or for post-mortem analysis."

That scale is key as threats are increasingly evasive and hidden. "Sometimes you don't know what's important until you go look for it, and if you don't have all the information at hand, then you can't make a proper decision about the impact to the network," he says.

**"A platform is something that transcends. Splunk is truly a platform that is able to take in data from anything that's willing to give it data, and then you are also able to interact by pulling data out of the platform and using it elsewhere."**

Jonathan Fair, Security Incident Handler
InfoTeK

## Reduces costs with security intelligence

The agency's operational savings are significant. By moving to the Splunk platform, it has dramatically reduced the number of tools that IT staff need to manage, and it reduced the number of servers required to support the SIEM. Before, the agency needed two security engineers to manage ArcSight, and now only one engineer is needed—and he only spends one-half of his time managing the Splunk platform.

"From a hardware/software cost perspective, our analysis has led us to see a 75 percent cost difference to do the same implementation between ArcSight and Splunk," says Fair.

But in the end, while the biggest benefit is the actionable insight needed to stop cyberthreats faster, the agency now has a platform that can be used to make data-driven decisions not just in IT but for other business use cases. "Splunk is capable of doing anything," says Fair. "You really can do whatever you can imagine, and it provides complete visibility into the environment."

Download Splunk for free or get started with the free cloud trial. Whether cloud, on-premises, or for large or small teams, Splunk has a deployment model that will fit your needs.

splunk>

Learn more: www.splunk.com/asksales

www.splunk.com