splunk> turn data into doing™

CASE STUDY

Transforming Intel's Security Posture With Innovations in Data Intelligence

Key Challenges

Intel needed to shift to a data-centric business model that increased data's value while decreasing its vulnerability.

Key Results

With Splunk® and Apache Kafka as its foundation, the Cyber Intelligence Platform (CIP) delivers full visibility into Intel's InfoSec organization, which has transformed information security management.

Industry: Technology

Solutions: Security, IT Operations

Turning Data Into Outcomes

- Speeds data analysis and detects sophisticated threats in minutes or hours, versus days or weeks
- Delivers a collaborative, unified approach to managing cybersecurity
- Provides streams processing and machine learning tools that deliver business value in additional areas, such as security operations and system health

It would be difficult to overestimate the impact and importance of Intel's technology contributions on society.

The company's engineering expertise is helping secure, power and connect billions of devices and the infrastructure of the smart, connected world. Over time, Intel has changed from a PC-centric company to a data-centric company. The company is developing new products, entering new markets and engaging new customers in innovative ways.

"Data is everything; data is king. It's powering our business; it's powering everything," says Brent Conran, chief information security officer at Intel. "It's transforming traditional industries and born-in-the-cloud industries. The ability to gain insights from data is the difference between a successful business or one that falls away."

This greater emphasis and reliance on data required Intel's Information Security (InfoSec) organization to build and maintain a comprehensive "defense-in-depth" strategy. The team automated prevention and detection tools at many levels — including the perimeter, network, endpoints, applications and data layer — to handle 99% of threats across Intel's environment.

Hunting the One Percent

Advanced threats continue to grow in frequency and sophistication. And the organization was burdened with a legacy SIEM that no longer met the needs of the organization. Only a handful of experts knew how to use this legacy SIEM, which couldn't scale with the ever-increasing demand for more types of data.

Intel InfoSec needed a strategy to detect sophisticated threats attempting to penetrate the organization's environment — what Intel InfoSec calls hunting the one percent. This strategy inspired Intel's Cyber Intelligence Platform (CIP), which is centered on leading-edge technologies, including Splunk and Apache Kafka. With high-performance servers based on Intel® Xeon® Platinum

processors, Intel 3D NAND Solid State Drives (SSDs) and Intel® Optane™ SSDs, the new CIP platform ingests over 12 terabytes of data per day and stores 15 petabytes of data. The data flows from hundreds of sources to a Kafka message bus, then into the Splunk platform, where users perform over 1.3 million searches per week.

With the Splunk Data-to-Everything Platform and hundreds of third-party tools, the InfoSec organization now has context-rich visibility and a common work surface, which improves the effectiveness of the entire InfoSec organization. The team now detects and responds to threats within hours or minutes — compared to weeks or hours previously.

Scaling Intel's Cyber Intelligence Platform

CIP's results led to additional data sources, new use cases and many more data models. Soon, use of the CIP expanded to teams like vulnerability management, compliance and enforcement, risk management and beyond, which placed additional demands on the infrastructure while requiring even faster compute and storage. To maximize the platform's performance, Intel's security solution architect and engineers needed a deeper understanding of the Splunk platform and Intel technologies.

> Data is everything; data is king. … It's transforming traditional industries and born-in-the-cloud industries. The ability to gain insights from data is the difference between a successful business or one that falls away."
>
> **Brent Conran,** Chief Information Security Officer

A collaborative Splunk and Intel team developed a joint reference configuration to help guide CIP's expansion across compute, memory and storage using the latest Intel products and technologies. Splunk and Intel are now sharing their success with IT peers, helping others scale their Splunk and Apache Kafka deployments to more effectively convert raw data into operational, business and security intelligence.

> We see the potential, and because we see the potential, we're investing time, energy and resources. We want Splunk to be successful because we think it will help us fulfill our mission.
>
> **Brent Conran,** Chief Information Security Officer

Providing Value for Today and Tomorrow

Intel's InfoSec team is expanding its use of Splunk and Kafka. The analysts and data scientists are transforming, enriching, joining, filtering and operating on data in stream. The team is also adding more machine learning tools for everything from incident response, operations and system health to workflow orchestration and alerts. In collaborating with Splunk, Intel is unlocking value for today and tomorrow.

"Intel Information Security is much more agile than we've ever been in the past," says Conran. "We put in a brand-new Splunk data lake, and we modernized our tools. By putting data in the right place and reskilling our people, we created a force multiplier. We are using machine learning to significantly increase the depth and speed of our cyber intelligence."

20-14330-TransformingIntelsSecurityPostureWithInnovationsinDataIntelligence-104-Tie2-CS