Transforming Intel's Security Posture With Innovations in Data Intelligence

Executive Summary

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. Equally difficult to overestimate would be the significance of secure data as an organization's most protected asset.

With Splunk® and Apache Kafka as its foundation, Intel IT developed a new Cyber Intelligence Platform that is transforming its approach to information security by:

- Speeding data analysis and reducing time to detect and respond to advanced threats
- Enabling a collaborative organization with a common language and work surface
- Providing streams processing and machine learning tools that deliver business value in additional areas, such as security operations and system health

Data is everything

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®

Industry

- Technology

Splunk Use Cases

- Security
- Cybersecurity Incident Response Management
- Security Monitoring
- Application Monitoring

Challenges

- Shift to a data-centric business model increases data value, but also vulnerability
- Legacy SIEM no longer fit for purpose
- Multiple, disconnected data siloes and teams delivering different data analysis interpretations

Business Impact

- Transformed information security management and control
- Detects sophisticated threats in minutes or hours, versus days or weeks
- Delivers a collaborative, unified approach to managing cybersecurity
- Delivers a cyber intelligence platform for Intel's entire InfoSec organization

Splunk Products

- Splunk Enterprise
- Splunk Enterprise Security
- Splunk IT Service Intelligence (ITSI)
- VictorOps
- Splunk Mission Control

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 Splunk's 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.

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, Intel

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."

> **"We built CIP to handle tens, and eventually hundreds, of terabytes of data per day, and to support hundreds of users building ad hoc searches, scheduled searches, data model accelerations and machine learning models. To be performant at scale, we needed servers with Intel's Xeon Scalable processors and Intel SSDs for high-performance compute and storage. Seconds matter when your mission is 'make it safe for Intel to go fast.'"**
>
> — Jac Noel, Security Solution Architect, Intel

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