RSA®Conference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

Modernizing the Security Operations Center: A Security Leader Panel

MODERATOR: **Kaela Sullivan**
Customer Marketing Manager
Splunk

PANELISTS: **Oliver Friedrichs**
VP, Security Products
Splunk

Jac Noel
Security Solution Architect
Intel

Lee Peterson
Manager of Global Cybersecurity
Engineering
Starbucks

#RSAC

Meet Your Panelists

Oliver Friedrichs

VP, Security Products,
Splunk

Lee Peterson

Manager of Global
Cybersecurity
Engineering, Starbucks

Jac Noel

Security Solution
Architect

How do you see deployment models for security operations technologies changing?
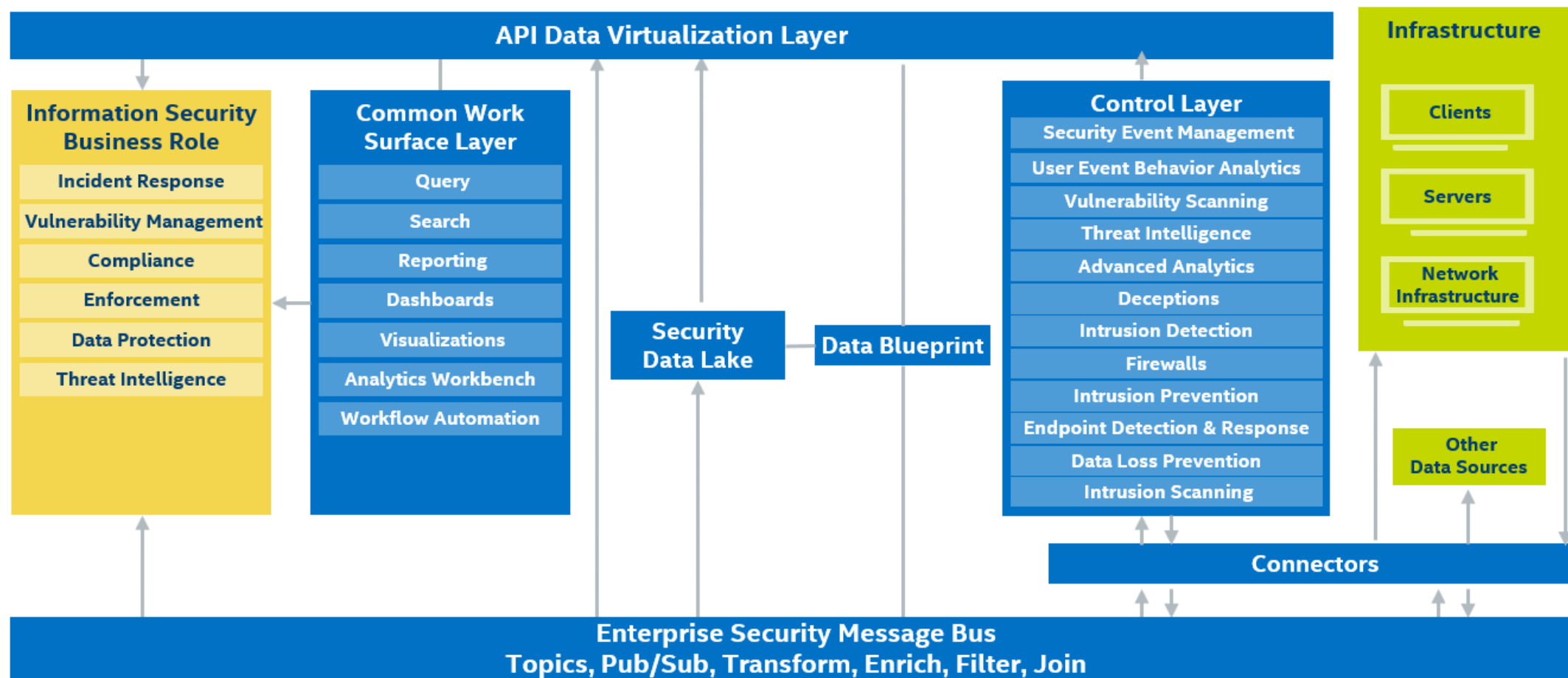
And what role will *cloud* play in the future?

Describe the current security posture over at Starbucks

How did Intel transform their security posture?

Reference Architecture
A platform that supports the entire organization

API Data Virtualization Layer

Infrastructure

- Clients
- Servers
- Network Infrastructure

Information Security Business Role
- Incident Response
- Vulnerability Management
- Compliance
- Enforcement
- Data Protection
- Threat Intelligence

Common Work Surface Layer
- Query
- Search
- Reporting
- Dashboards
- Visualizations
- Analytics Workbench
- Workflow Automation

Security Data Lake

Data Blueprint

Control Layer
- Security Event Management
- User Event Behavior Analytics
- Vulnerability Scanning
- Threat Intelligence
- Advanced Analytics
- Deceptions
- Intrusion Detection
- Firewalls
- Intrusion Prevention
- Endpoint Detection & Response
- Data Loss Prevention
- Intrusion Scanning

Other Data Sources

Connectors

Enterprise Security Message Bus
Topics, Pub/Sub, Transform, Enrich, Filter, Join

splunk> listen to your data

RSAConference2020

How has automation in the industry helped tackle
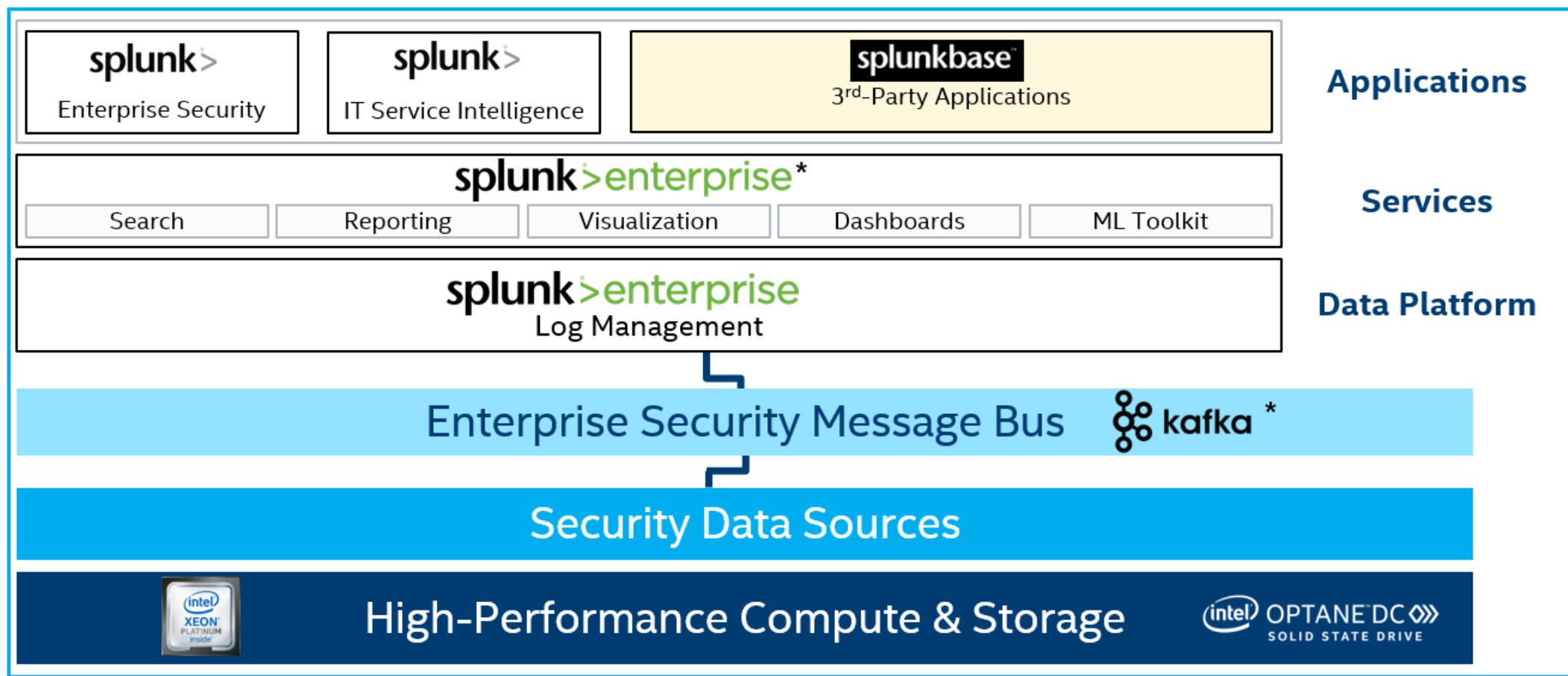high volume tasks?

How is Starbucks utilizing SOAR?

How important is reducing complexity within the SOC?

Can you explain Intel's Cyber Intelligence Platform Infrastructure?

How has the common work surface been beneficial to your team at Intel?
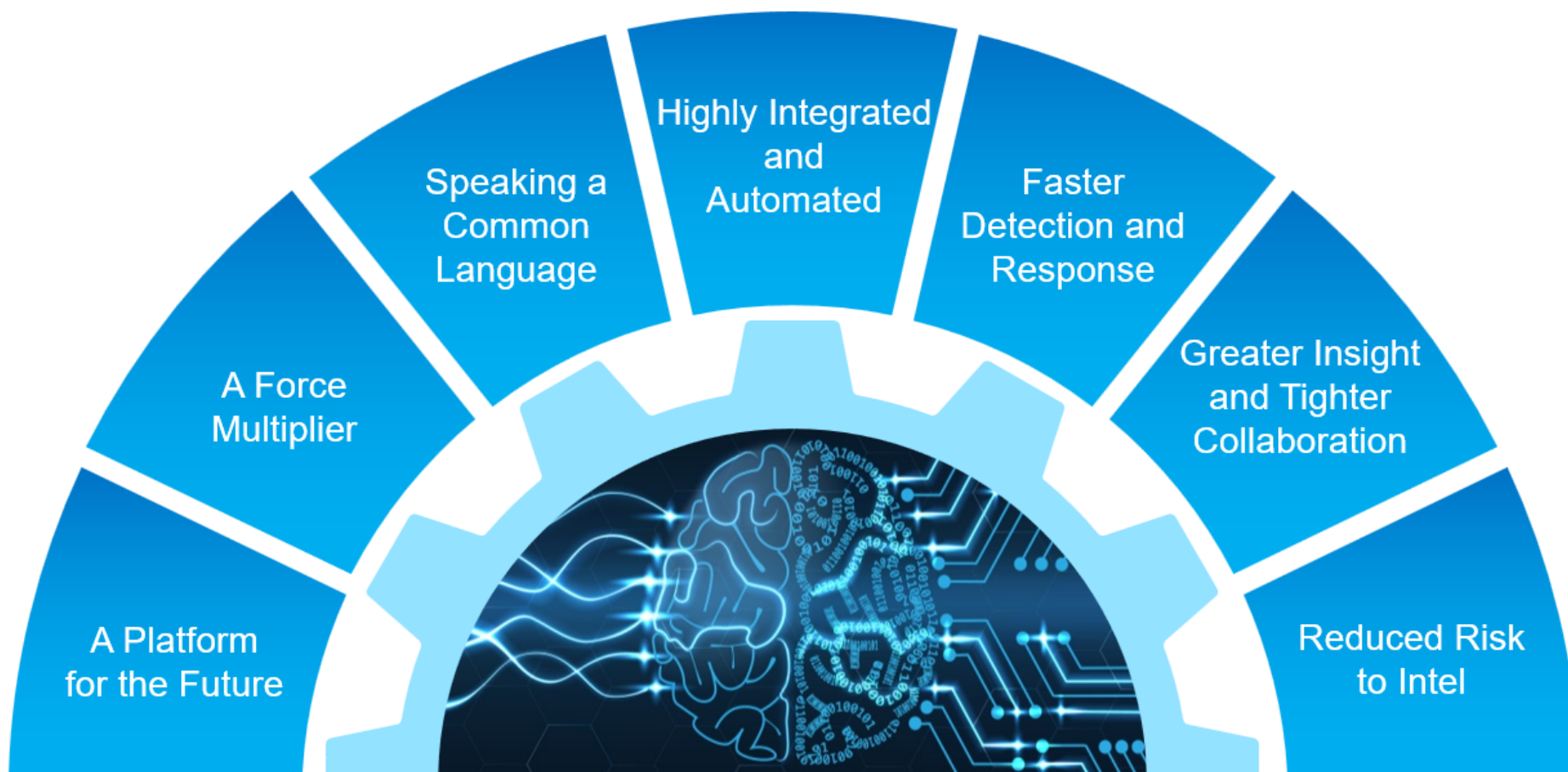
As the volume of data has grown over the years, how have your organizations handled this issue?

How have you seen the skill shortage in the industry affect your security efforts?

Given the skills gap, is it challenging to staff your SOC 24x7?

Do we need a cultural change to shrink the gap in skill shortages?