RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: SPO1-T06

Cybersecurity Silo-Busters: 1
Cyberthreat Actors: 0

Sridhar Muppidi

IBM Fellow and CTO
IBM Security

Devin Somppi

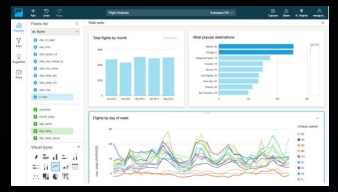
Lead of Security Operations
BriteSky, Enterprise Cloud Provider

BriteSky
Enterprise Cloud Provider™

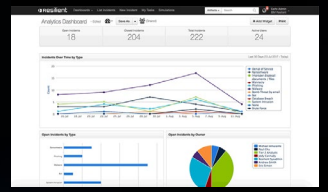
Enterprise Cloud. Simplified.

Threat operations at BriteSky

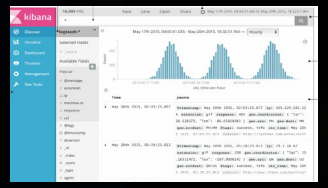
Flight Analysis



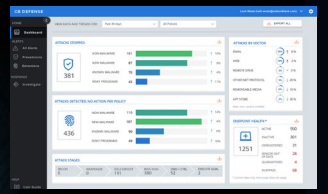
Incident Response



TIP

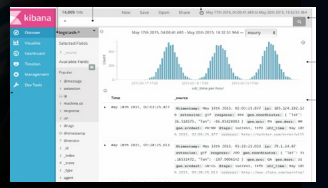


Endpoint Security

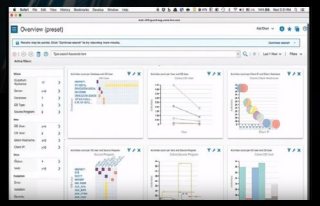


SIEM

Cloud Storage



Threat Management



Data Security

Cybersecurity is a universal challenge

What's at stake…

20.8 billion
things we need to secure

5 billion
personal data records stolen

$6 trillion
lost to cybercrime over the next 2 years

What we face…

Compliance updates

GDPR fines can cost
billions
for large global companies

Skills shortage

By 2022, there will be
1.8 million
unfulfilled cybersecurity jobs

Too many tools

Organizations are using
too many
tools from too many vendors

Data integration: a barrier to getting value from security data

55%

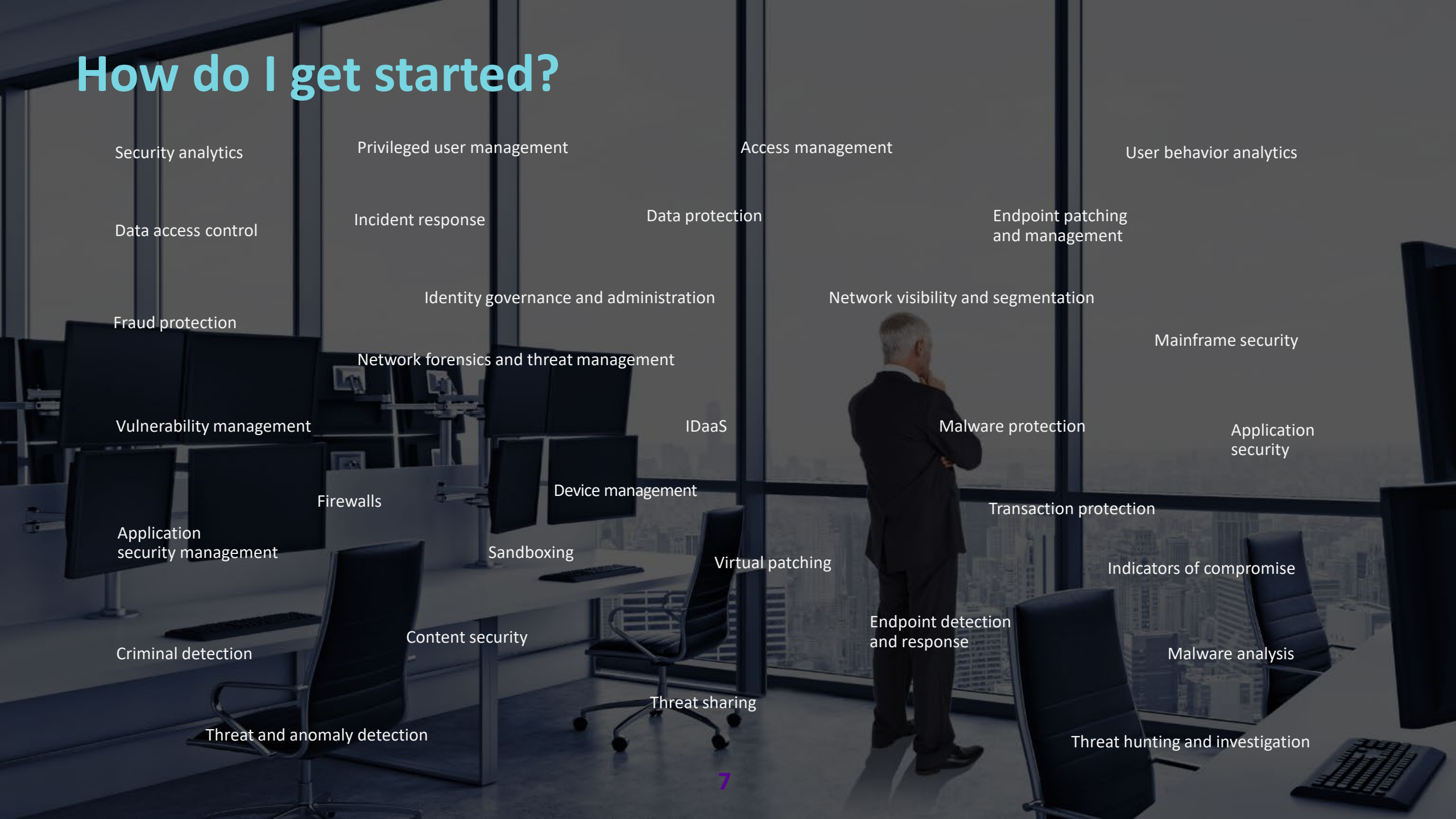
Time consuming, complex data integration processes limit which data sources we can ingest.

Source: IBM Security Research

Simplifying security can have meaningful impact

Source: Forrester Research

How do I get started?



Drive collaboration by breaking siloes

1. Gain total insights for all data, wherever it resides
2. Respond more quickly, with unified experiences
3. Improve security posture with collective intelligence

The future of security is connected

Catalog

Applications | Solutions | Services

from Vendors, Partners, Clients, etc.

Cloud Platform

Open Threat & Data Integration

AI and Analytics

Orchestration

Existing Infrastructure

On-premises security tools and infrastructure

Public and private clouds

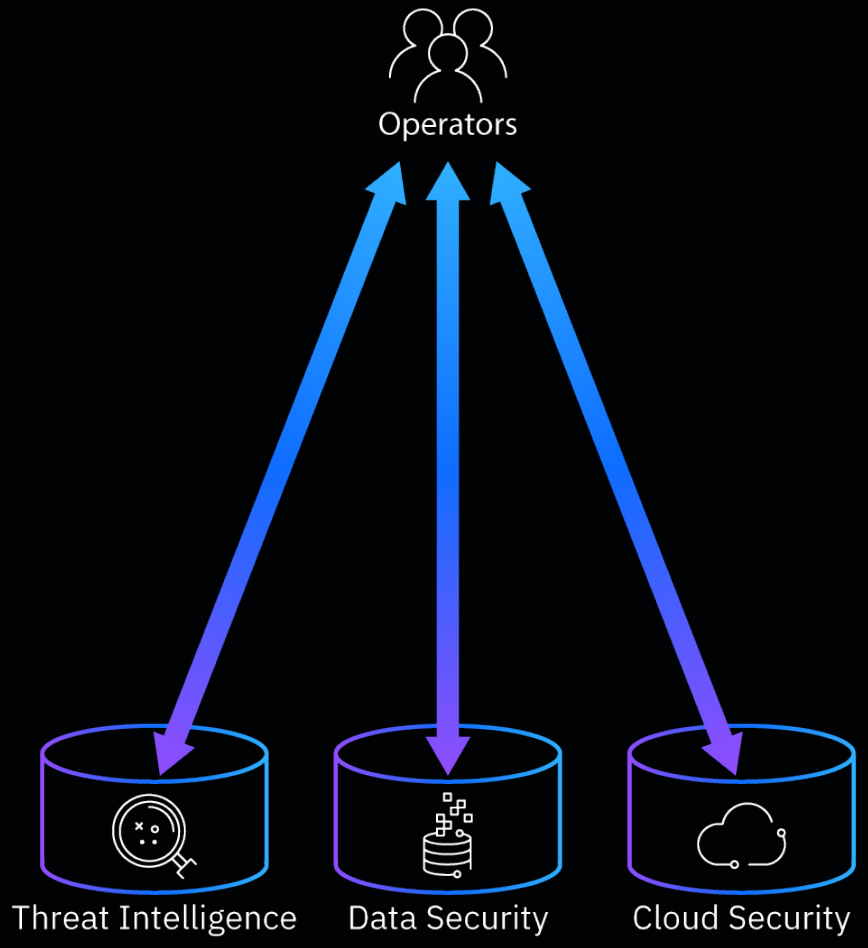
Mobile devices and endpoints

RSAConference2019

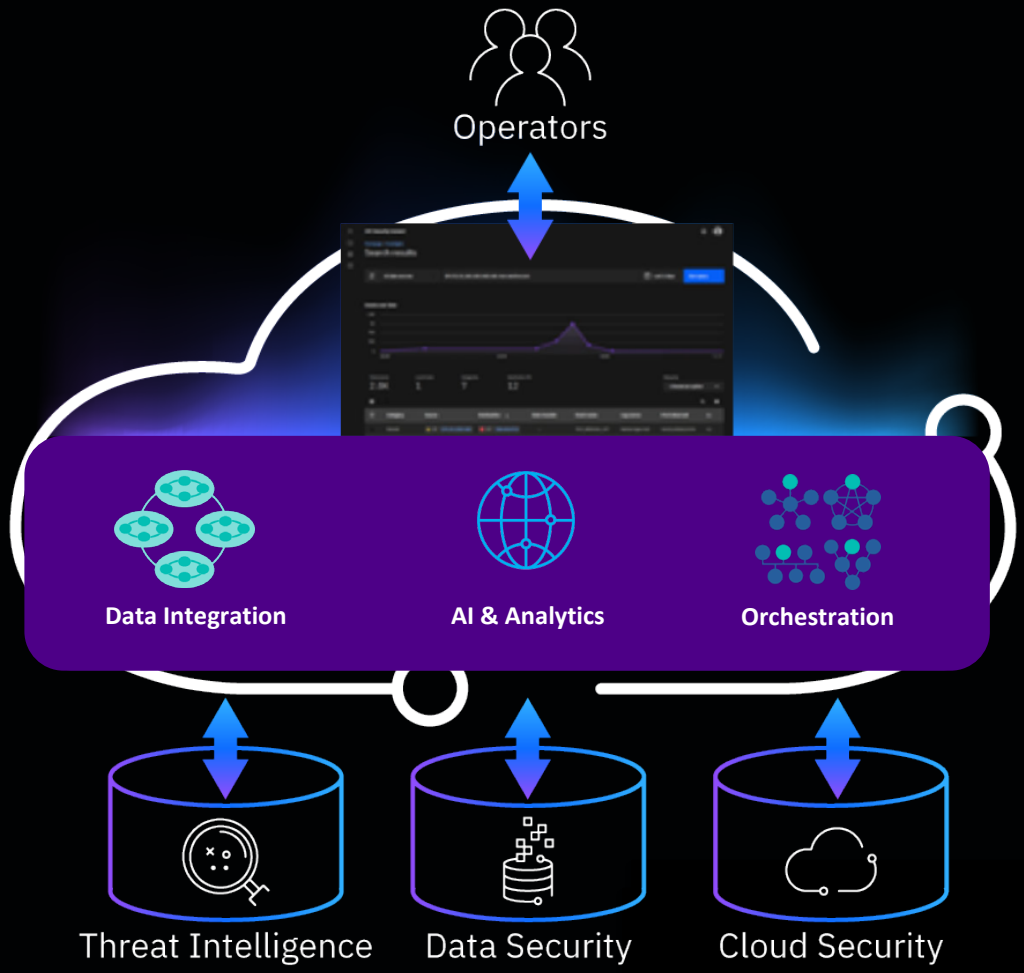
Use Case: Responding to Threats

Threat operations: respond effectively

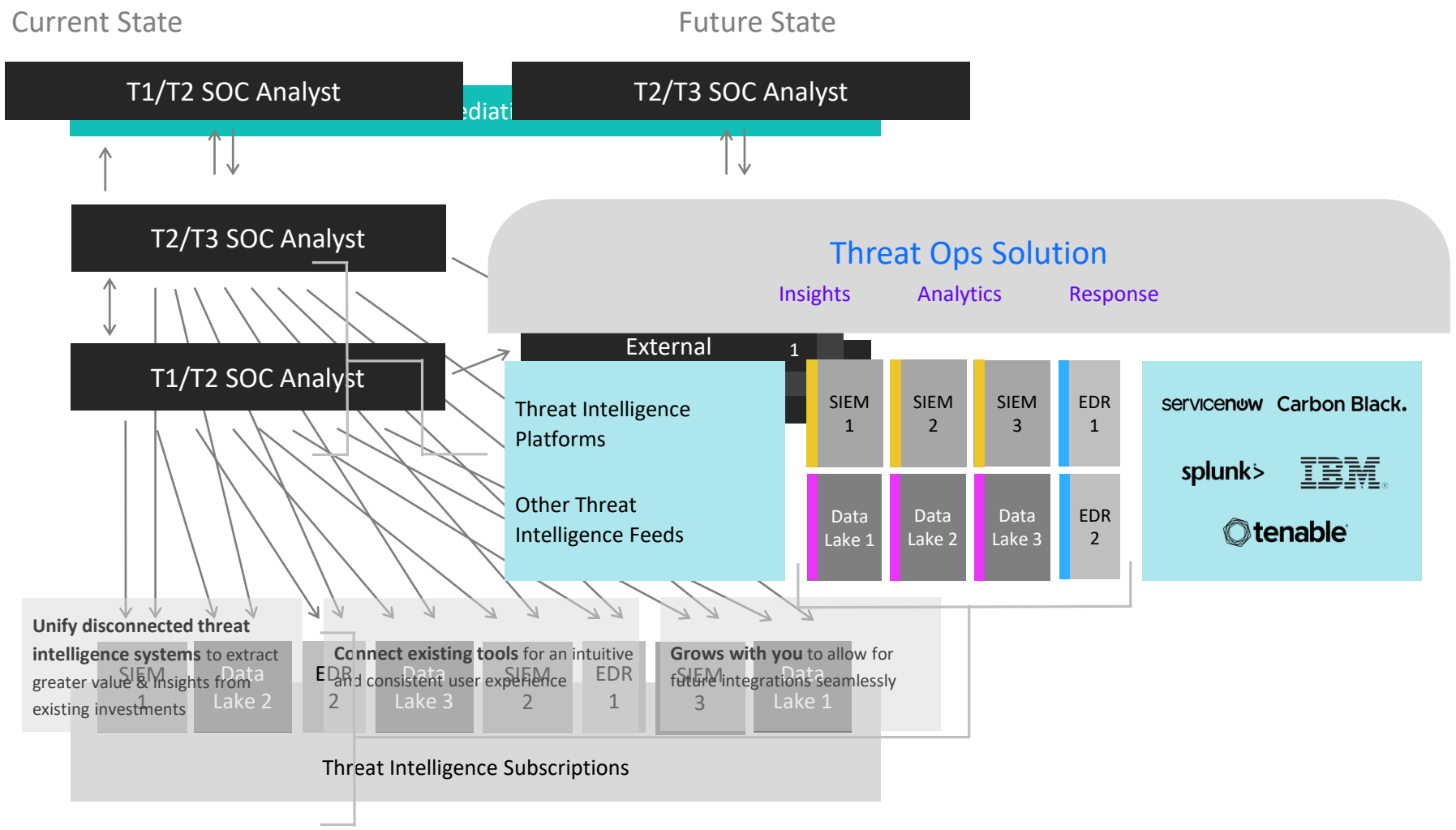
Siloed applications hamper workflow & result in missed context due to isolated analytics



Connected applications, on a common platform, sharing analytics, context and enhancing each other



Threat Ops: SOC integration



SOC Analysts correlate data from **multiple disparate, isolated products**, conduct investigations **across various tools**, and respond with **inefficient processes**.

Re-thinking security analysts' roles

Change analysts' roles:

- Do I still need Level 1, 2 and 3?
- Can I reduce on-boarding time and time to action for analysts?
- Can I expand the hiring pool for analysts?

Expand offering; look at more data sources

Protect consumers efficiently

Break out of your siloes to discover what's possible

Better Value | Faster Response | Easier UX

IBM, Cisco, Capgemini, Carbon Black, Check Point, CrowdStrike, EY, ForeScout, Forcepoint, Fortinet, McAfee, Qualys, Smarttech, Symantec, tenable network security, Trend Micro, vmware, aws, Azure, splunk>

Start innovating!

Join in the endeavor to turn security into a team sport:

- Start busting data siloes
- Collaborate and demand open tools
- Visit IBM, Booth **#N5759** to learn how to begin your journey

RSAConference2019

Thank you!