RSAConference2019
San Francisco | March 4 – 8 | Moscone Center

BETTER.

SESSION ID: SPO1-T06

Cybersecurity Silo-Busters: 1
Cyberthreat Actors: 0

Devin Somppi

Lead of Security Operations
BriteSky, Enterprise Cloud Provider

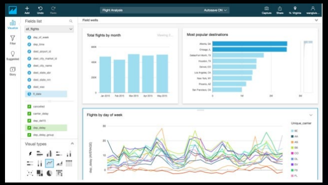
Sridhar Muppidi

IBM Fellow and CTO
IBM Security

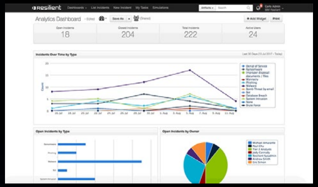
BriteSky: Enterprise Cloud. Simplified.

Threat operations at BriteSky Enterprise Cloud Provider

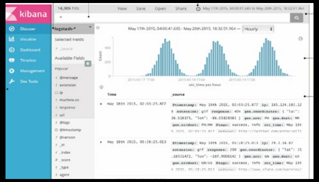
Flight Analysis



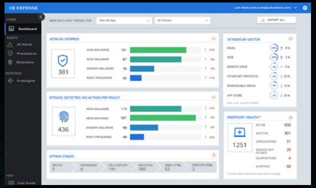
Incident Response



TIP

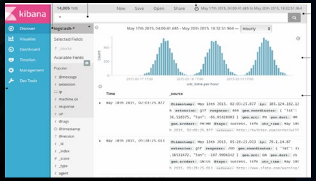


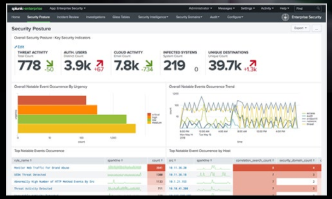
Endpoint Security



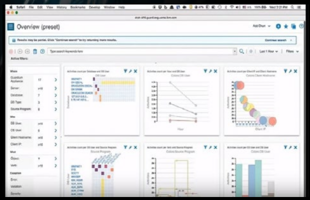
SIEM

Cloud Storage

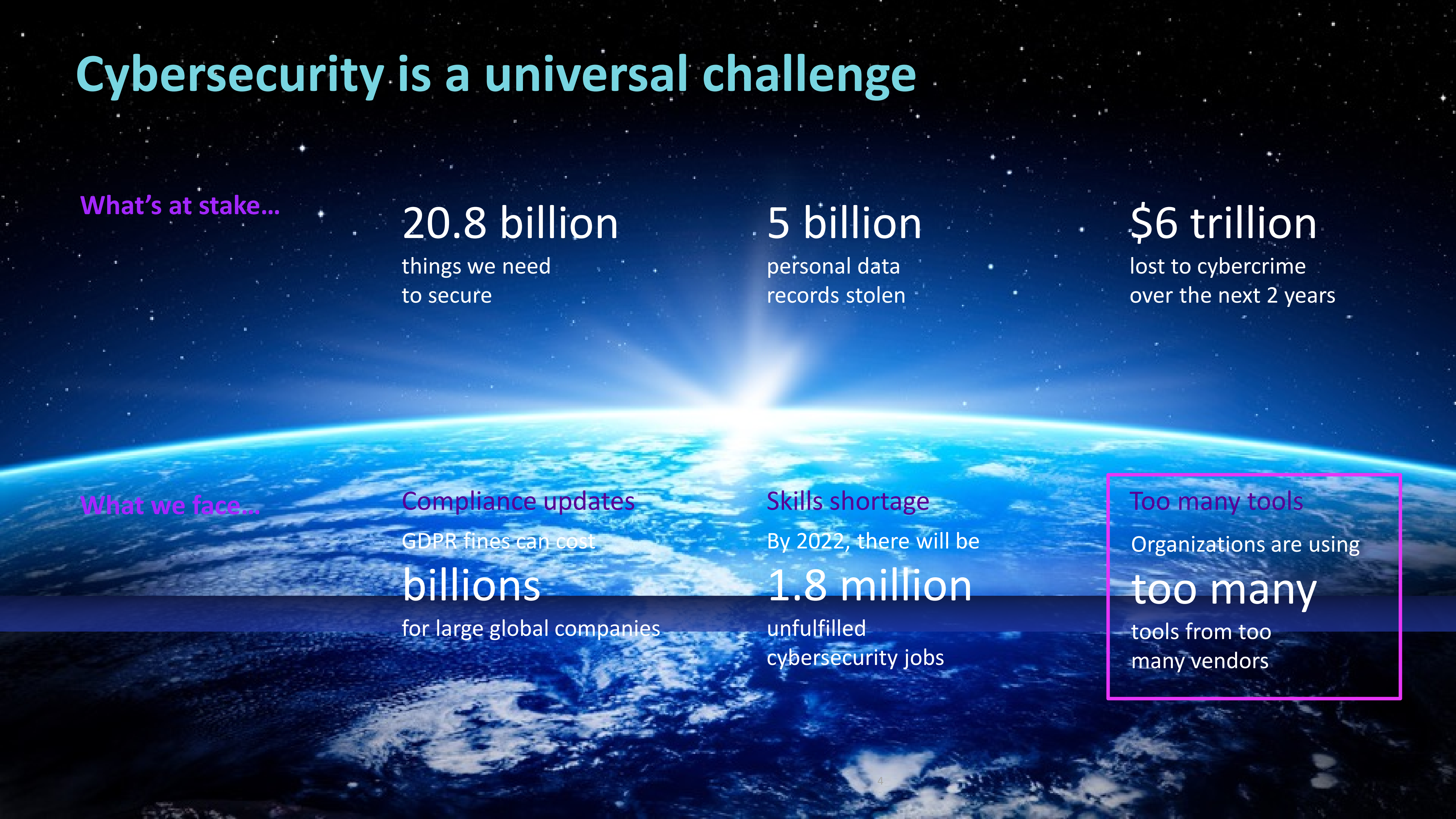




Threat Management



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

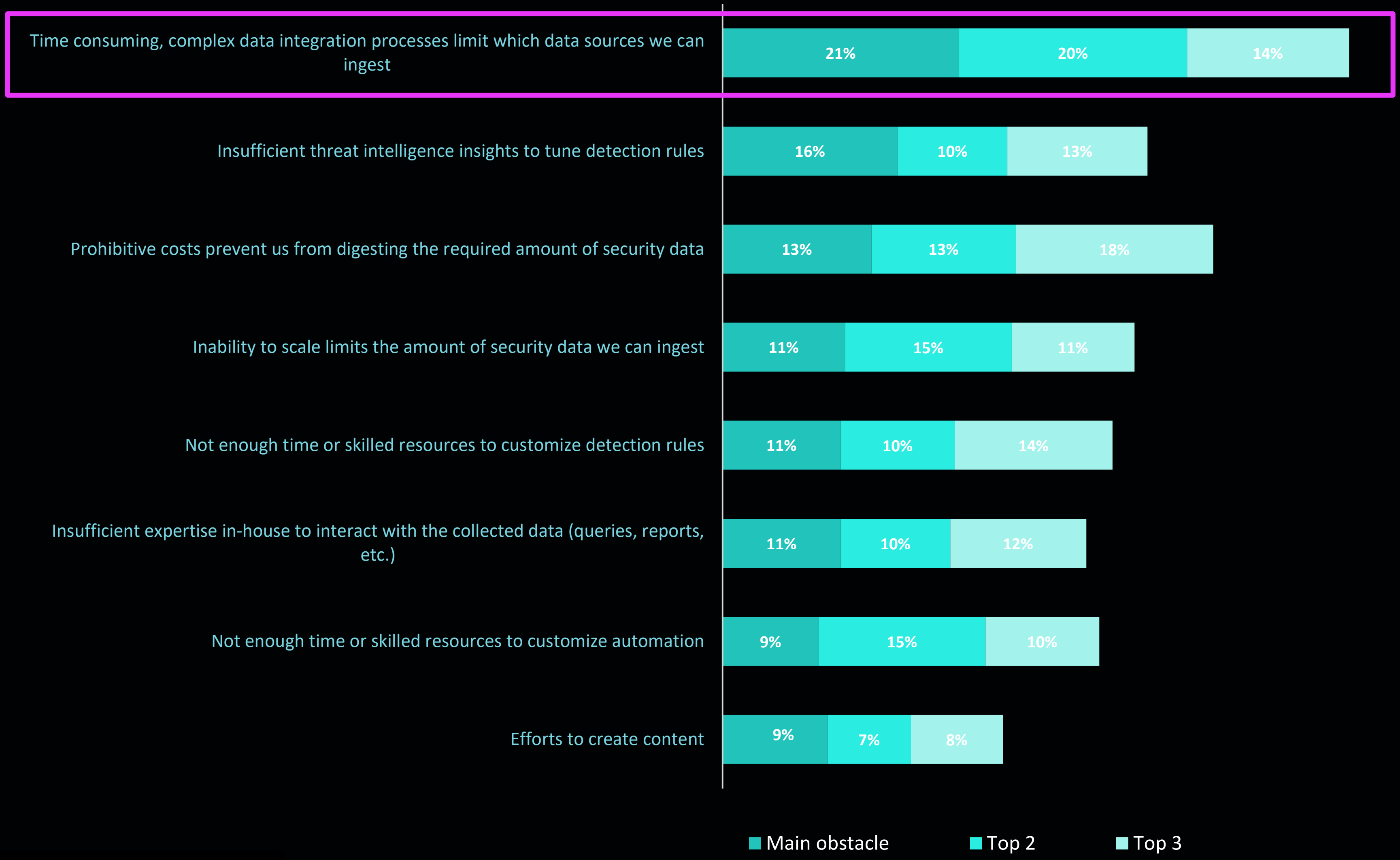
Skills shortage

By 2022, there will be
1.8 million
unfulfilled
cybersecurity jobs

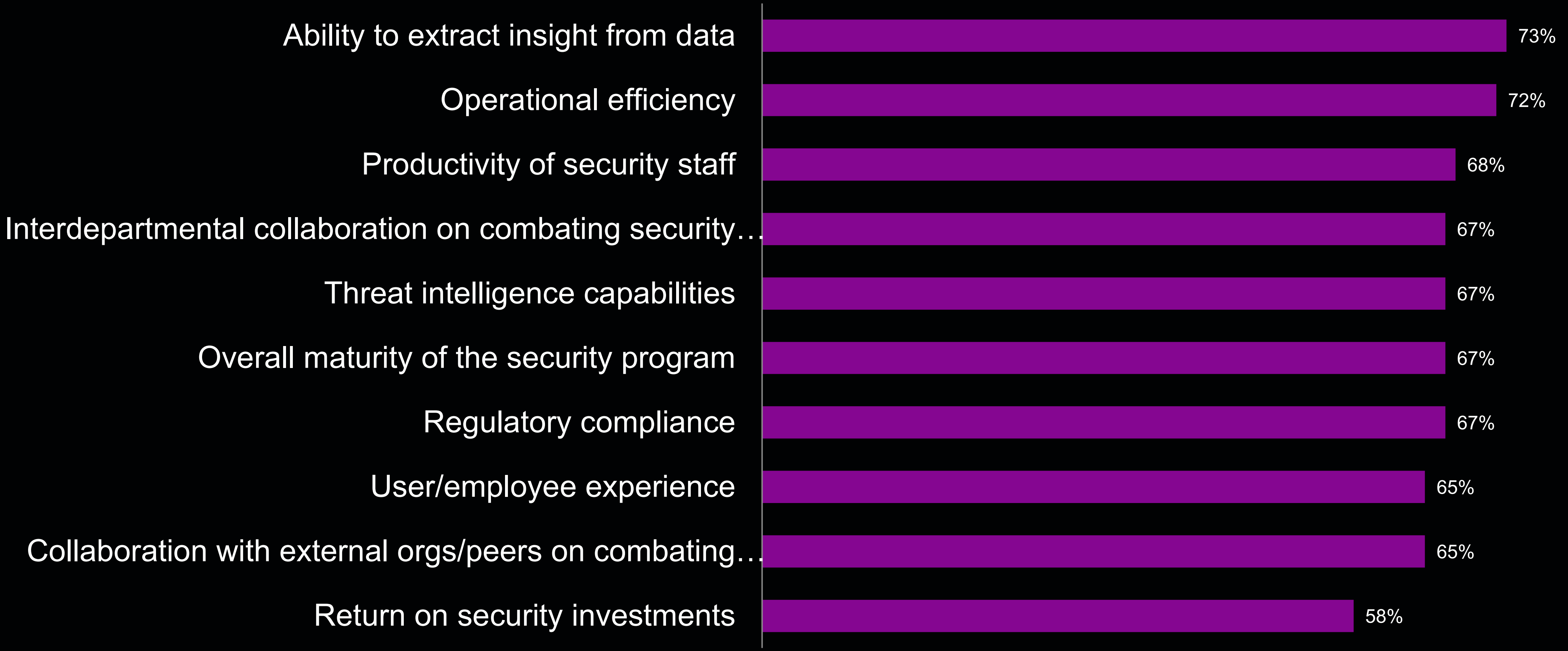
Too many tools

Organizations are using
too many
tools from too
many vendors

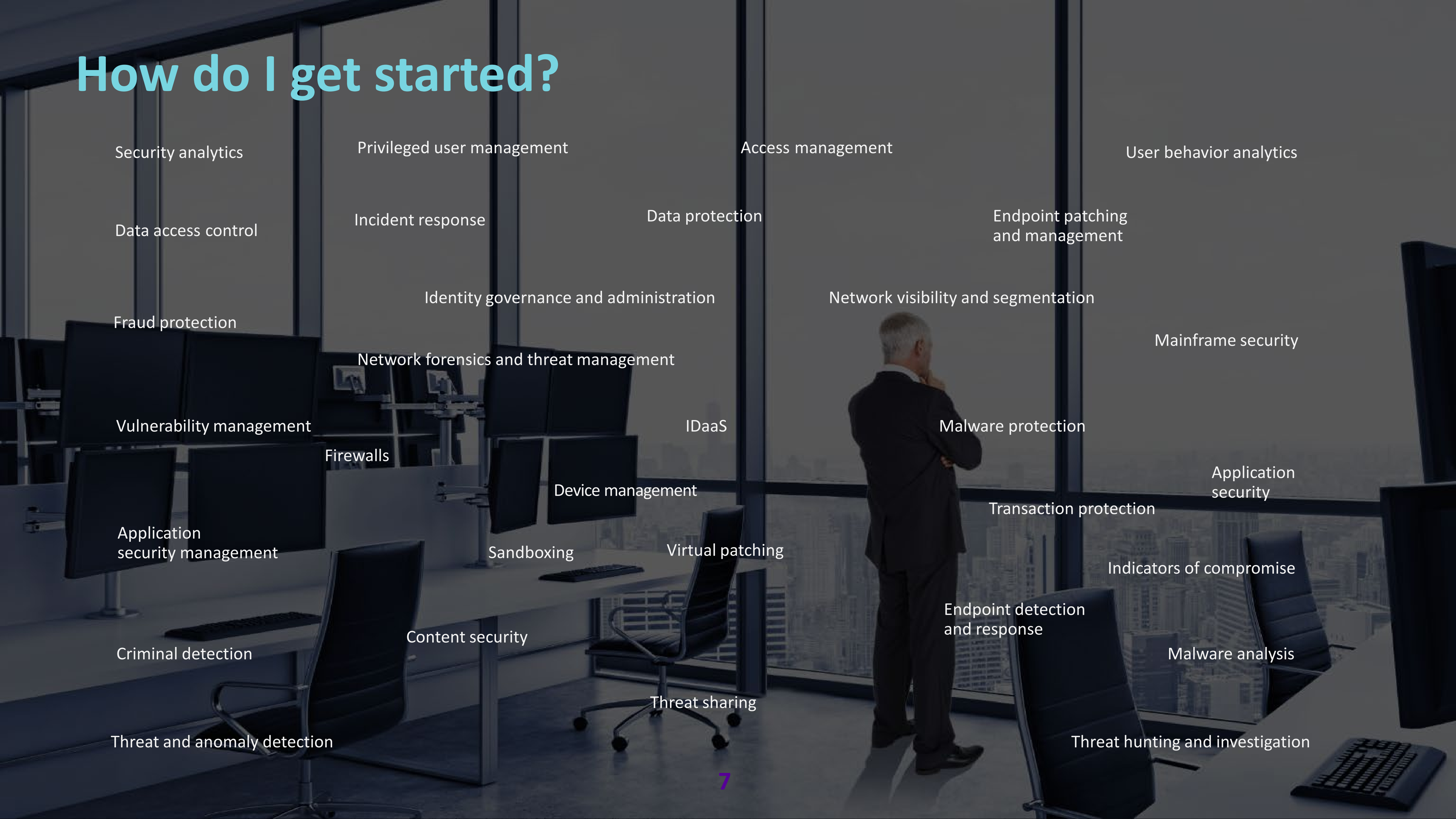
Data integration: a barrier to getting value from security data



Simplifying security can have meaningful impact



How do I get started?



Security analytics

Privileged user management

Access management

User behavior analytics

Data access control

Incident response

Data protection

Endpoint patching and management

Identity governance and administration

Network visibility and segmentation

Fraud protection

Mainframe security

Network forensics and threat management

Vulnerability management

IDaaS

Malware protection

Firewalls

Application security

Device management

Transaction protection

Application security management

Sandboxing

Virtual patching

Indicators of compromise

Endpoint detection and response

Content security

Criminal detection

Malware analysis

Threat sharing

Threat and anomaly detection

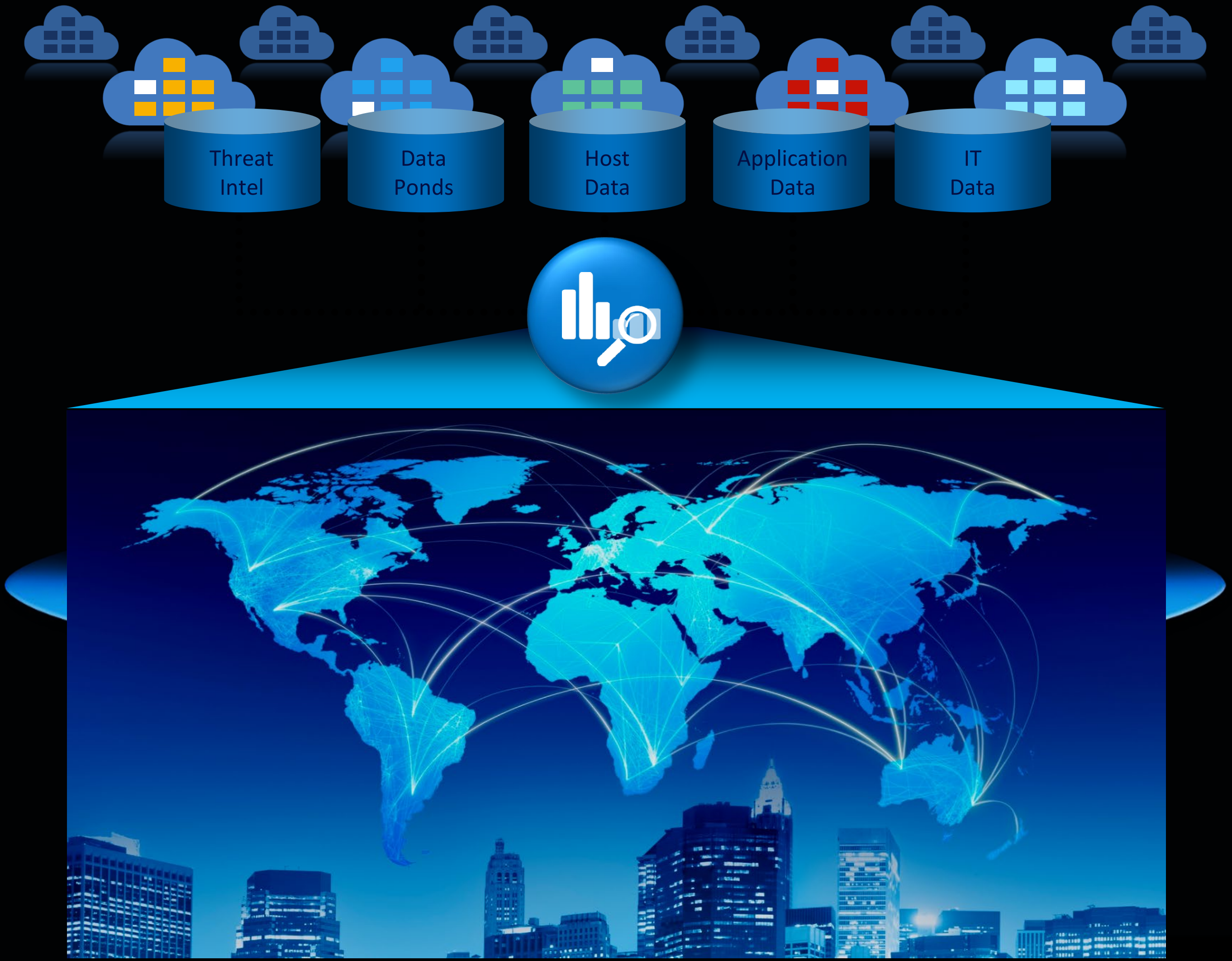
Threat hunting and investigation

Drive collaboration and outcome-based security

1. Gain total insights for all data, wherever it resides

2. Respond more quickly, with unified experiences

3. Improve security posture with collective intelligence



Drive outcome-based security

Catalog

Applications | Solutions | Services

from Vendors, Partners, Clients, etc.

Cloud Platform

AppDev Framework

AI and analytics

Open Threat & Data Integration

Existing infrastructure

On-premises security tools and infrastructure

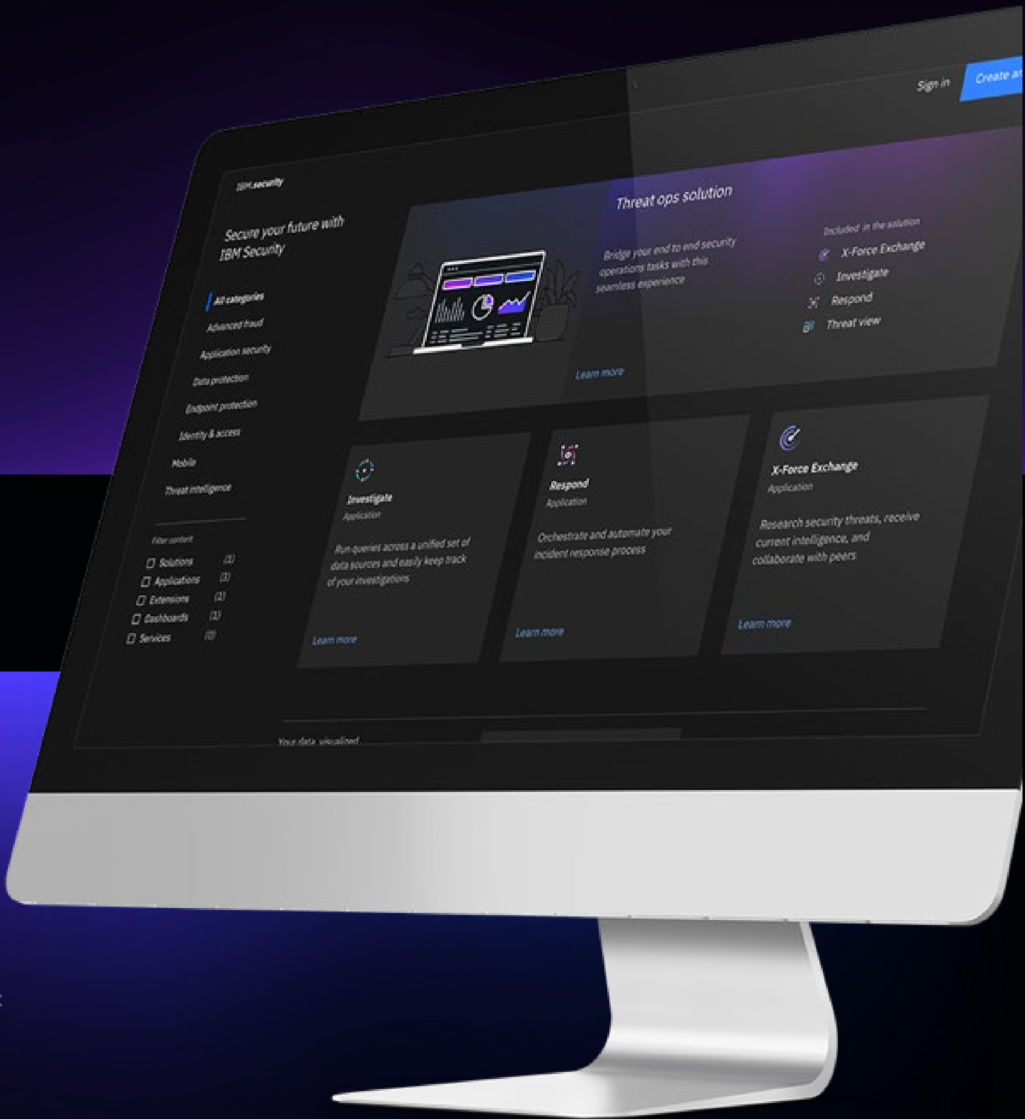
Public and private clouds

Mobile devices and endpoints

IBM ArcSight splunk> McAfee paloalto NETWORKS

aws Azure vmware cisco CROWDSTRIKE Carbon Black. Symantec

Capgemini CONSULTING.TECHNOLOGY.OUTSOURCING Cognizant Deloitte. QUALYS CONTINUOUS SECURITY tenable network security



Sign in

Create a

IBM security

Secure your future with IBM Security

Threat ops solution

Bridge your end to end security operations tasks with this seamless experience

Included in the solution

X-Force Exchange

Investigate

Respond

Threat view

Learn more

All categories

Advanced fraud

Application security

Data protection

Endpoint protection

Identity & access

Mobile

Threat intelligence

Filter content

- ☐ Solutions (1)
- ☐ Applications (3)
- ☐ Extensions (1)
- ☐ Dashboards (1)
- ☐ Services (0)

Investigate
Application

Run queries across a unified set of data sources and easily keep track of your investigations

Learn more

Respond
Application

Orchestrate and automate your incident response process

Learn more

X-Force Exchange
Application

Research security threats, receive current intelligence, and collaborate with peers

Learn more

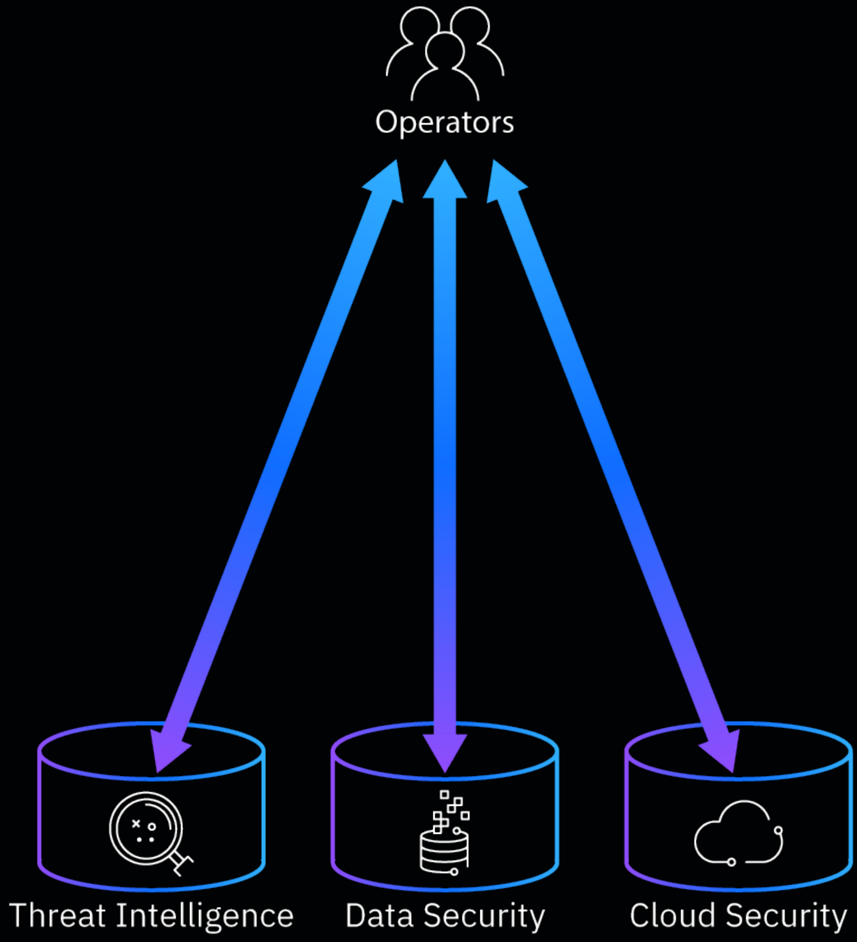
Your data, visualized

RSA Conference2019

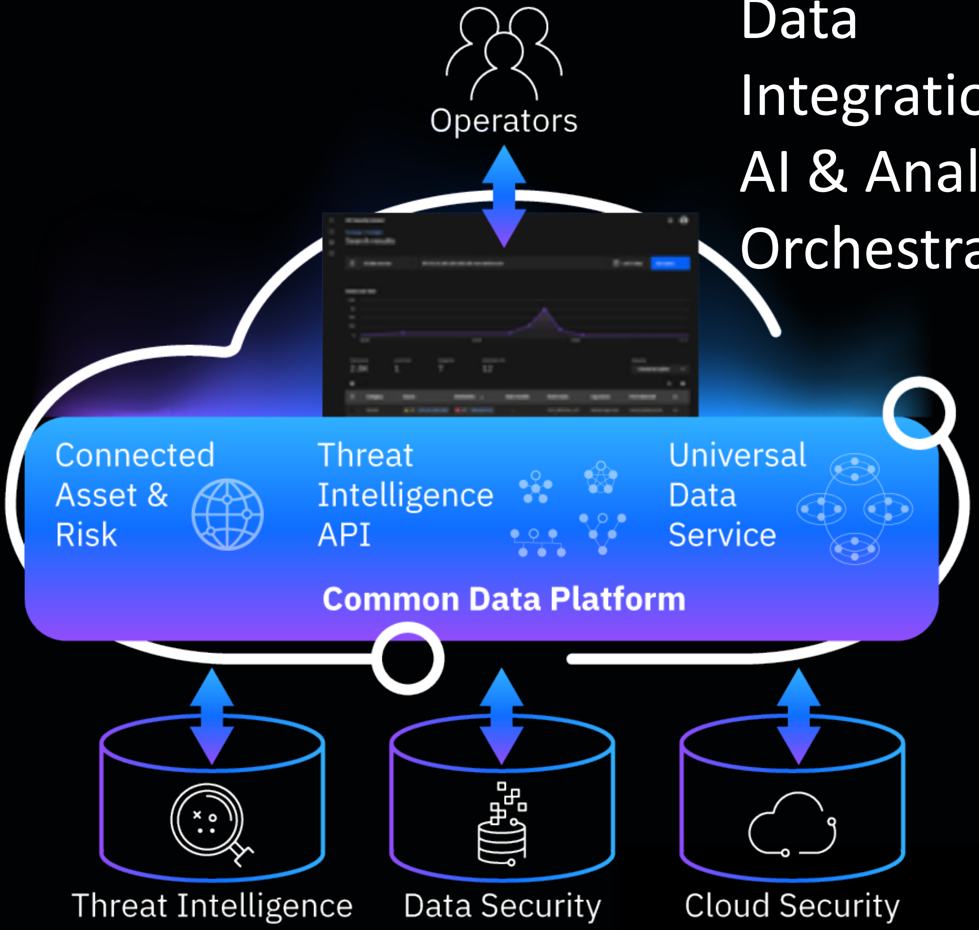
Use Case: Responding to Threats

Threat operations: Respond effectively

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

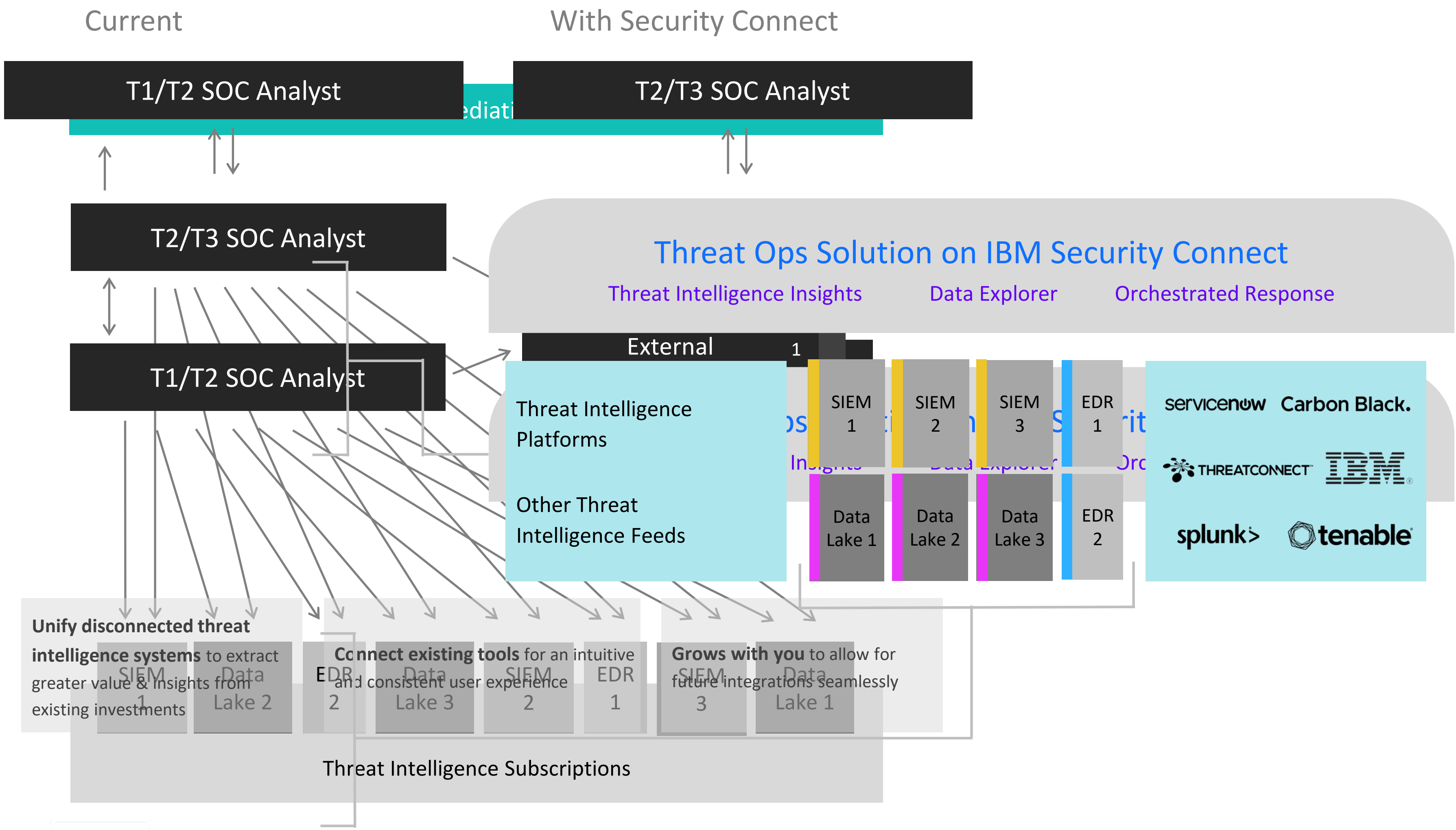


Connected applications, on a common platform, sharing analytics, insights, and enhancing each other



Data
Integration
AI & Analytics
Orchestration

Threat Ops: SOC Integration



Unify disconnected threat intelligence systems to extract greater value & insights from existing investments

Connect existing tools for an intuitive and consistent user experience

Grows with you to allow for future integrations seamlessly

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

Re-thinking the role of security analyst

- Change the roles of analyst
  - Do I still need Level 1, Level 2 and Level 3?
  - Can I reduce the onboarding time for analyst?
  - Can I expand my hiring pool for analyst?
- Expand my offering, to look at more data sources
- Onboard customers more quickly with more different use cases

Art of Possible

Threat Ops
Data Security
Digital Trust
Consumer IoT
Insider Threat
Use Cases…….

Better Value
Faster Response
Easier UX

IBM
hp ArcSight
splunk>
McAfee
paloalto NETWORKS

aws
Azure
vmware
cisco
CROWDSTRIKE
Carbon Black.
Symantec

Capgemini CONSULTING.TECHNOLOGY.OUTSOURCING
Cognizant
Deloitte.
QUALYS CONTINUOUS SECURITY
tenable network security

Get Inspired!

Innovators:

Join in the endeavor to turn security into a team sport

- Start busting your data siloes
- Visit IBM Booth #N5759 to learn how to begin the journey

Thank you!