IBM Cloud Pak for Security

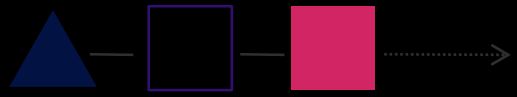
Connected security built for a hybrid, multicloud world

—

IBM **Security**

IBM

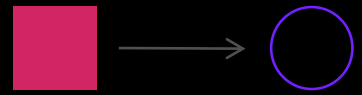
Security is fragmented, disconnected, & exacerbated by multicloud

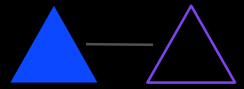


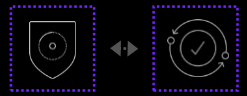
Cloud Object Store Access

Containers

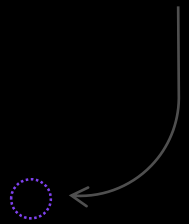
Threat Hunting

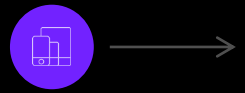




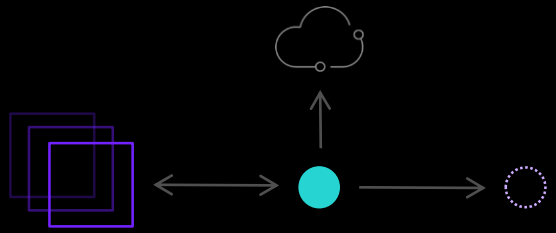


DevOps

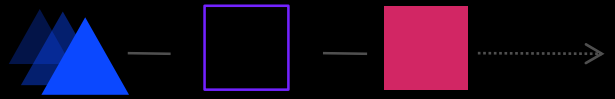




Mobile Devices

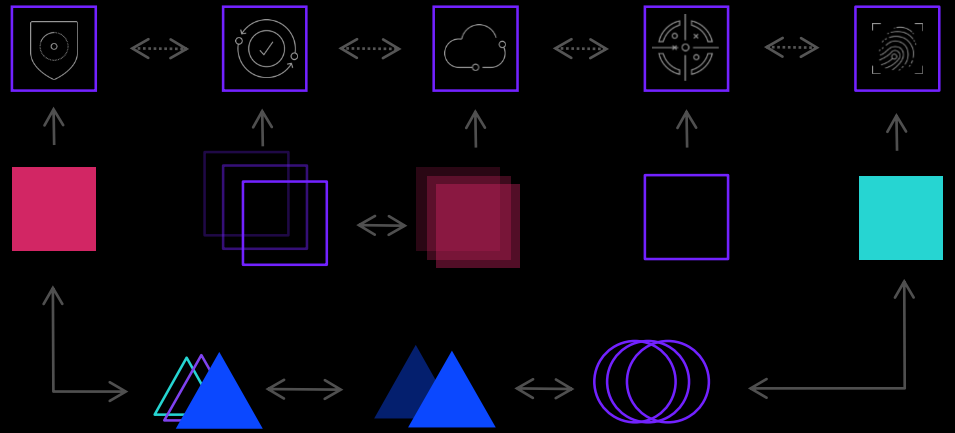


Cloud Security



Critical Data Monitoring

What if security were unified, connected?



Gain security insights

Connect data

Take action faster

Connect workflows

Run anywhere

Connect openly

Gain security insights

Connect data

- Uncover your hidden threats
- Make better risk-based decisions
- Leave your data where it is
- Get more out of your investments

Take action faster

Connect workflows

- Respond faster as a team and business
- Orchestrate across security use cases
- Reduce your integration costs
- Extend your team's capabilities

Run anywhere

Connect openly

- Run on-premise, private cloud or public cloud
- Increase and shift investment as needed
- Reduce vendor lock-in
- Promote interoperability

Open Cybersecurity Alliance (OCA): Co-founded by IBM to promote and support open security

Who

Global like-minded cybersecurity vendors, end users, thought leaders & individuals

Vision

Open Cyber Security Ecosystem:
Products freely exchange information, insights, analytics & orchestrated response

How

Open
Commonly developed code & tooling
Mutually agreed upon technologies, standards & procedures

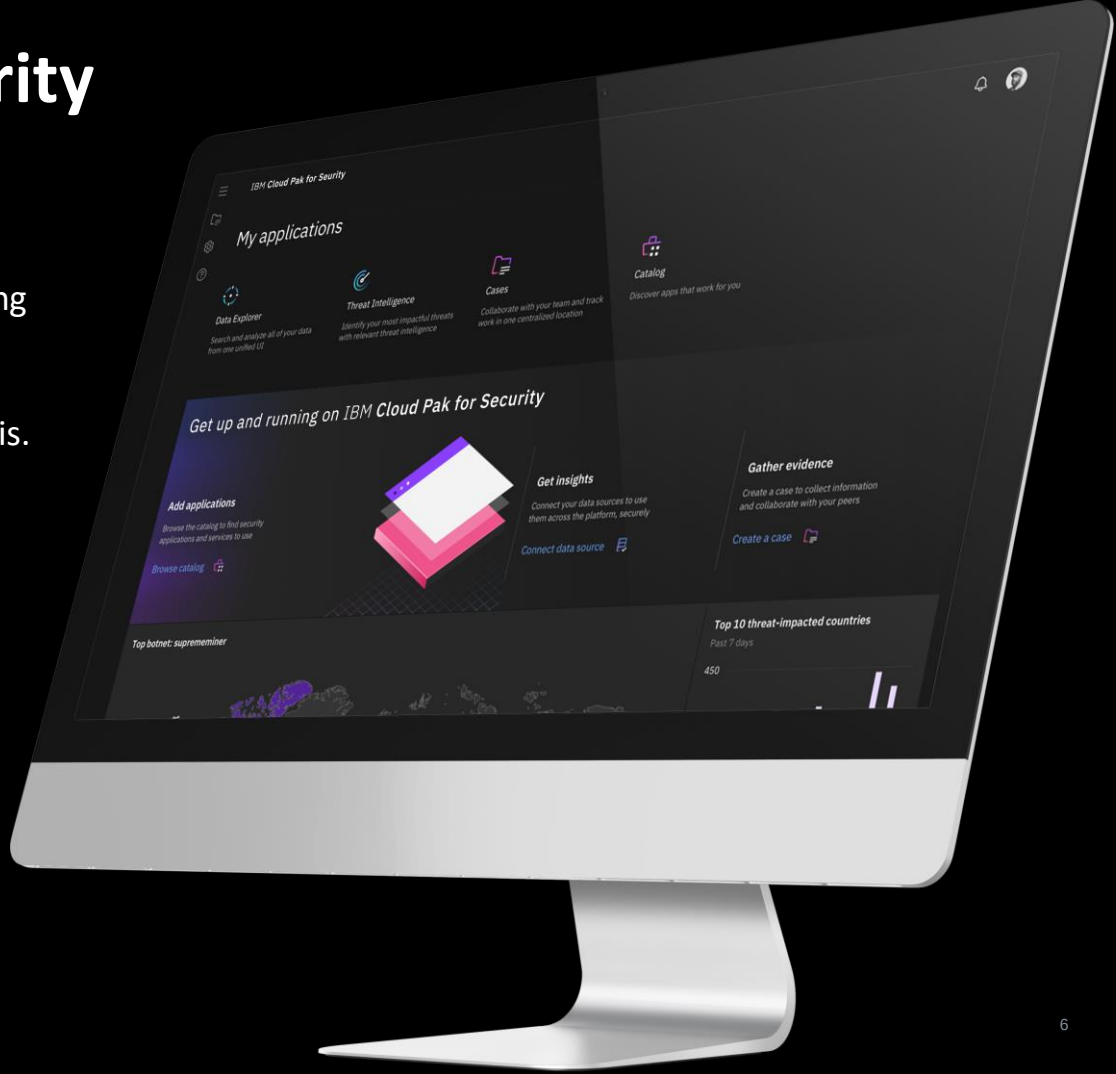
Initial committed projects – Stix Shifter and Open DXL Ontology now on Github

Engagement in OCA – number of members increased from 16 to 24

IBM **Cloud Pak for Security**

A platform to more quickly integrate your existing security tools to generate deeper insights into threats, orchestrate actions and automate responses—all while leaving your data where it is.

- Hybrid, multicloud architecture
- Connected, open ecosystem
- Automation & orchestration



Cloud Paks – Pre-integrated for cloud use cases

Cloud Pak for Applications

Build, deploy, and run applications

IBM containerized software

Container platform and operational services — Red Hat OpenShift

Cloud Pak for Data

Collect, organize, and analyze data

IBM containerized software

Container platform and operational services — Red Hat OpenShift

Cloud Pak for Integration

Integrate applications, data, and APIs

IBM containerized software

Container platform and operational services — Red Hat OpenShift

Cloud Pak for Automation

Transform business processes, decisions, and content

IBM containerized software

Container platform and operational services — Red Hat OpenShift

Cloud Pak for Multicloud Management

Multicloud visibility, governance, and automation

IBM containerized software

Container platform and operational services — Red Hat OpenShift

Cloud Pak for Security

Connect security data, tools and workflows

IBM containerized software

Container platform and operational services — Red Hat OpenShift

IBM public cloud

AWS

Microsoft Azure

Google Cloud

Private

IBM **Z**
IBM **LinuxOne**
IBM **Power** Systems

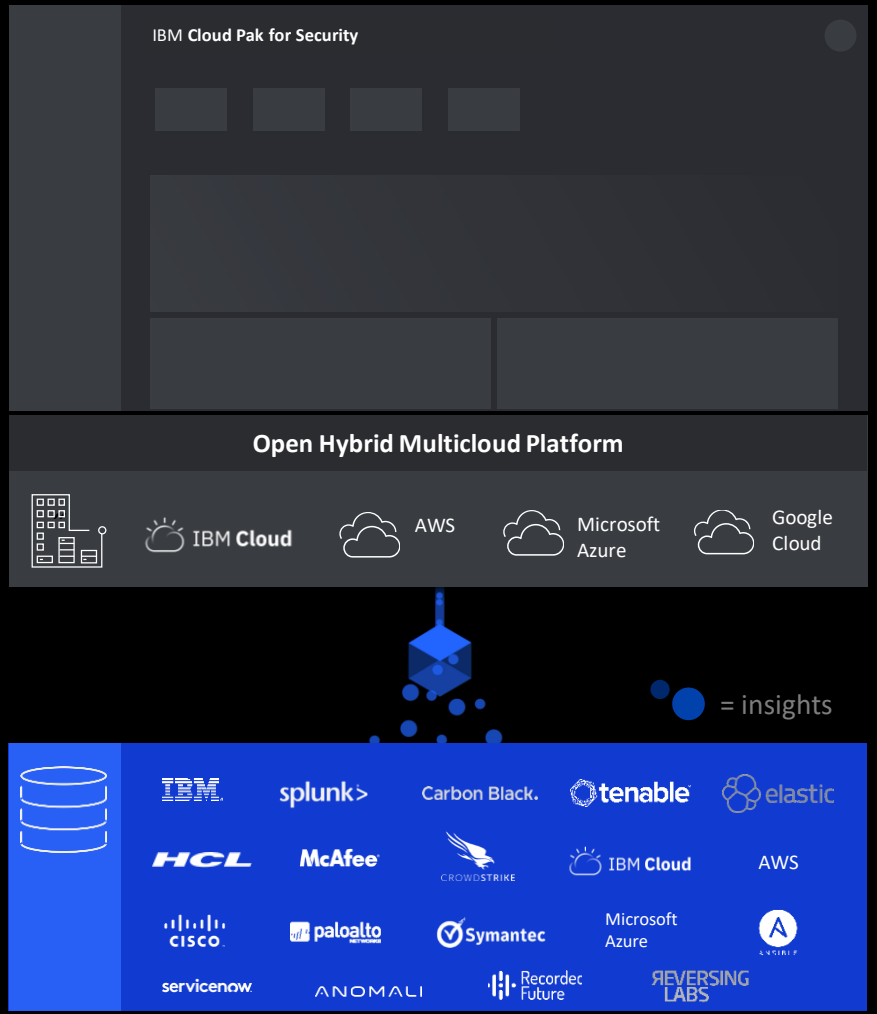
End points

Unified data service

Get complete insights while leaving your data where it is

Open partner ecosystem

Securely connect third-party security tools within existing security infrastructure



Hybrid, multicloud platform

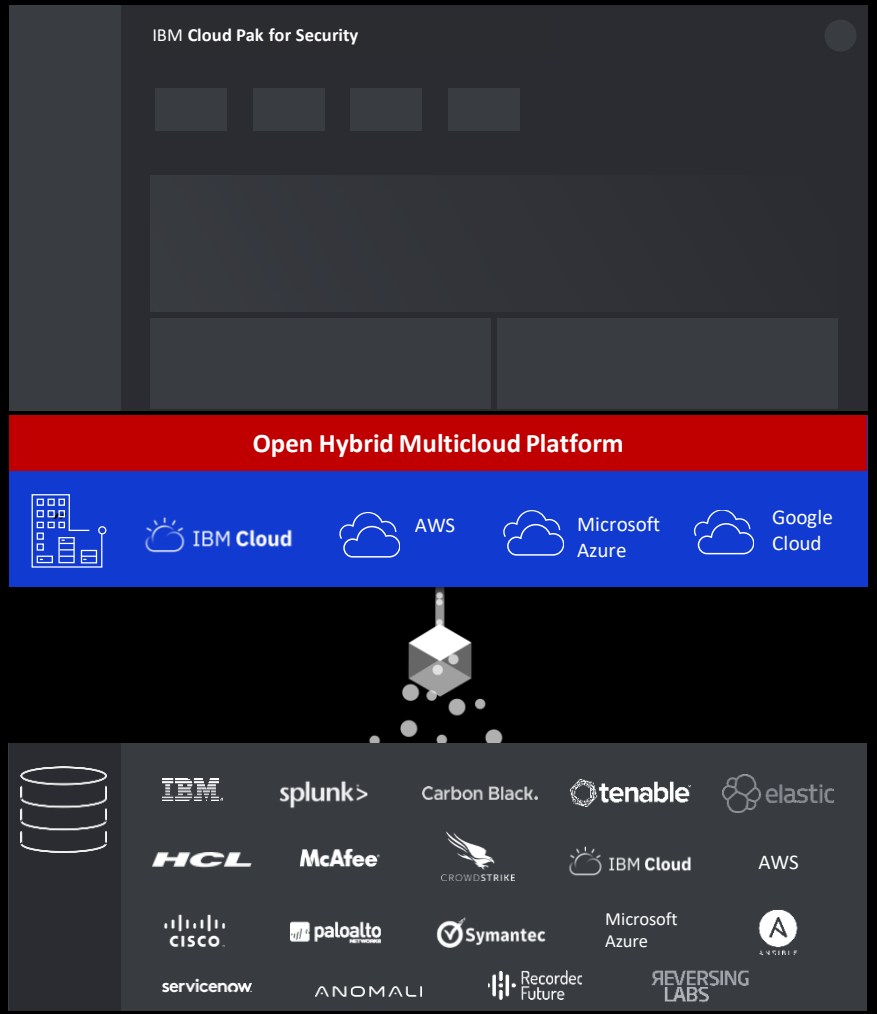
Modern, open architecture for public, private, hybrid clouds, ready to deploy and run anywhere

Unified data insights

Get complete insights while leaving your data where it is

Open partner ecosystem

Securely connect third-party security tools within existing security infrastructure



Unified interface & design system

Work across one unified experience, lower training costs, build apps faster

Outcome-driven solutions

Out-of-the-box ability to address security workflows, anchored by orchestration and automation

Hybrid, multicloud platform

Modern, open architecture for public, private, hybrid clouds, ready to deploy and run anywhere

Unified data insights

Get complete insights while leaving your data where it is

Open partner ecosystem

Securely connect third-party security tools within existing security infrastructure

IBM **Cloud Pak for Security**

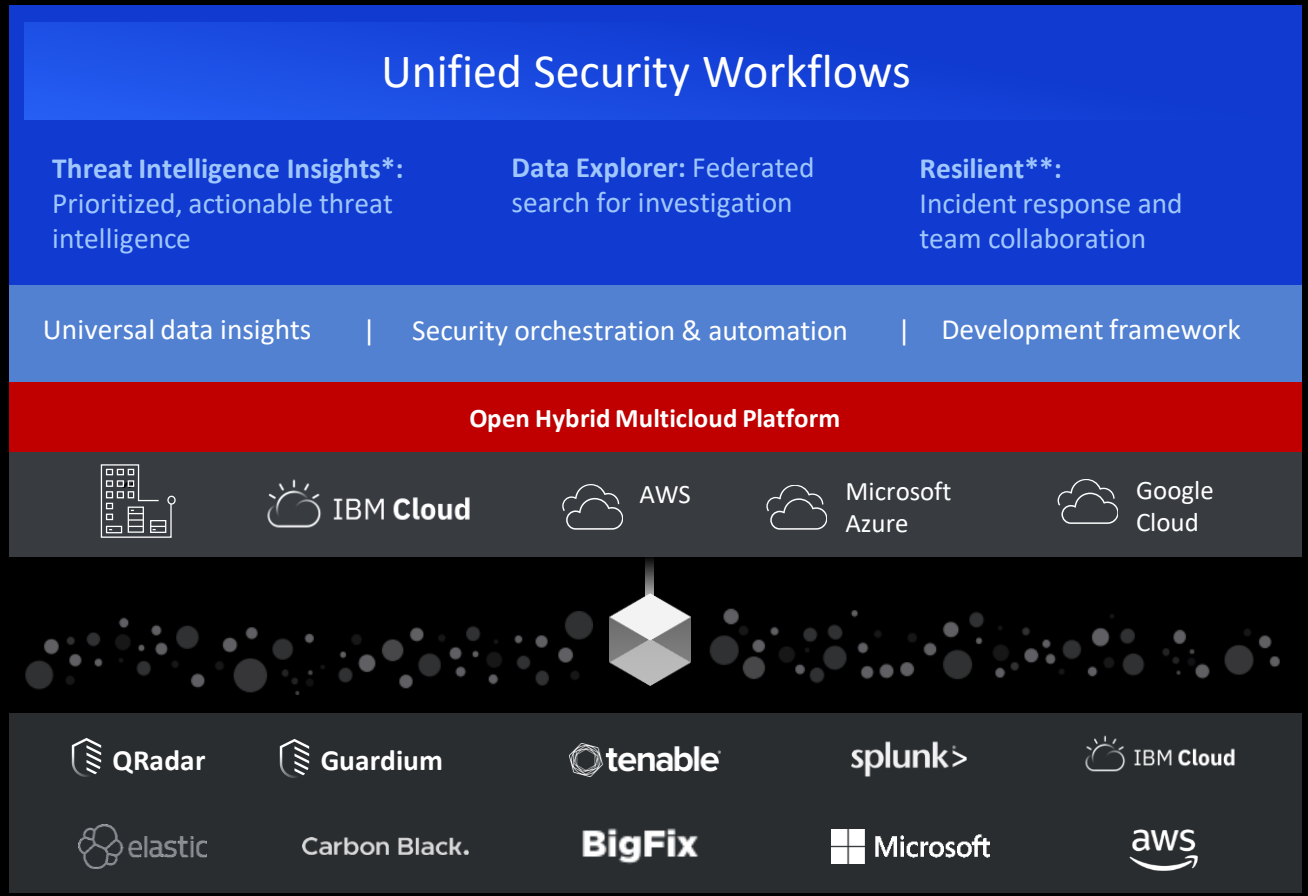
Gain security insights | Take action faster | Run anywhere

Security capabilities

Core platform services

Hybrid multicloud architecture

Open integration with existing security tools and data sources



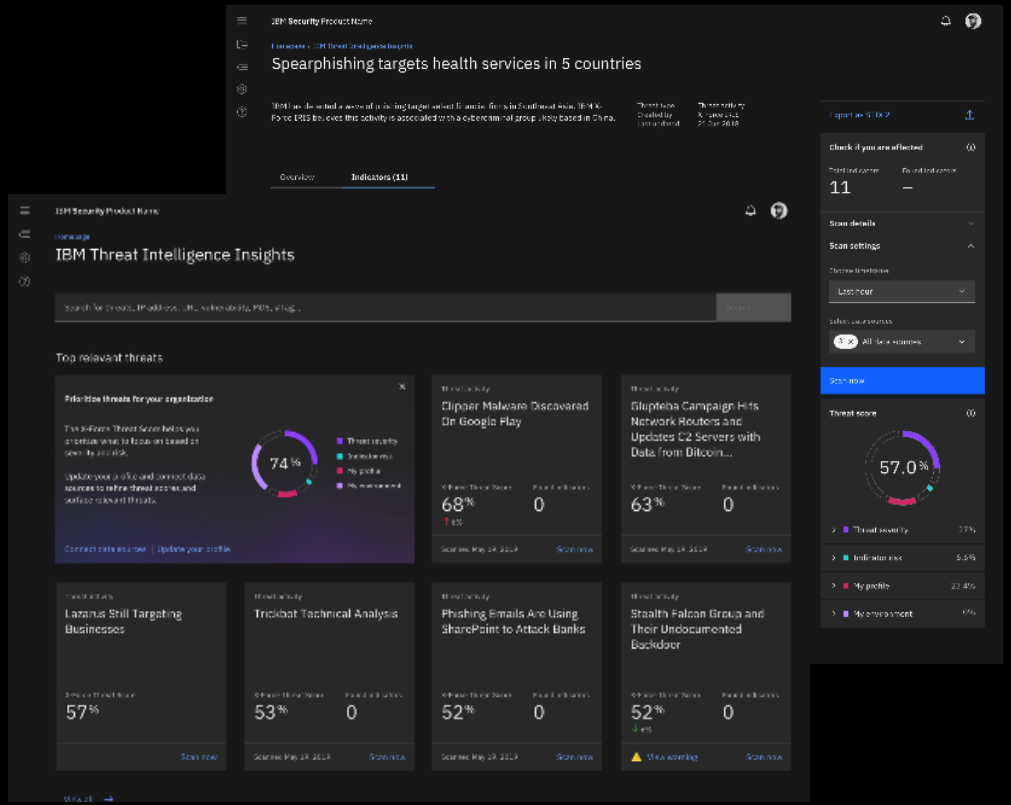
*Threat Intelligence Insights planned to GA in March 2020

**Resilient available as VM and planned on OpenShift in Q2 2020

Threat Intelligence Insights

Prioritized, actionable threat intelligence

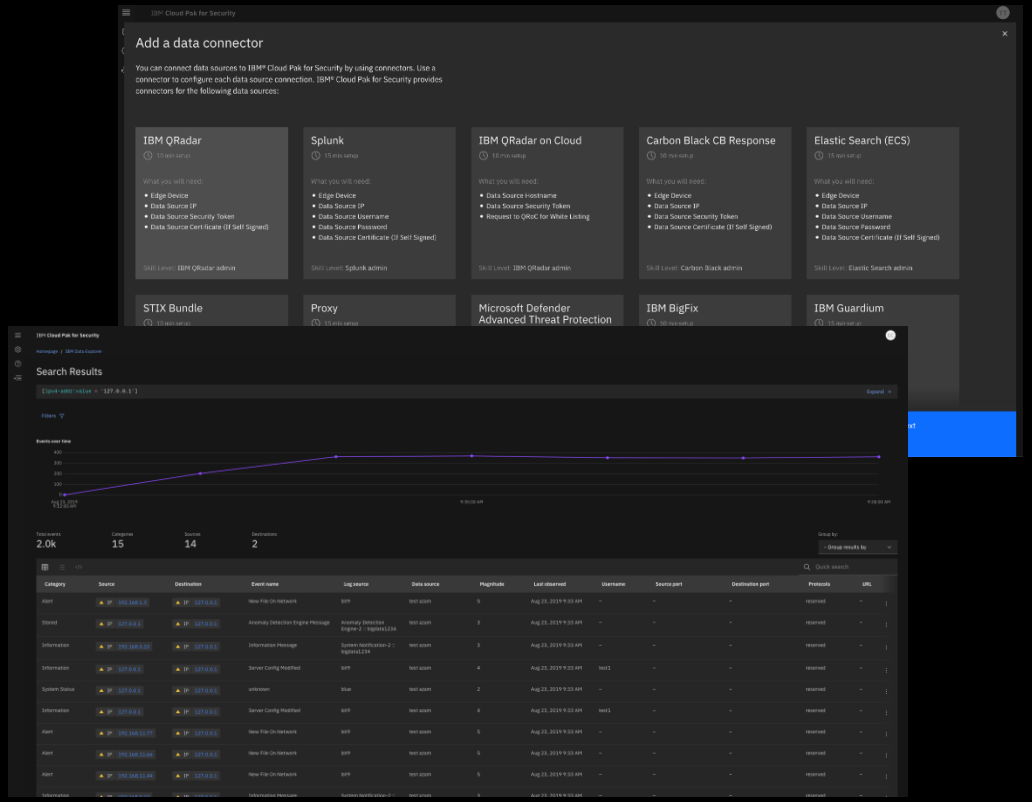
- **Act upon threat intelligence** with the X-Force Premium Threat Intelligence Reports, which provide contextual information curated by IBM X-Force IRIS team
- **Prioritize threats** with X-Force Threat Score, an adaptive score, calculated based on your relevance, severity, penetration, impact and actual environmental sightings
- **Identify threats active in your environment** with Am I Affected, which runs continuous and automated searches across connected data sources
- **Work from a single console** to investigate threats and indicators of compromise (IOCs) seamlessly across multiple siloed solutions and remediate cyber threats



Data Explorer

Federated search & investigation

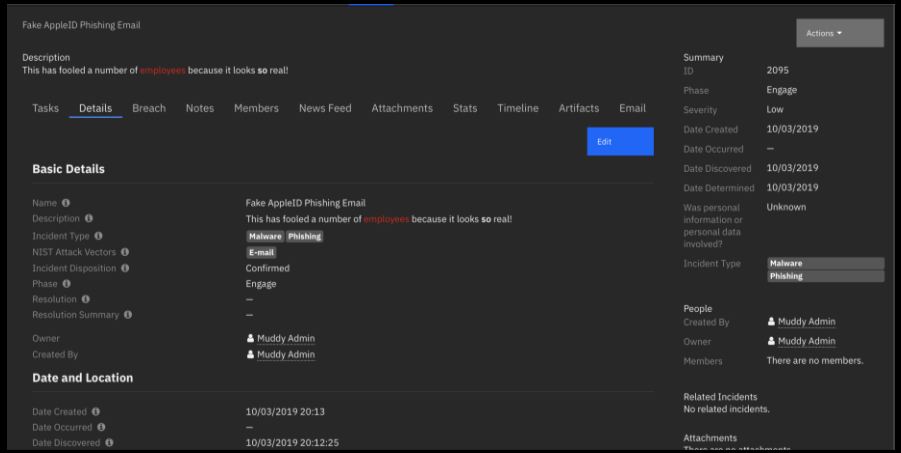
- **Connect your critical security data** with connectors to cloud and security data sources, without moving your data
- **Run queries against multiple data sources** while keeping the data at rest
- **Investigate from a single, unified interface** to search threats and IOCs
- **Find insights with a powerful search of all connected data,** leaving your data where it is
- **Seamlessly track investigations** with case management
- **Expand data sources and capabilities** with SDK or IBM services to create new connectors

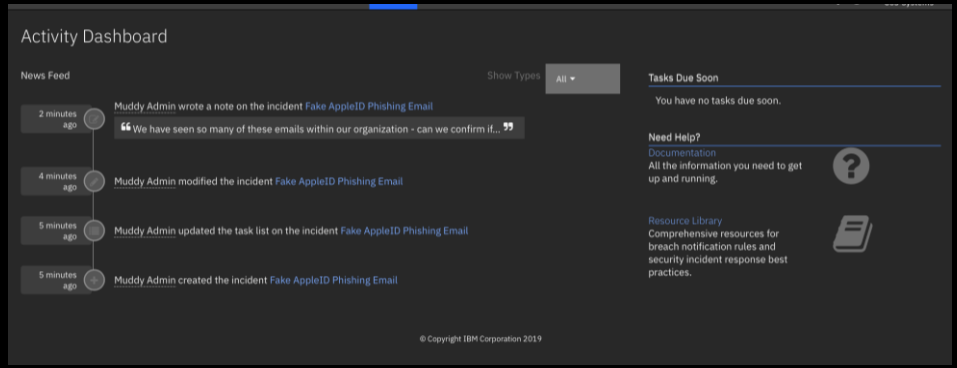


Resilient

Incident response

- **Reduce time to respond to and remediate** complex cyber threats by automating IR processes
- **Streamline and automate** manual and repetitive tasks such as IOC enrichment
- **Guide and execute investigation and response actions consistently** with robust case management and tasks
- **Prioritize analyst workload** on high-value investigation and response activities by guiding analyst response
- **Drive investigations across the organization** via extensive 3rd party apps and integrations
- **Customize and extend playbooks** through visual workflow editor





The future is open

Built for Open

- Open Ecosystem / Data Connectors
- Open Source Initiatives
- OASIS Open Cybersecurity Alliance

Smart, works for you

Powered by Experts

- Connector development
- Expertise on demand for access as needed
- Comprehensive strategy consulting

Connected security built for a hybrid, multicloud world

Gain security insights | Take action faster | Run anywhere

Thank you

Follow us on:

ibm.com/security

securityintelligence.com

ibm.com/security/community

xforce.ibmcloud.com

@ibmsecurity

youtube/user/ibmsecuritysolutions