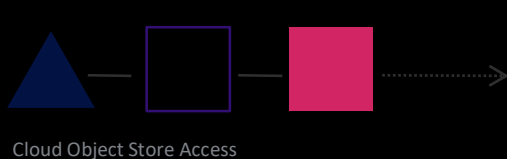


# IBM Cloud Pak for Security

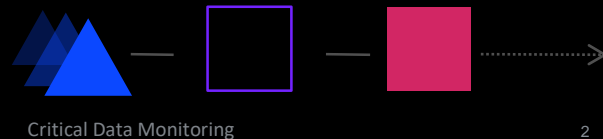
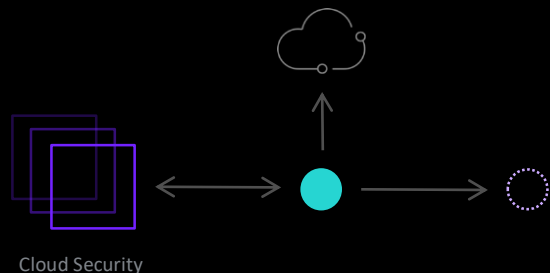
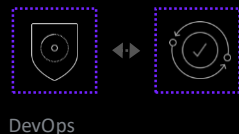
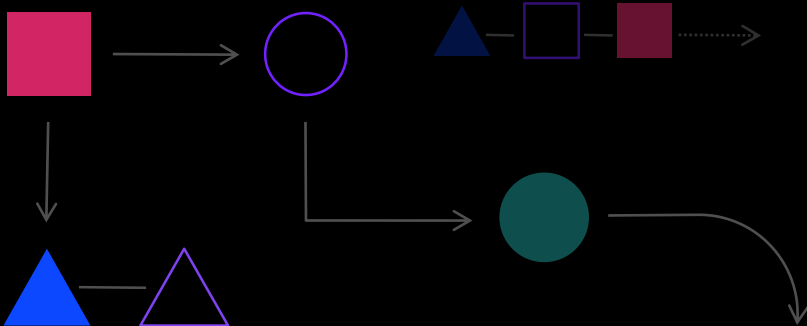
## **Connected security built for a hybrid, multicloud world**

---

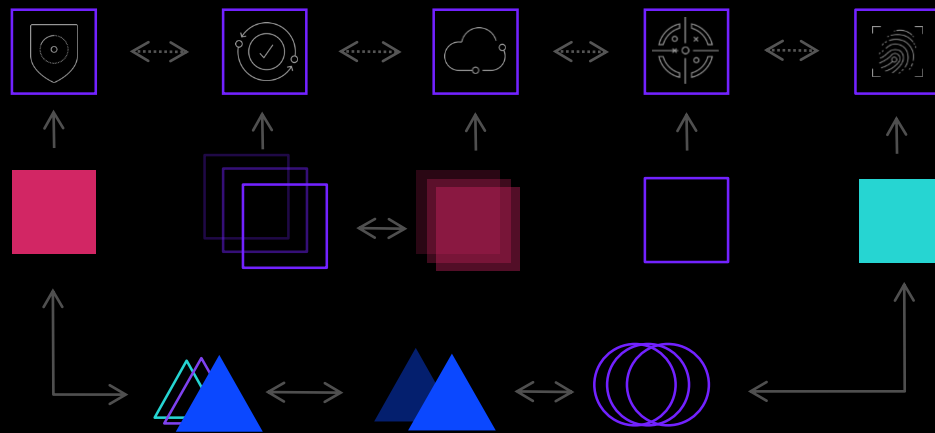
# Security is fragmented, disconnected, & exacerbated by multicloud



Threat Hunting



# 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

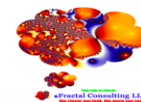
Global like-minded cybersecurity vendors, end users, thought leaders & individuals

## 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



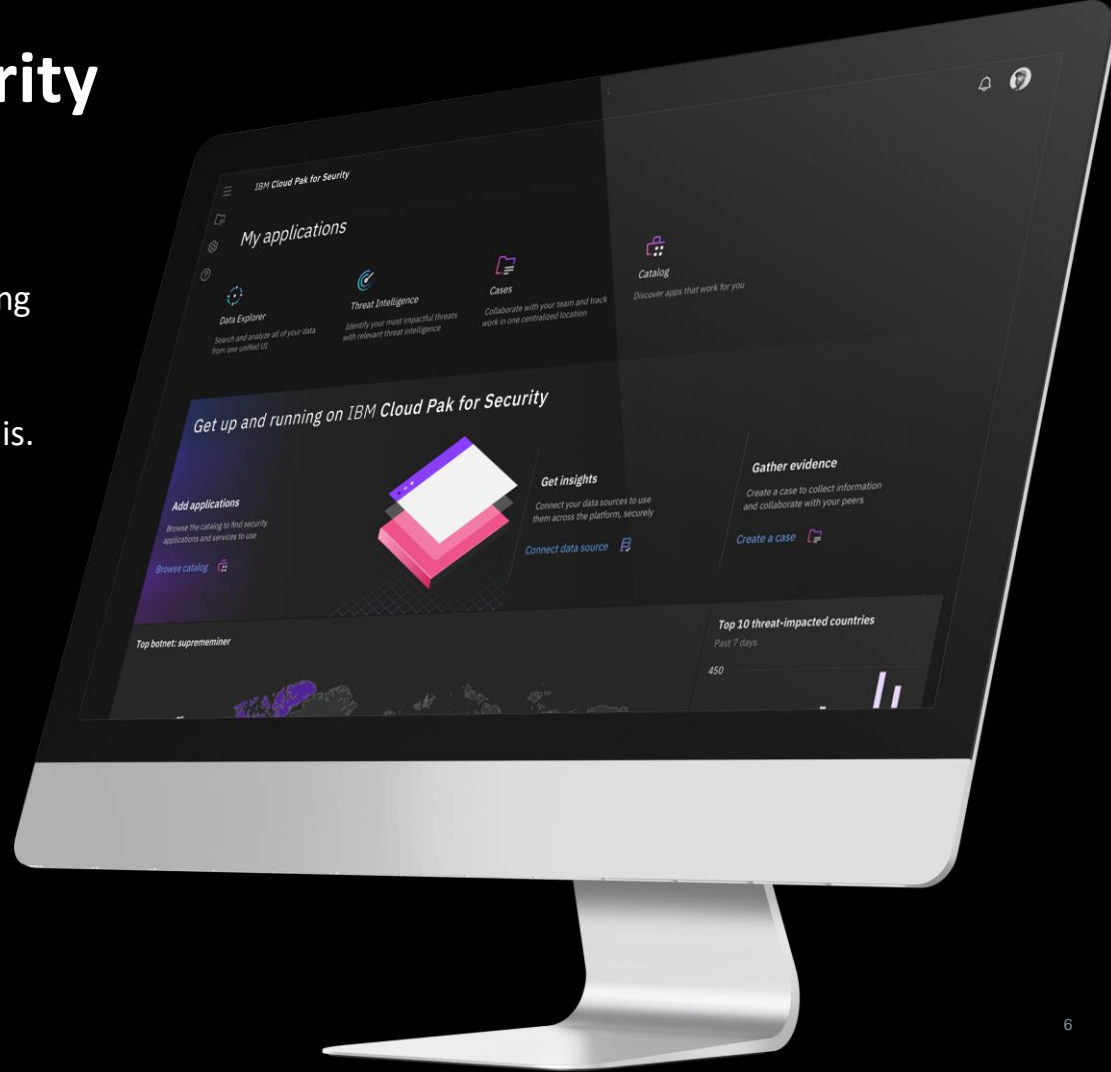
Initial committed projects – Stix Shifter and  
Open DXL Ontology now on Github

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



## Cloud Pak for Data

Collect, organize, and analyze data

IBM containerized software



Container platform and operational services



## Cloud Pak for Integration

Integrate applications, data, and APIs

IBM containerized software



Container platform and operational services



## Cloud Pak for Automation

Transform business processes, decisions, and content

IBM containerized software



Container platform and operational services



## Cloud Pak for Multicloud Management

Multicloud visibility, governance, and automation

IBM containerized software



Container platform and operational services



## Cloud Pak for Security

Connect security data, tools and workflows

IBM containerized software



Container platform and operational services



IBM public cloud



AWS



Microsoft Azure



Google Cloud



Private



IBM Z  
IBM LinuxOne  
IBM Power Systems

End points

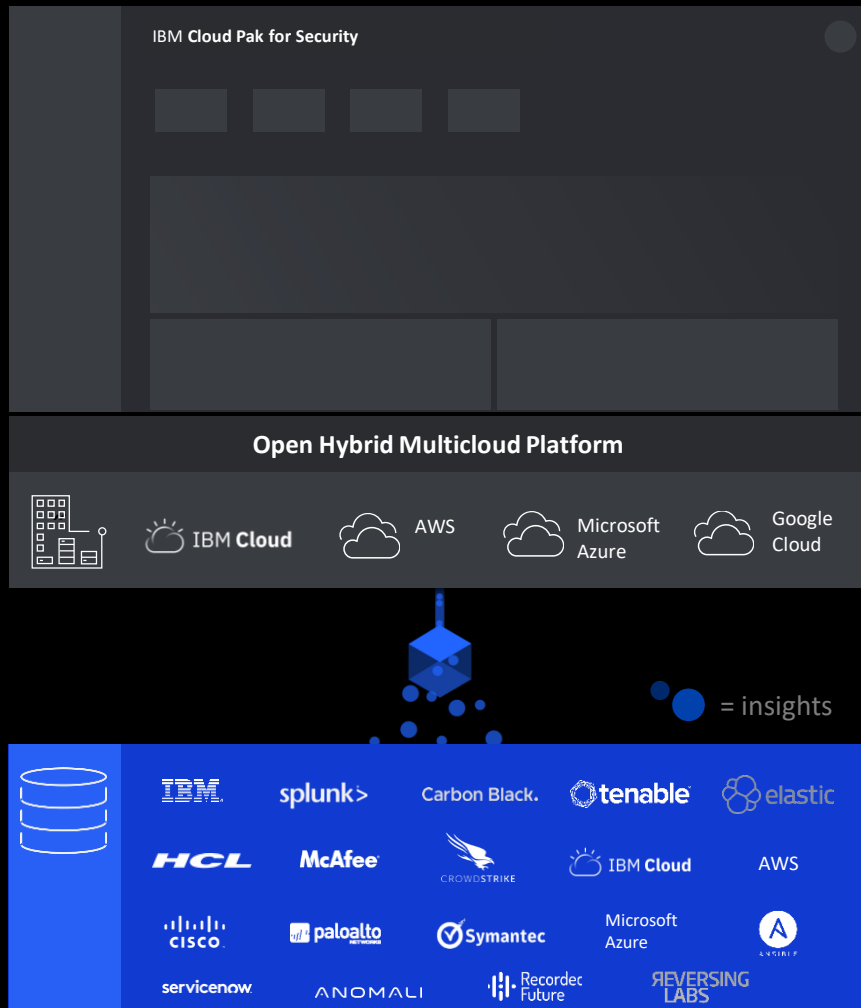


## Unified data service

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

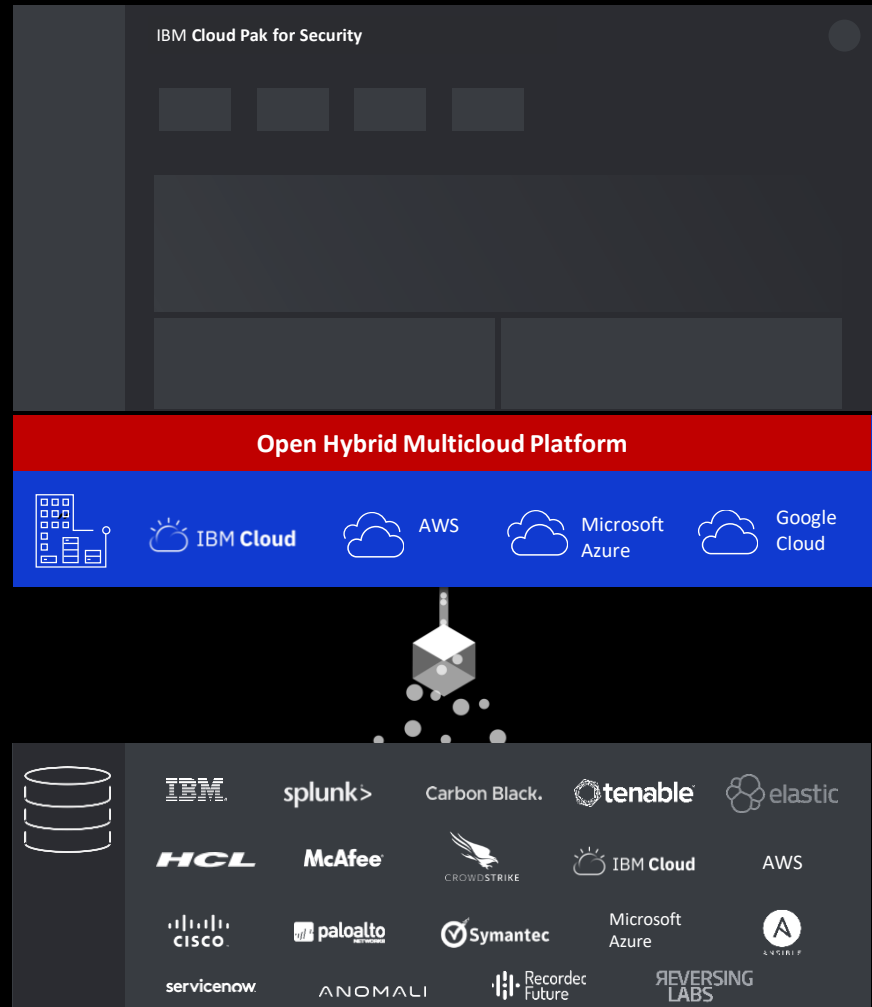
Modern, open architecture for public, private, hybrid clouds, ready to deploy and run anywhere

## 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

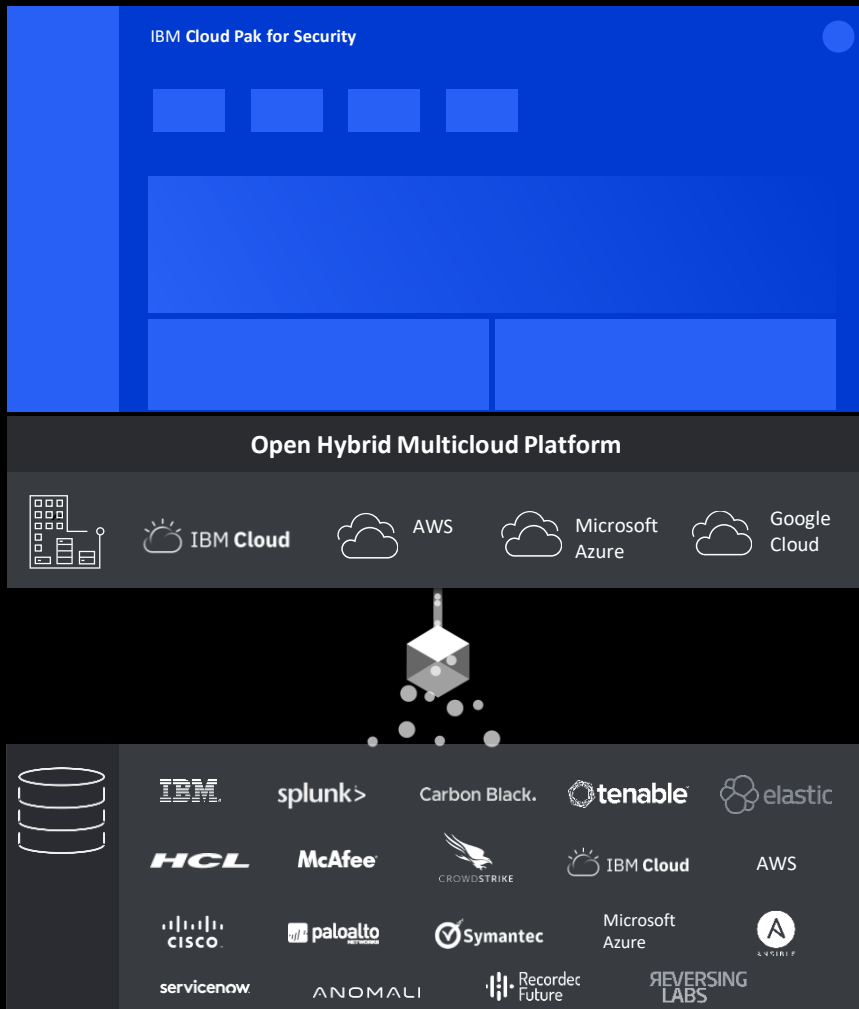
Modern, open architecture for public, private, hybrid clouds, ready to deploy and run anywhere

# 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

Security capabilities

Core platform services

Hybrid multicloud architecture

Open integration with existing security tools and data sources

Gain security insights

Take action faster

Run anywhere

## Unified Security Workflows

**Threat Intelligence Insights\*:**  
Prioritized, actionable threat intelligence

**Data Explorer:** Federated search for investigation

**Resilient\*\*:**  
Incident response and team collaboration

Universal data insights

Security orchestration & automation

Development framework

### Open Hybrid Multicloud Platform



IBM Cloud

AWS

Microsoft Azure

Google Cloud



QRadar

Guardium

tenable

splunk>

IBM Cloud

elastic

Carbon Black.

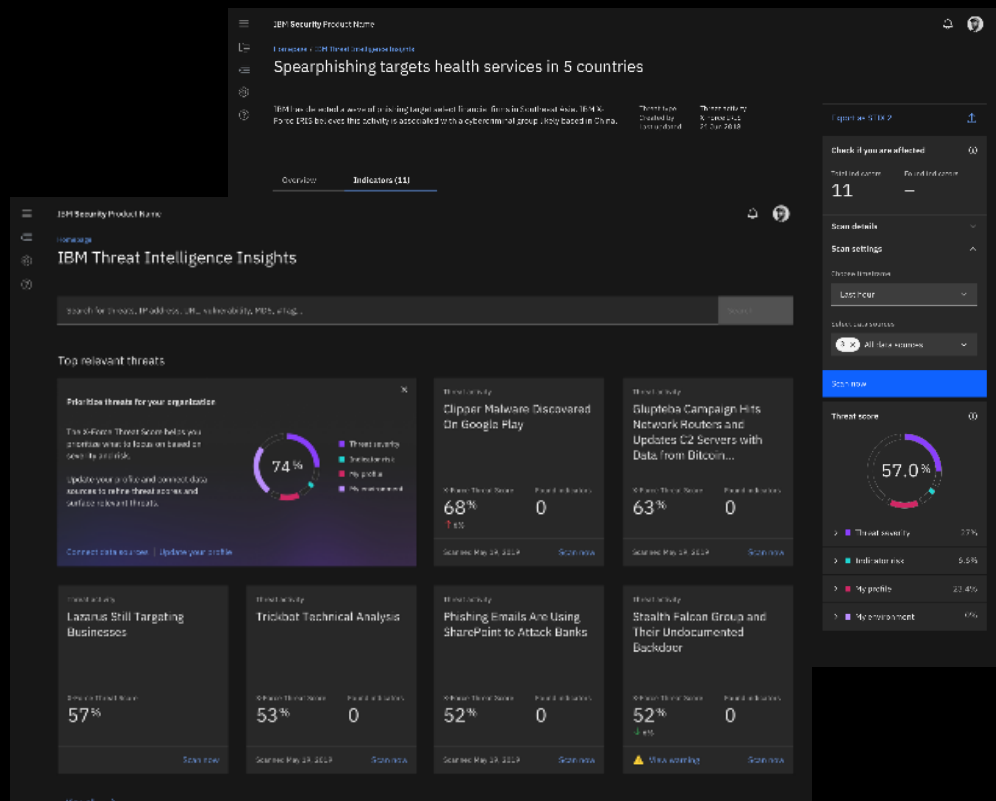
BigFix

Microsoft

aws

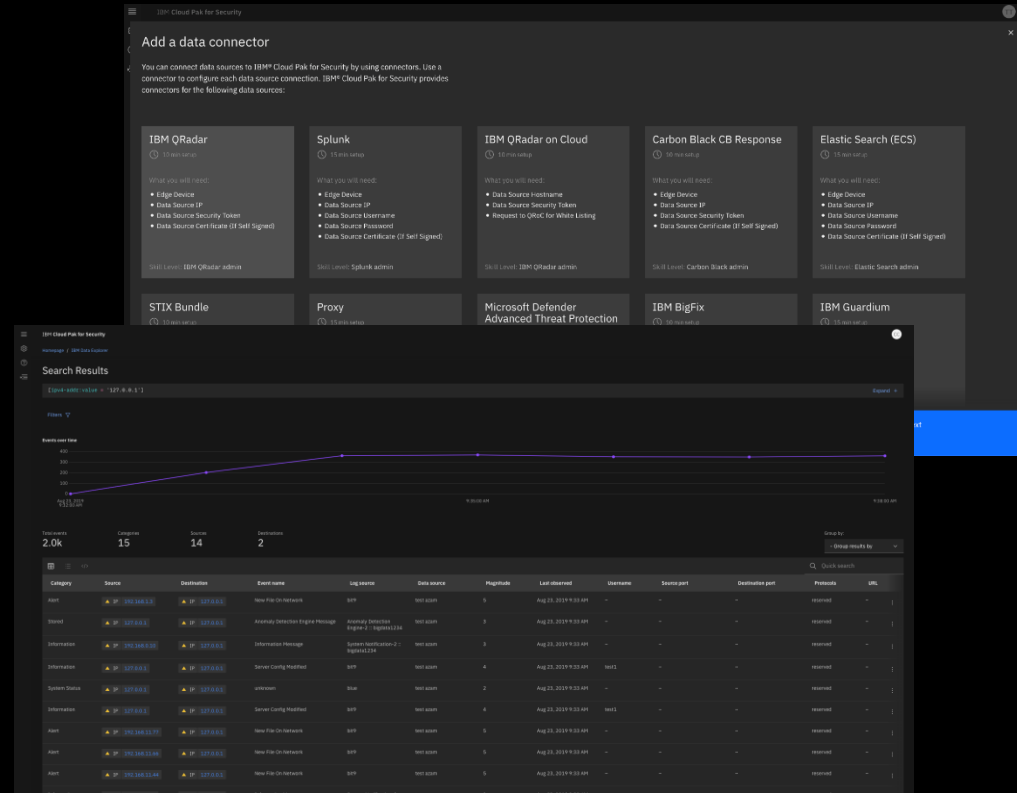
# Prioritized, actionable threat intelligence

- **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



# 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



# 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 screenshot shows the 'Fake AppleID Phishing Email' incident page. It includes a description, a summary table, and a 'Basic Details' section.

Summary	
ID	2095
Phase	Engage
Severity	Low
Date Created	10/03/2019
Date Occurred	—
Date Discovered	10/03/2019
Date Determined	10/03/2019
Was personal information or personal data involved?	Unknown
Incident Type	Malware Phishing
People	
Created By	Muddy Admin
Owner	Muddy Admin
Members	There are no members.
Related Incidents	No related incidents.
Attachments	

**Basic Details**

Name	Fake AppleID Phishing Email
Description	This has fooled a number of employees because it looks so real!
Incident Type	Malware Phishing
NIST Attack Vectors	E-mail
Incident Disposition	Confirmed
Phase	Engage
Resolution	—
Resolution Summary	—
Owner	Muddy Admin
Created By	Muddy Admin
Date and Location	
Date Created	10/03/2019 20:13
Date Occurred	—
Date Discovered	10/03/2019 20:12:25

The screenshot shows the 'Activity Dashboard' for the 'Fake AppleID Phishing Email' incident. It displays a timeline of events and a 'Tasks Due Soon' section.

**Activity Dashboard**

News Feed

Show Types: All

- 2 minutes ago: Muddy Admin wrote a note on the incident Fake AppleID Phishing Email.   
 "We have seen so many of these emails within our organization - can we confirm it..."
- 4 minutes ago: Muddy Admin modified the incident Fake AppleID Phishing Email
- 5 minutes ago: Muddy Admin updated the task list on the incident Fake AppleID Phishing Email
- 5 minutes ago: Muddy Admin created the incident Fake AppleID Phishing Email

**Tasks Due Soon**

You have no tasks due soon.

**Need Help?**

Documentation: All the information you need to get up and running.

**Resource Library**

Comprehensive resources for breach notification rules and security incident response best practices.

© Copyright IBM Corporation 2019

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, multcloud world

Gain security insights | Take action faster | Run anywhere



# Thank you

Follow us on:

[ibm.com/security](https://ibm.com/security)

[securityintelligence.com](https://securityintelligence.com)

[ibm.com/security/community](https://ibm.com/security/community)

[xforce.ibmcloud.com](https://xforce.ibmcloud.com)

[@ibmsecurity](https://twitter.com/ibmsecurity)

[youtube/user/ibmsecuritysolutions](https://youtube/user/ibmsecuritysolutions)

© Copyright IBM Corporation 2019. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.

**IBM Security**

