Modernize your security with an open, multicloud platform

IBM Cloud Pak for Security
Threat Management

IBM Cloud Pak for Security

My applications

Data Explorer

Search and analyze all of your data from one unified UI

Case Management

Collaborate with your team and track work in a centralized location

Threat Intelligence Insights

Identify your most impactful threats with relevant threat intelligence

Orchestration & Automation

Connect your data sources

Connect your data sources to securely use them across the platform

Connect data sources

Add your team

Add other users to your account subscription and manage their roles

Add users

Update company profile

Add your organization's industry and locations to get personalized insights

Update profile

Threat intelligence report lookup

Search for IPs, URLs, file hashes, vulnerabilities, threats, malware...

Search

Trending reports

IP 195.54.160.130

IP 185.156.73.44

IP 192.0.78.25

IP 5.101.0.209

IP 184.168.131.241

Dashboard

Threat Intelligence Insights

Worldwide Malicious Activity: bedep

A few seconds ago

Worldwide Malicious Activity Metadata for bedep

A few seconds ago

Botnet Information	Value
Affected Territories	2
Peak	2020-05-23
Trend	↘

Top 10 Threat-Impacted Locations

Name
Title
Email

Ransomware and data attacks were the most popular attacks in 2020

Ransomware

23%
Ransomware of attacks

$123M+
Estimated profits from top ransomware

13%
Data theft of attacks

Attacks related to COVID-19 & healthcare

#7
Healthcare's rank in top attacked industries

28%
Of attacks on healthcare ransomware

Threats to supply chain, manufacturing & energy industries

#2
Manufacturing's rank in top attacked industries

#3
Energy's rank in top attacked industries

Business priorities are driving digital transformation

Users and Endpoints

Accessing from anywhere
using any device

Data and Apps

Data is a shared resource
for users and apps

Infrastructure

Servers and networks distributed
across hybrid cloud environments

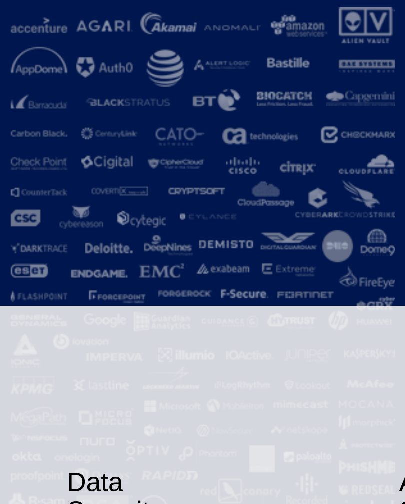
Security needs to safeguard these key transformations, but that can be a challenge...

Traditional security can’t keep pace

Too much to do

- ❑ Meet with CIO and stakeholders
- ❑ Nail down third-party risk
- ❑ Manage GDPR program with privacy office
- ❑ Respond to questions from state auditors
- ❑ Update CEO for board meeting
- ❑ Update budget projections
- ❑ Write security language for vendor's contract
- ❑ Make progress on the never-ending identity project
- ❑ Review and updated project list
- ❑ Edit communication calendar
- ❑ Update risk rankings on security roadmap
- ❑ Clarify policies governing external storage devices
- ❑ Provide testing and encryption tool direction
- ❑ Provide data handling best practices
- ❑ Help with new acquisition
- ❑ Meet with senior project managers
- ❑ Send new best practices to development teams
- ❑ Review logs for fraud ongoing investigation
- ❑ Help with insider threat discovery
- ❑ Determine location of sensitive data in cloud
- ❑ Investigate possible infection on legacy system
- ❑ Continue pen testing of new business mobile app
- ❑ Help architects understand zero trust
- ❑ Answer security policy emails
- ❑ Format security status report for executives
- ❑ Meet with recruiter to discuss staffing
- ❑ Write test plan requirements for new products
- ❑ Meet regarding improving security of facilities

Too many vendors



Too much complexity

Too many alerts

Too many silos

Identity and Access Management

Data Security

Application Security

Network Security

Endpoint Security

Clients need a modern, open, zero trust approach

Client's Security Challenges

- Cloud Security
- Advanced Threats
- Compliance and Privacy
- Skills Shortage
- Mobile, Edge and IoT / OT

IBM Solutions

IBM **Security**

Align
your security strategy to your business

Protect
digital users, assets, and data

Manage
defenses against growing threats

Modernize
your security with an open, multicloud platform

IBM Differentiation

- Deep Expertise
- AI-Driven Technology
- Open Platform
- Largest Ecosystem

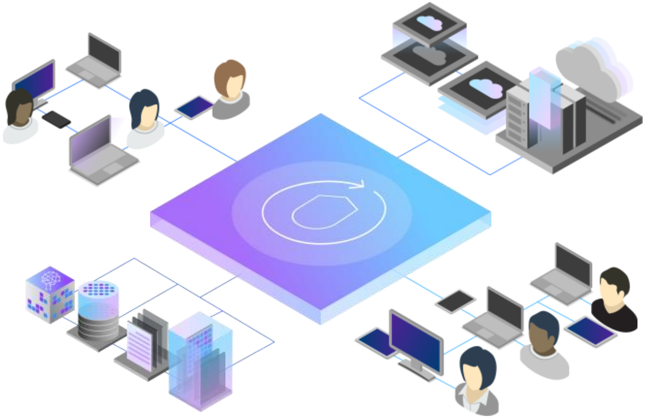
IBM Security clients are growing their business with a zero trust approach

Preserve customer privacy

Simplify and secure user onboarding

Manage user preferences and consent

Enforce privacy regulations controls



Protect the hybrid cloud

Manage & control all accesses

Monitor cloud activity and configurations

Secure cloud native workload

Reduce the risk of insider threat

Enforce least privilege access

Discover risky user behavior

Embed threat intelligence

Secure the remote workforce

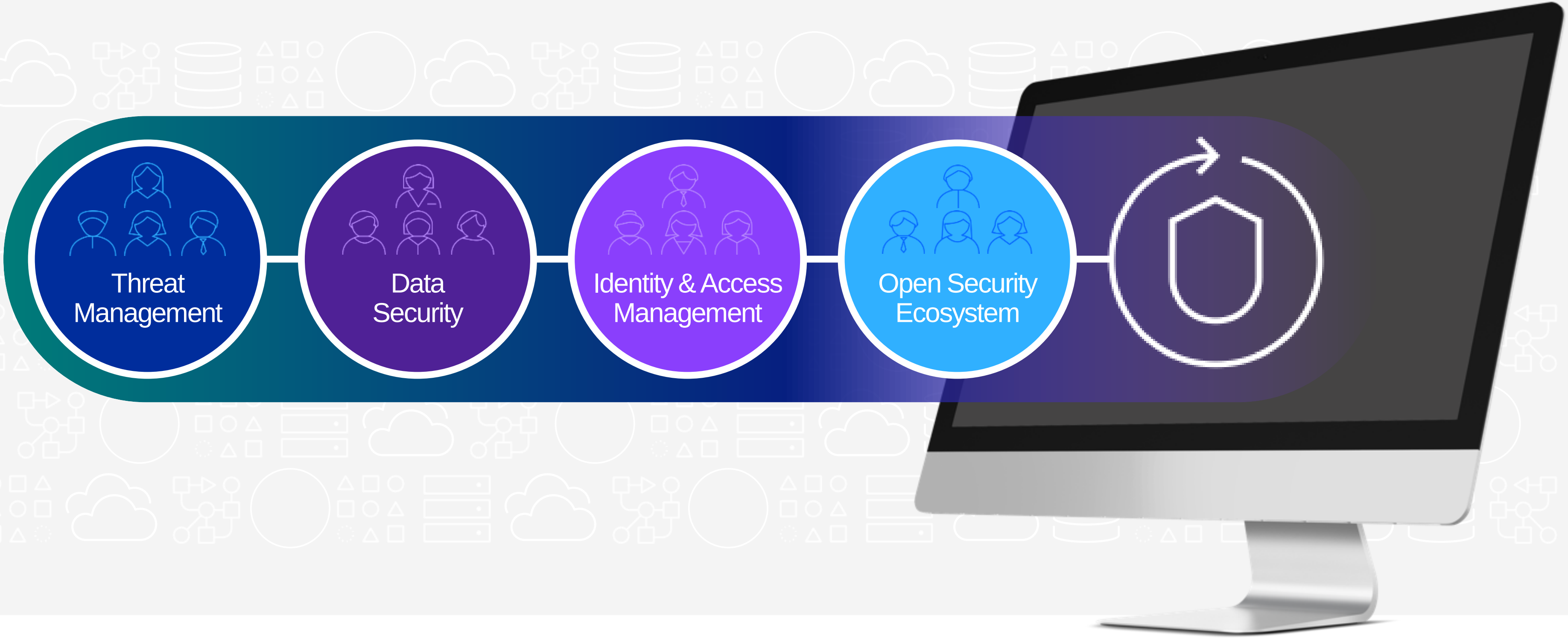
Secure BYO & unmanaged devices

Eliminate VPNs

Provide passwordless experiences

> “Zero trust helps us enable critical business capabilities while managing security”
>
> - CISO, Global Chemical Manufacturer

A unified and open approach for teams to connect data and workflows

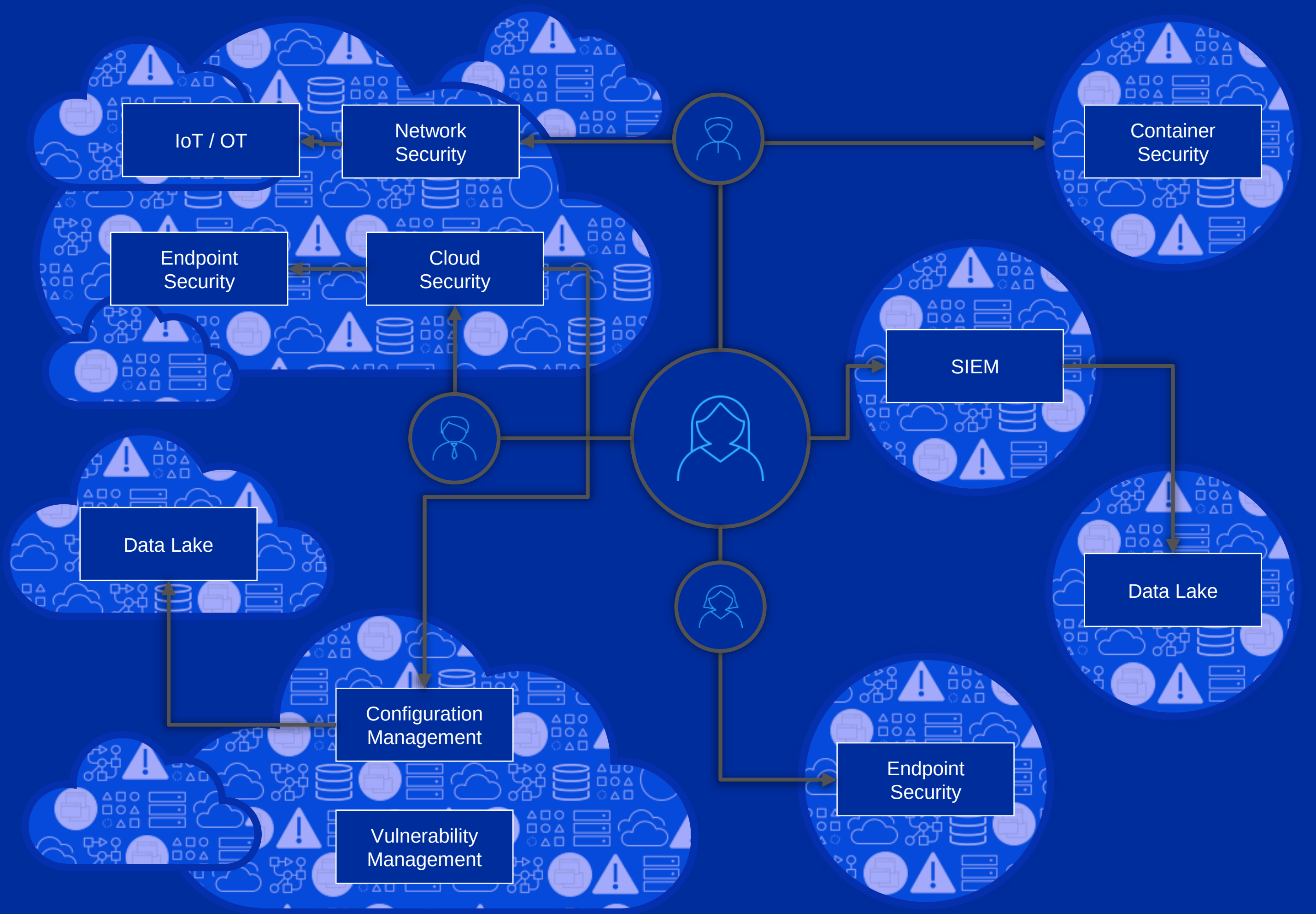


60% of companies use 25+ unique security products, and 44% engage with 10+ vendors

Growing threats, tools, and data are inhibiting security operations

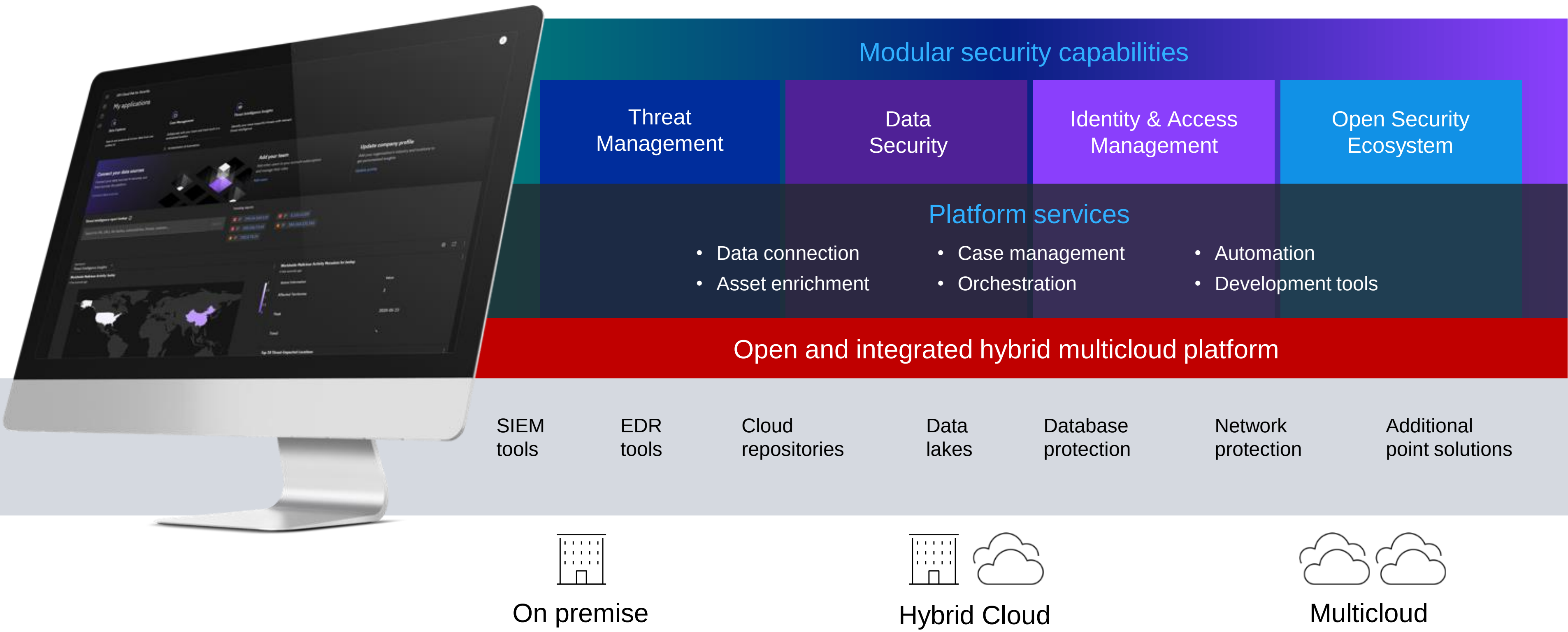
SOC analysts need help...

- Prioritizing the increasing number of events, alerts and intelligence data
- Quickly navigating multiple tools and data sources to investigate threats
- Reducing manual processes and even more tools to resolve security incidents



IBM Cloud Pak for Security

An open multicloud platform to gain security insights, take action faster, and modernize your architecture



Modular security capabilities

- Threat Management
- Data Security
- Identity & Access Management
- Open Security Ecosystem

Platform services

- Data connection
- Asset enrichment
- Case management
- Orchestration
- Automation
- Development tools

Open and integrated hybrid multicloud platform

- SIEM tools
- EDR tools
- Cloud repositories
- Data lakes
- Database protection
- Network protection
- Additional point solutions

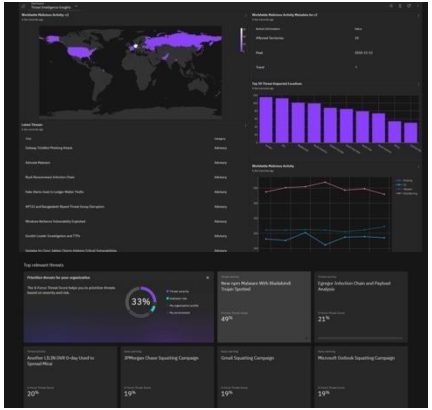
On premise

Hybrid Cloud

Multicloud

Outcomes of threat management solutions

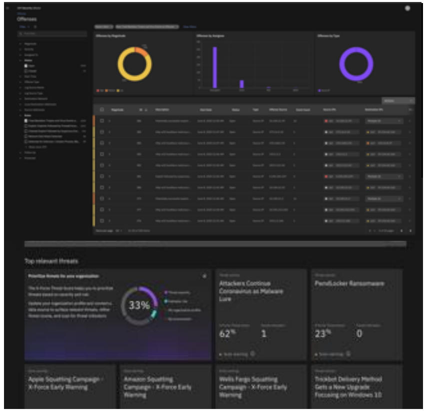
Visibility



600+

validated integrations to reduce risk and MTTD

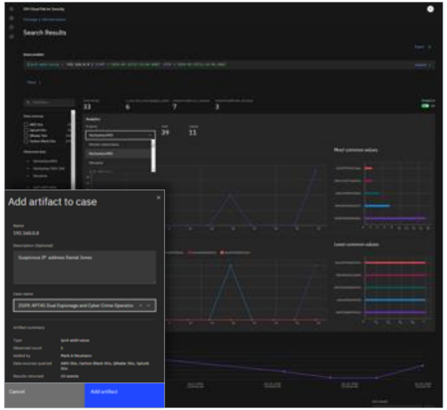
Detection


Offenses
Top relevant threats
33%
Attackers Continue Coronavirus as Malware Lure
PwndLocker Ransomware
62%
1
23%
0
Apple Squatting Campaign - X-Force Early Warning
Amazon Squatting Campaign - X-Force Early Warning
Wells Fargo Squatting Campaign - X-Force Early Warning
Trickbot Delivery Method Gets a New Upgrade Focusing on Windows 10

51%

increase in ability to detect attacks

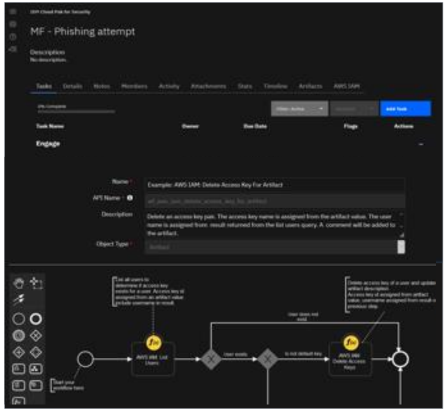
Investigation



60x

improvement in threat investigation time

Response



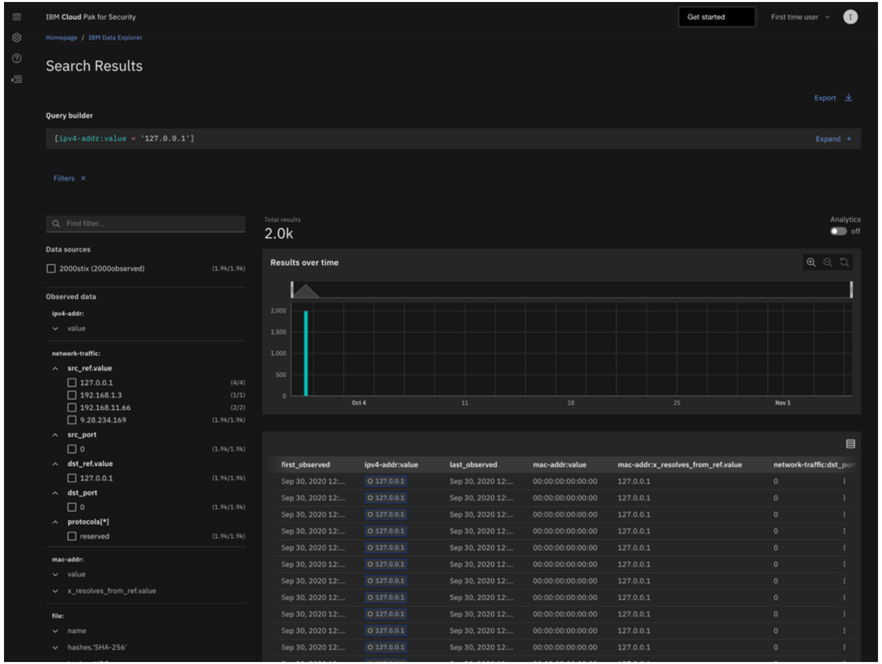
8x

increase in speed to respond to security incidents

Data Explorer

Federated search and investigation

- View all critical security data without moving it using pre-built connectors to cloud and security data sources
- Single query language (STIX) to investigate across all data sources for threats, patterns, IOCs, and more
- Automatically enrich data and attributes with integrations into threat intelligence feeds, assets, and risk databases
- Statistical insights without querying provides immediate analysis on least common, most common, and potential outlier values
- Seamless integration with SOAR cases to share insights, searches, and findings
- Expand data sources and capabilities, creating new connectors using an SDK or IBM services



Search Results

Query builder

```
[ipv4-addr:value = '127.0.0.1']
```

Data sources

□ 2000stix (2000observed) (1.9k/1.9k)

Observed data

ipv4-addr:
- value

network-traffic:
- src_ref.value
  - □ 127.0.0.1 (4/4)
  - □ 192.168.1.3 (1/1)
  - □ 192.168.11.66 (2/2)
  - □ 9.28.234.169 (1.9k/1.9k)
- src_port
  - □ 0 (1.9k/1.9k)
- dst_ref.value
  - □ 127.0.0.1 (1.9k/1.9k)
- dst_port
  - □ 0 (1.9k/1.9k)
- protocols[*]
  - □ reserved (1.9k/1.9k)

mac-addr:
- value
- x_resolves_from_ref.value

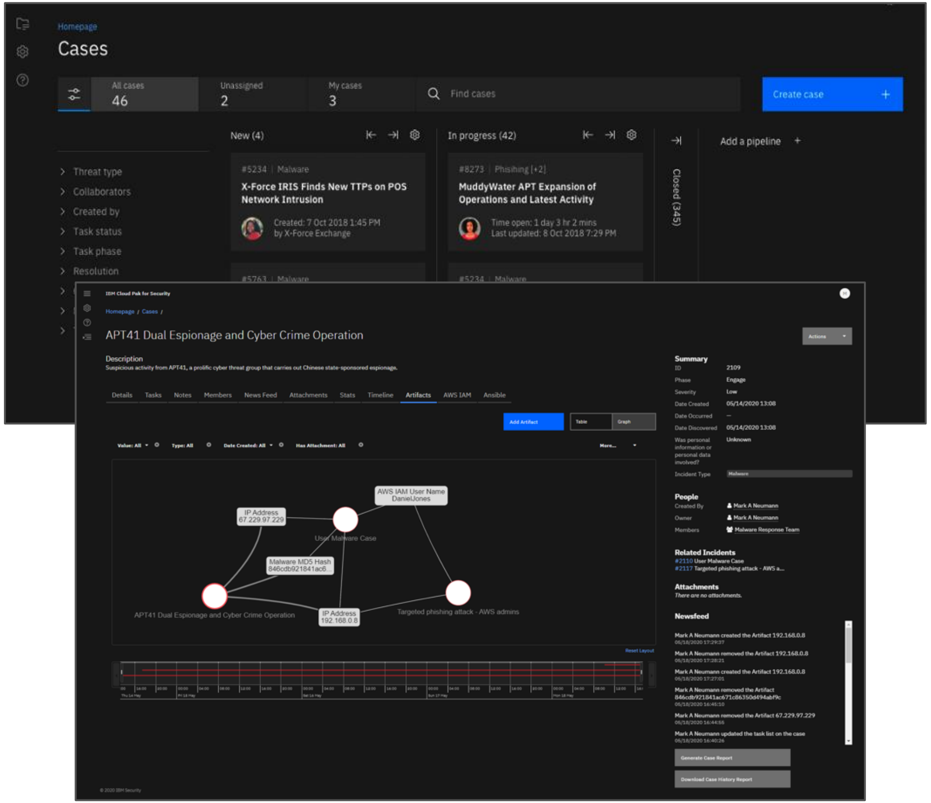
file:
- name
- hashes.'SHA-256'

first_observed	ipv4-addr:value	last_observed	mac-addr:value	mac-addr:x_resolves_from_ref.value	network-traffic:dst_port
Sep 30, 2020 12:...	127.0.0.1	Sep 30, 2020 12:...	00:00:00:00:00:00	127.0.0.1	0
Sep 30, 2020 12:...	127.0.0.1	Sep 30, 2020 12:...	00:00:00:00:00:00	127.0.0.1	0
Sep 30, 2020 12:...	127.0.0.1	Sep 30, 2020 12:...	00:00:00:00:00:00	127.0.0.1	0
Sep 30, 2020 12:...	127.0.0.1	Sep 30, 2020 12:...	00:00:00:00:00:00	127.0.0.1	0
Sep 30, 2020 12:...	127.0.0.1	Sep 30, 2020 12:...	00:00:00:00:00:00	127.0.0.1	0
Sep 30, 2020 12:...	127.0.0.1	Sep 30, 2020 12:...	00:00:00:00:00:00	127.0.0.1	0
Sep 30, 2020 12:...	127.0.0.1	Sep 30, 2020 12:...	00:00:00:00:00:00	127.0.0.1	0
Sep 30, 2020 12:...	127.0.0.1	Sep 30, 2020 12:...	00:00:00:00:00:00	127.0.0.1	0
Sep 30, 2020 12:...	127.0.0.1	Sep 30, 2020 12:...	00:00:00:00:00:00	127.0.0.1	0
Sep 30, 2020 12:...	127.0.0.1	Sep 30, 2020 12:...	00:00:00:00:00:00	127.0.0.1	0
Sep 30, 2020 12:...	127.0.0.1	Sep 30, 2020 12:...	00:00:00:00:00:00	127.0.0.1	0

Case Management

Security Orchestration, Automation, and Response (SOAR)

- Reduce time to respond to and remediate complex cyber threats by automating incident response processes
- Streamline and automate manual and repetitive tasks such as IOC enrichment and easily identify leverage points used by attackers, track IOCs over time and classify attributes
- Guide and execute investigation and response actions consistently with robust case management and tasks, leveraging visual process techniques from lean manufacturing
- Drive investigations across the organization via simple point-and-click deployment of 160+ third-party integrations
- Customize and extend dynamic playbooks through a visual workflow editor
- Meet compliance regulatory requirements with a privacy add-on



#5234 | Malware
X-Force IRIS Finds New TTPs on POS Network Intrusion
Created: 7 Oct 2018 1:45 PM
by X-Force Exchange

#8273 | Phishing [+2]
MuddyWater APT Expansion of Operations and Latest Activity
Time open: 1 day 3 hr 2 mins
Last updated: 8 Oct 2018 7:29 PM

#5763 | Malware

#5234 | Malware

APT41 Dual Espionage and Cyber Crime Operation

Description
Suspicious activity from APT41, a prolific cyber threat group that carries out Chinese state-sponsored espionage.

Summary

ID	2109
Phase	Engage
Severity	Low
Date Created	05/14/2020 13:08
Date Occurred	—
Date Discovered	05/14/2020 13:08
Was personal information or personal data involved?	Unknown
Incident Type	Malware

People

Created By	Mark A Neumann
Owner	Mark A Neumann
Members	Malware Response Team

Related Incidents
#2110 User Malware Case
#2117 Targeted phishing attack - AWS a...

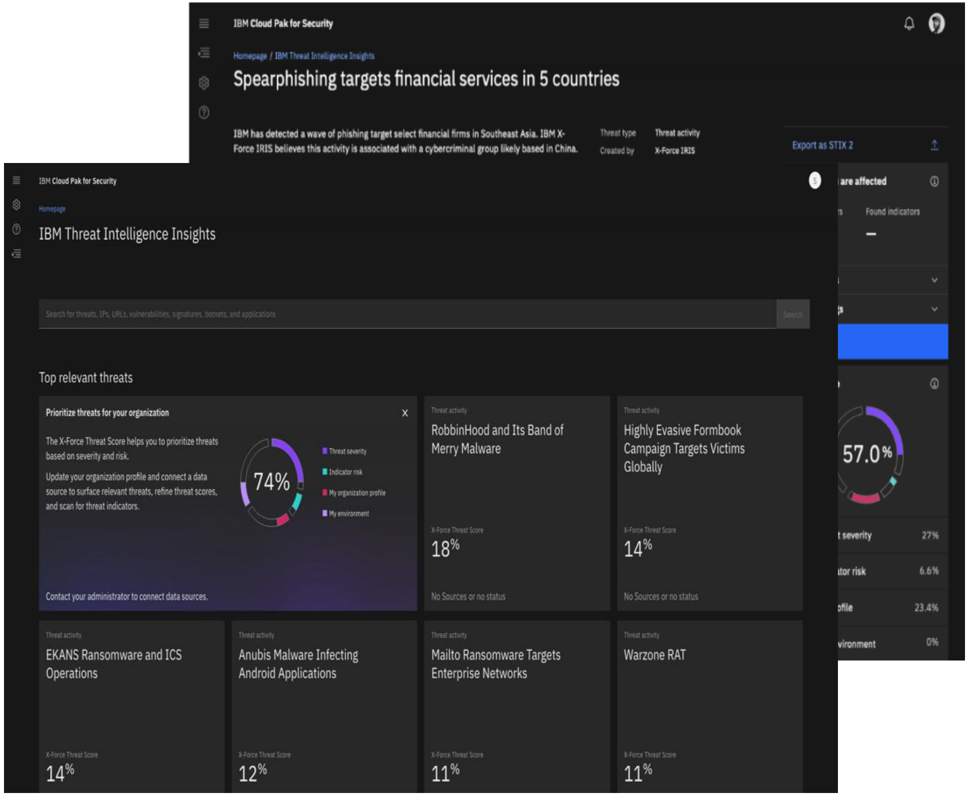
Attachments
There are no attachments.

Newsfeed
Mark A Neumann created the Artifact 192.168.0.8
05/18/2020 17:29:37
Mark A Neumann removed the Artifact 192.168.0.8
05/18/2020 17:28:21
Mark A Neumann created the Artifact 192.168.0.8
05/18/2020 17:27:01
Mark A Neumann removed the Artifact 846cdb921841ac671c86350d494abf9c
05/18/2020 16:45:10
Mark A Neumann removed the Artifact 67.229.97.229
05/18/2020 16:44:55
Mark A Neumann updated the task list on the case
05/18/2020 16:40:26

Threat Intelligence Insights

Prioritized, actionable threat intelligence

- Gain global threat intelligence through reports with contextual information curated by the IBM X-Force team
- Prioritize threats with the X-Force Threat Score, based on relevance, severity, penetration, impact and environmental sightings
- Identify and act on threats active in the environment with “Am I Affected”—continuous, automated searches across data sources; cases created automatically for active threats
- Leverage investments in 3rd-party threat intelligence feeds through a simple single configuration screen and enrich information throughout the platform



IBM Cloud Pak for Security

Homepage / IBM Threat Intelligence Insights

Spearphishing targets financial services in 5 countries

IBM has detected a wave of phishing target select financial firms in Southeast Asia. IBM X-Force IRIS believes this activity is associated with a cybercriminal group likely based in China.

Threat type: Threat activity
Created by: X-Force IRIS

Export as STIX 2

are affected

Found indicators: —

57.0%

t severity	27%
ator risk	6.6%
ofile	23.4%
vironment	0%

IBM Cloud Pak for Security

Homepage

IBM Threat Intelligence Insights

Search for threats, IPs, URLs, vulnerabilities, signatures, botnets, and applications

Top relevant threats

Prioritize threats for your organization

The X-Force Threat Score helps you to prioritize threats based on severity and risk.

Update your organization profile and connect a data source to surface relevant threats, refine threat scores, and scan for threat indicators.

74%

Contact your administrator to connect data sources.

Threat activity	X-Force Threat Score	
RobbinHood and Its Band of Merry Malware	18%	No Sources or no status
Highly Evasive Formbook Campaign Targets Victims Globally	14%	No Sources or no status
EKANS Ransomware and ICS Operations	14%	
Anubis Malware Infecting Android Applications	12%	
Mailto Ransomware Targets Enterprise Networks	11%	
Warzone RAT	11%	

Get started

1.
Learn more about IBM Cloud Pak for Security
ibm.com/products/cloud-pak-for-security

2.
Try IBM Garage Business Framing for free
ibm.biz/trygarage

Modernize your security with an open, multicloud platform

Gain security insights

With a unified console that provides visibility and analytics across IBM and 3rd party security tools, data, and clouds

Take action faster

With AI and automation, simplify operations and streamline response, to save time and lower risk

Modernize your architecture

Run anywhere with an open, multi-cloud platform that gives you flexibility, extensibility and avoids lock-in

Thank you

Follow us on:

ibm.com/security

securityintelligence.com

ibm.com/security/community

xforce.ibmcloud.com

@ibmsecurity

youtube.com/ibmsecurity

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

IBM