

# See What Matters Most

IBM **SECURITY** QRadar

We have  
enough data,  
but not  
enough  
insights

44%

of alerts are not investigated

54%

legitimate alerts are not remediated

36%

say “keeping up with alerts” is top concern

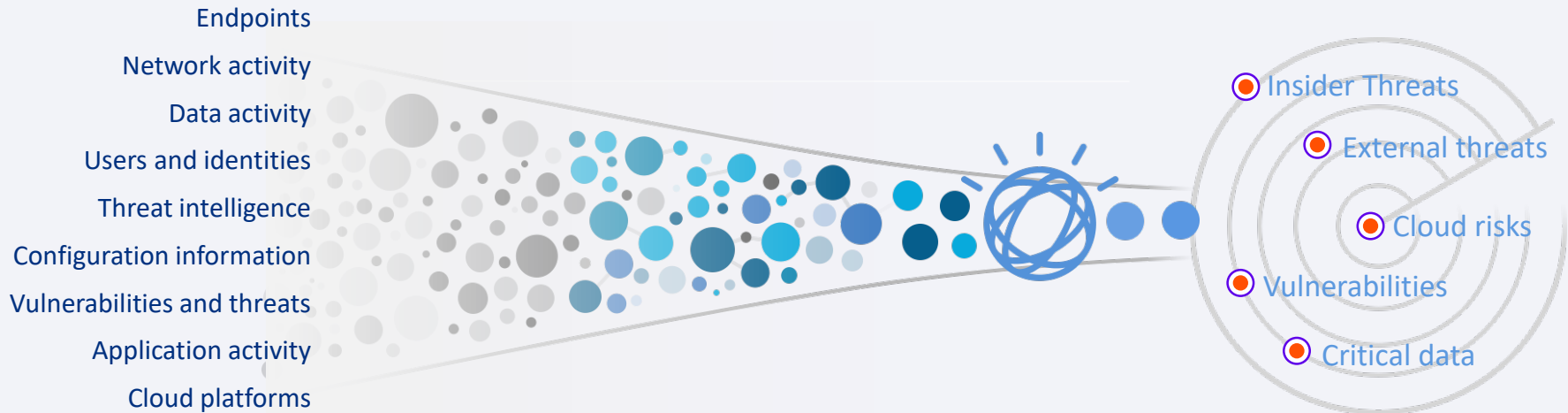
# 4 pillars of effective SIEM

Complete  
Visibility

Prioritized  
Threat Detection

Automated  
Investigations

Integrated  
Response



# 4 pillars of effective SIEM

## Complete Visibility



- Normalization
- Categorization
- Enrichment
- Network, endpoint, cloud, user and application

## Prioritized Threat Detection



- MITRE ATT&CK
- Models
- Behavior chaining
- Global threat intelligence

## Automated Investigations



- AI
- Data mining
- Supervised learning
- Unstructured data analysis
- Federated Search

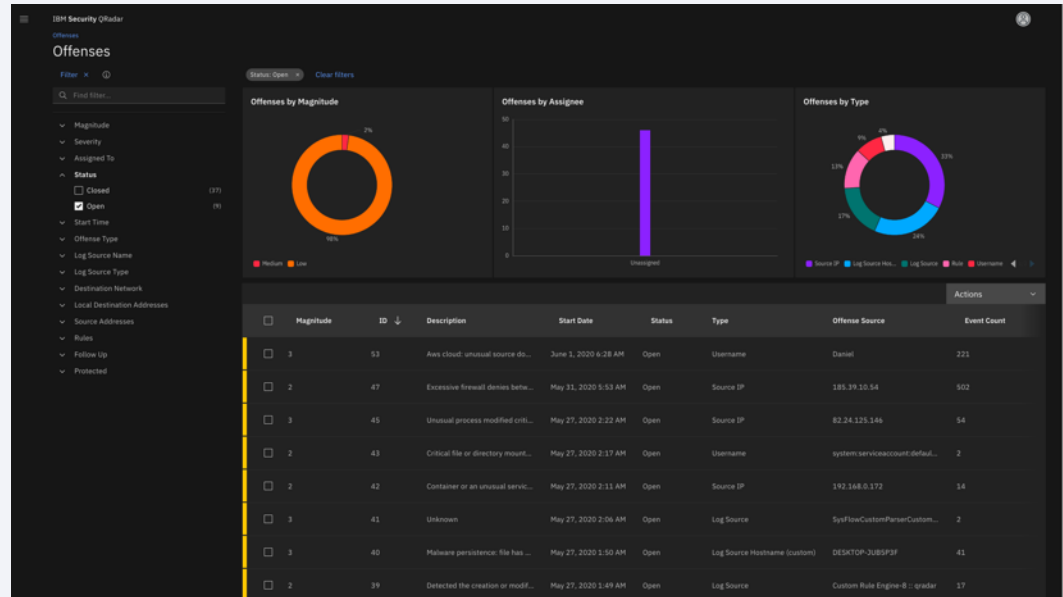
## Integrated Response



- Dynamic playbooks
- Automation
- Orchestration
- Privacy breach reporting

# IBM Security QRadar

- **Unify SOC workflows** by effectively addressing threats with an integrated visibility, detection, investigation and response platform
- **Augment security staff** with AI-assisted triage and automated response playbooks
- **Mature security operations** with visualized use case coverage, OOTB content, and expert threat intelligence powered by IBM's X-Force IRIS
- **Address regulatory risk** and report on compliance adherence with out-of-the-box content for GDPR, ISO 27001, HIPAA, and more



# Complete visibility

Visibility  
into cloud  
usage and  
risks

Real-time  
insights into  
user  
behavior

The screenshot displays the IBM Security QRadar console interface. The main panel shows a list of events with columns for Event Name, Log Source, Source IP, Destination IP, Event Count, and Event. The events are filtered by 'Unusual activity' and show various AWS Cloud events such as 'AWS Cloud: Detected an API call to...', 'Run Instances', 'Console Login', and 'Successful Login to AWS Console F...'. The right-hand panel provides a detailed view of a selected event, including 'Event Overview' (General Audit Event), 'Event Custom Properties' (Region: us-east-2), and 'Payload' (JSON data). The 'Source and destination information' section shows the Source IP as 213.178.155.78 and Destination IP as 127.0.0.1.

Expose  
threats as  
they move  
across the  
network

Endpoint  
visibility  
with  
Sysmon

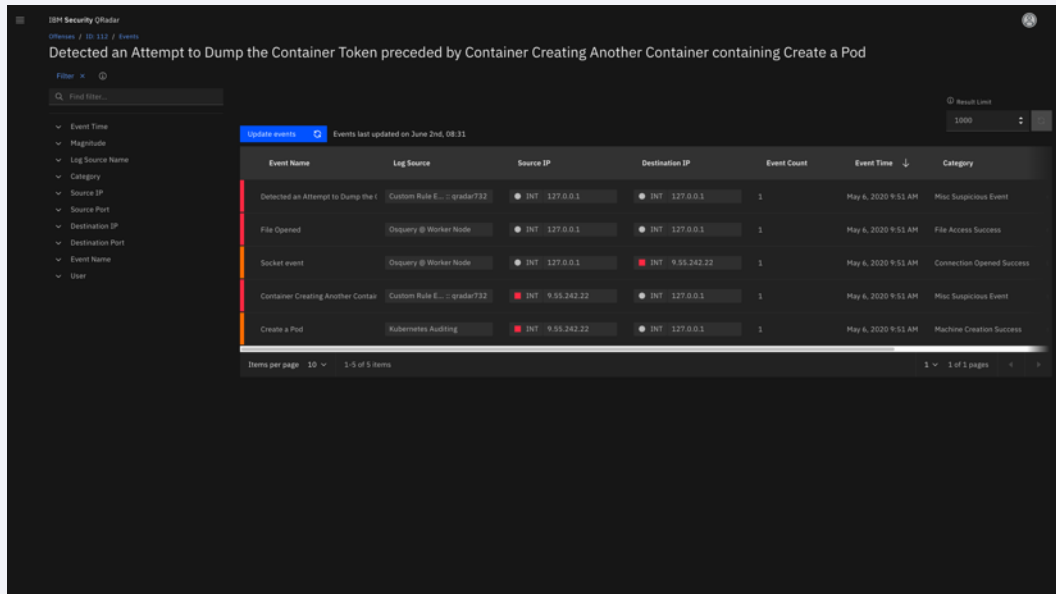
“QRadar drastically reduced the time it took us to connect our 100+hybrid multi-cloud accounts to QRadar. This made it easy to consume both events and network flow traffic from our AWS and other cloud environments.”

Large US-based Insurance Company

# Threat detection

Identify  
known and  
unknown  
threats

Real time  
detection  
across 100's  
of security  
use cases



The screenshot displays the IBM Security QRadar interface. At the top, a header indicates the current offense: "Detected an Attempt to Dump the Container Token preceded by Container Creating Another Container containing Create a Pod". Below this, a table lists individual events. The table has columns for Event Name, Log Source, Source IP, Destination IP, Event Count, Event Time, and Category. The events listed include "Detected an Attempt to Dump the...", "File Opened", "Socket event", "Container Creating Another Contain...", and "Create a Pod". Each event row is color-coded (red, yellow, or green) and includes a status icon. The interface also shows a filter sidebar on the left, a search bar, and pagination controls at the bottom.

Event Name	Log Source	Source IP	Destination IP	Event Count	Event Time	Category
Detected an Attempt to Dump the C...	Custom Rule E... : qradar732	INT 127.0.0.1	INT 127.0.0.1	1	May 6, 2020 9:51 AM	Misc Suspicious Event
File Opened	Osquery @ Worker Node	INT 127.0.0.1	INT 127.0.0.1	1	May 6, 2020 9:51 AM	File Access Success
Socket event	Osquery @ Worker Node	INT 127.0.0.1	INT 9.55.242.22	1	May 6, 2020 9:51 AM	Connection Opened Success
Container Creating Another Contain...	Custom Rule E... : qradar732	INT 9.55.242.22	INT 127.0.0.1	1	May 6, 2020 9:51 AM	Misc Suspicious Event
Create a Pod	Kubernetes-Auditing	INT 9.55.242.22	INT 127.0.0.1	1	May 6, 2020 9:51 AM	Machine Creation Success

Dynamically  
adjust  
as attacks  
unfold

Automaticall  
y link  
multiple  
malicious  
behaviors

"IBM QRadar improves the speed and effectiveness of detecting threats by nearly 75%."

Forrester

# Automated investigation

Let Watson  
automatically  
determine  
threat  
priorities

Map  
investigations to  
MITRE ATT&CK  
tactics and  
techniques

The screenshot shows the IBM Security QRadar Search results page. At the top, there's a 'Query Builder' section with a SQL query: `SELECT magnitude, sourceip, destinationip, QIDDESCRIPTION qid AS 'Event Name', LOGSOURCENAME logsource AS 'Log Source', CONCAT(CATEGORYNAME, 'highLevelCategory', ':') CATEGORYNAME category AS 'Category Name', DATEFORMAT(startTime, 'MM/DD/YYYY') AS 'Start Time' FROM events WHERE TEXT SEARCH '213.178.155.78' LIMIT 10000 LAST 3 Days`. Below the query builder, there's a table of search results. The table has columns: magnitude, sourceip, destinationip, destinationport, Event Name, Log Source, and Category Name. The results are filtered by 'Log Source Name: AWS' and 'Category: AWS'. The table shows several rows of data, including events like 'Amazon AWS Cloud Trail Store...', 'Get Object', 'List Buckets', 'Run Instances', 'Object Download Attempt', 'Virtual Machine Creation Attempt', 'Read Activity Attempted', and 'General Audit Event'.

magnitude	sourceip	destinationip	destinationport	Event Name	Log Source	Category Name
2	213.178.155.78	127.0.0.1	0	Amazon AWS Cloud Trail Store...	AWS	Unknown Stored
2	213.178.155.78	127.0.0.1	0	Get Object	AWS	Audit Object Download Attempt
2	213.178.155.78	127.0.0.1	0	List Buckets	AWS	Audit Read Activity Attempted
2	213.178.155.78	127.0.0.1	0	Run Instances	AWS	Audit Virtual Machine Creation...
2	213.178.155.78	127.0.0.1	0	Run Instances	AWS	Audit Virtual Machine Creation...
2	213.178.155.78	127.0.0.1	0	Run Instances	AWS	Audit Virtual Machine Creation...
2	213.178.155.78	127.0.0.1	0	Run Instances	AWS	Audit Virtual Machine Creation...
2	213.178.155.78	127.0.0.1	0	Run Instances	AWS	Audit Virtual Machine Creation...
2	213.178.155.78	127.0.0.1	0	Run Instances	AWS	Audit Virtual Machine Creation...
2	213.178.155.78	127.0.0.1	0	Run Instances	AWS	Audit Virtual Machine Creation...

Understand the  
source and impact  
of the attack so you  
can respond  
effectively

Hunt threats via a  
search

“QRadar offers strong support for incident investigation by providing context enrichment from internal and external sources, suggesting next steps based on attacker actions and prioritizing alerts for further action.”

Gartner



# Integrated response

Guided response  
and case  
management to  
help analysts

Align compliance  
and privacy  
through breach  
reporting support

The screenshot displays the IBM Security Integrated Response console. At the top, a progress bar shows '6% Complete'. Below this, a table lists tasks with columns for Task Name, Owner, Due Date, Flags, and Actions. The tasks are categorized into 'Initial' (ping host 192.168.0.8) and 'Engage' (Notify DPO). A detailed view of the 'Engage' task is shown, including instructions for analyzing indicators of compromise and detecting/analyzing malware. The right sidebar provides metadata for the incident, including phase (Engage), dates, incident type (Malware), people involved (Jamie Cowper, L1 Team, Orchestration Engine), related incidents, and a newsfeed of updates.

Task Name	Owner	Due Date	Flags	Actions
<b>Initial</b>				
ping host 192.168.0.8	Orchestration ...	No due date		
<b>Engage</b>				
Notify DPO	Unassigned	03/05/2020		
Analyse Indicators of Compromise (Artifacts)				
Disconnect or isolate malware-infected systems				
Analyze malware-infected systems				
Review the output and status of anti-virus software				
Research AV vendor databases				
Analyze network traffic for malware activity				

**Instructions**

Look for attributes of the malware. Ideally you should leverage a purpose-built forensic workstation to perform this analysis (e.g. <http://computer-forensics.sans.org/community/downloads>). Determine the type of malware, how it is being transported, how it infects the system, etc. Look for specific attributes that can be used to identify, contain and eradicate it. Try to determine a vector common to all systems experiencing anomalous behavior (or having been rendered unavailable) - from which a malicious payload could have been delivered. Examples include centralized enterprise applications, centralized file shares (for which the identified systems were mapped or had access), privileged user account common to the identified systems, network segment or boundary, or a common DNS server for name resolution. It is important not to trust software and utilities on the infected system as

**Phase** Engage

**Date Created** 03/04/2020

**Date Occurred** 03/04/2020

**Next Due Date** 03/04/2020

**Incident Type** Malware

**People**

**Created By** Jamie Cowper

**Owner** Jamie Cowper

**Members** L1 Team, Orchestration Engine

**Related Incidents**

- #6849 Suspected APT - infected machine...
- #6858 APT41 - multiple endpoints
- #6859 Targeted phishing attack - AWS a...

**Attachments**

There are no attachments.

**Newsfeed**

- Slawek Gawlowski updated the task list on the Incident a day ago
- Slawek Gawlowski modified the Incident a day ago
- Orchestration Engine changed status to Closed on the task ping host 192.168.0.8 a day ago

Act fast with  
automation and  
orchestration across  
security and IT Ops  
tools

Measure results,  
improve visibility  
with incident and  
SOC dashboards

“We refer to the whole IBM ecosystem as a force multiplier; we’ve evolved into an organization with a completely comprehensive and dynamic program around security incident response”

Brian Herr, Chief Security and Privacy Officer, Secure-24

# IBM Security QRadar a Leader 11 consecutive times

Clear leader in 'Completeness of Vision' and best position ever.

The 2020 Gartner MQ for SIEM had a strong focus on:

- SOAR, Automation, Incident Response
- Endpoint Analytics
- UBA
- Cloud
- Use of Threat Intelligence

Figure 1. Magic Quadrant for Security Information and Event Management



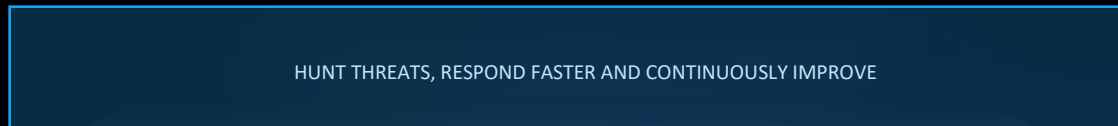
Source: Gartner (February 2020)

# IBM Security QRadar

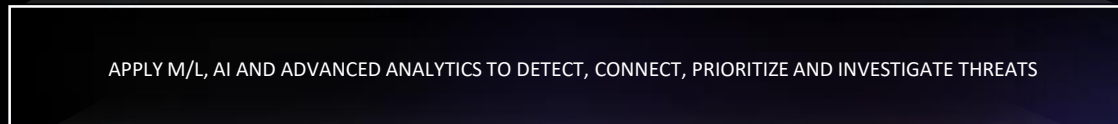
## SOLVE SECURITY CHALLENGES



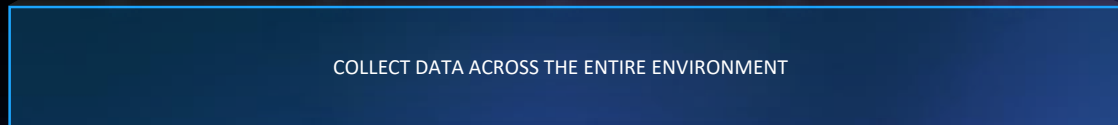
## RESPONSE



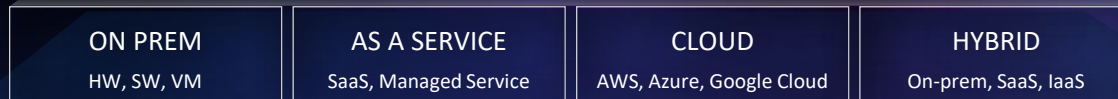
## DETECTION & INVESTIGATION



## VISIBILITY



## DEPLOYMENT MODELS



IBM Security App Exchange

Seamless integration and content to augment platform.

# Happy QRadar customers\*

NRGi



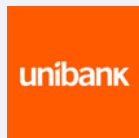
The  
Weather  
Company  
An IBM Business

VISA



TalkTalk

CargillsBank  
BANKING ON THE HUMAN SPIRIT



EXCELLIUM



AT&T



WaveStrong  
Information Security Professionals

(\*Not a complete list)

Designed to make your  
job easier

“The security intelligence from  
X-Force and the out-of-the-box  
analytics capabilities made  
QRadar stand out...”

— CTO, Large IT Consulting Firm

*Independent QRadar Study by Ponemon Institute*

73%

OF CLIENTS RECOGNIZED VALUE  
WITHIN ONE WEEK

50%

FEWER FALSE POSITIVES THAN OTHER  
SIEM SOLUTIONS

“Cargills Bank was able to leapfrog these limitations by using IBM QRadar SIEM and QRadar Advisor with Watson to receive real-time, prioritized alerts. IBM’s best-in-class cognitive security portfolio will help us pre-empt threats and mitigate risk, thereby supporting our position as a leading digital bank.”

**Rohan Muttiah**  
**Chief Operating Officer, Cargills Bank**

# 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.com/ibmsecurity](https://youtube.com/ibmsecurity)

© Copyright IBM Corporation 2020. 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.

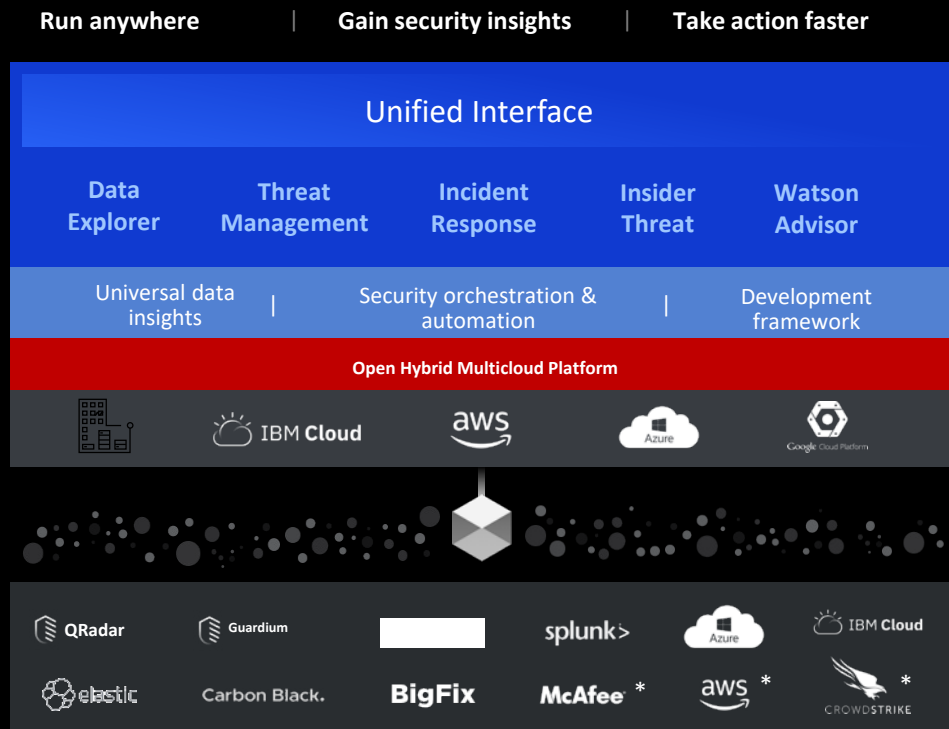




IBM Security QRadar

# Back up slides

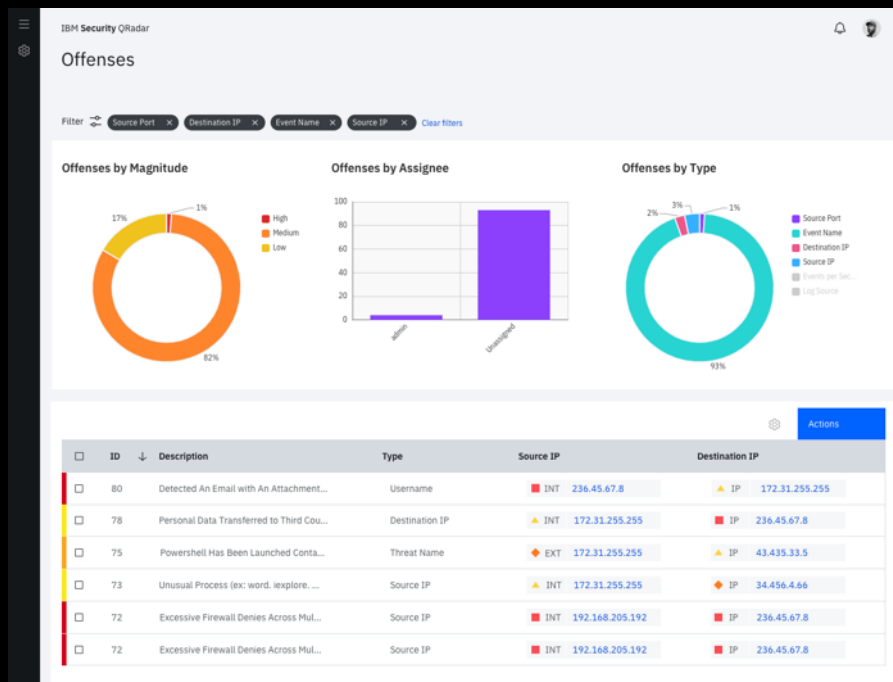
# Simplify and modernize on a single architecture with CP4S



- Unified architecture with a consistent and integrated UX
- Seamlessly leverage existing data and security systems without moving them
- Streamline workflows with case management, orchestration, and automation at the core
- Open, standards-based, multi-cloud platform based on Red Hat OpenShift enables future-proof freedom of choice
- Ecosystem of technology and partners unlocking innovation and simplicity
- Consistent, simplified and streamlined pricing

# Threat Detection & Investigation

- **Unify SOC workflows** by effectively addressing threats with an integrated visibility, detection, investigation and response platform
- **Augment security staff** with AI-assisted triage and automated response playbooks
- **Mature security operations** with visualized use case coverage, OOTB content, and expert threat intelligence powered by IBM's X-Force IRIS
- **Address regulatory risk** and report on compliance adherence with out-of-the-box content for GDPR, ISO 27001, HIPAA, and more



IBM Security QRadar

# Add additional sub-product slides here