IBM Security QRadar SOAR

Let's secure.

Use Case:
A day in the life of a security analyst.

A deep-dive presentation and demonstration of IBM Security QRadar SOAR.

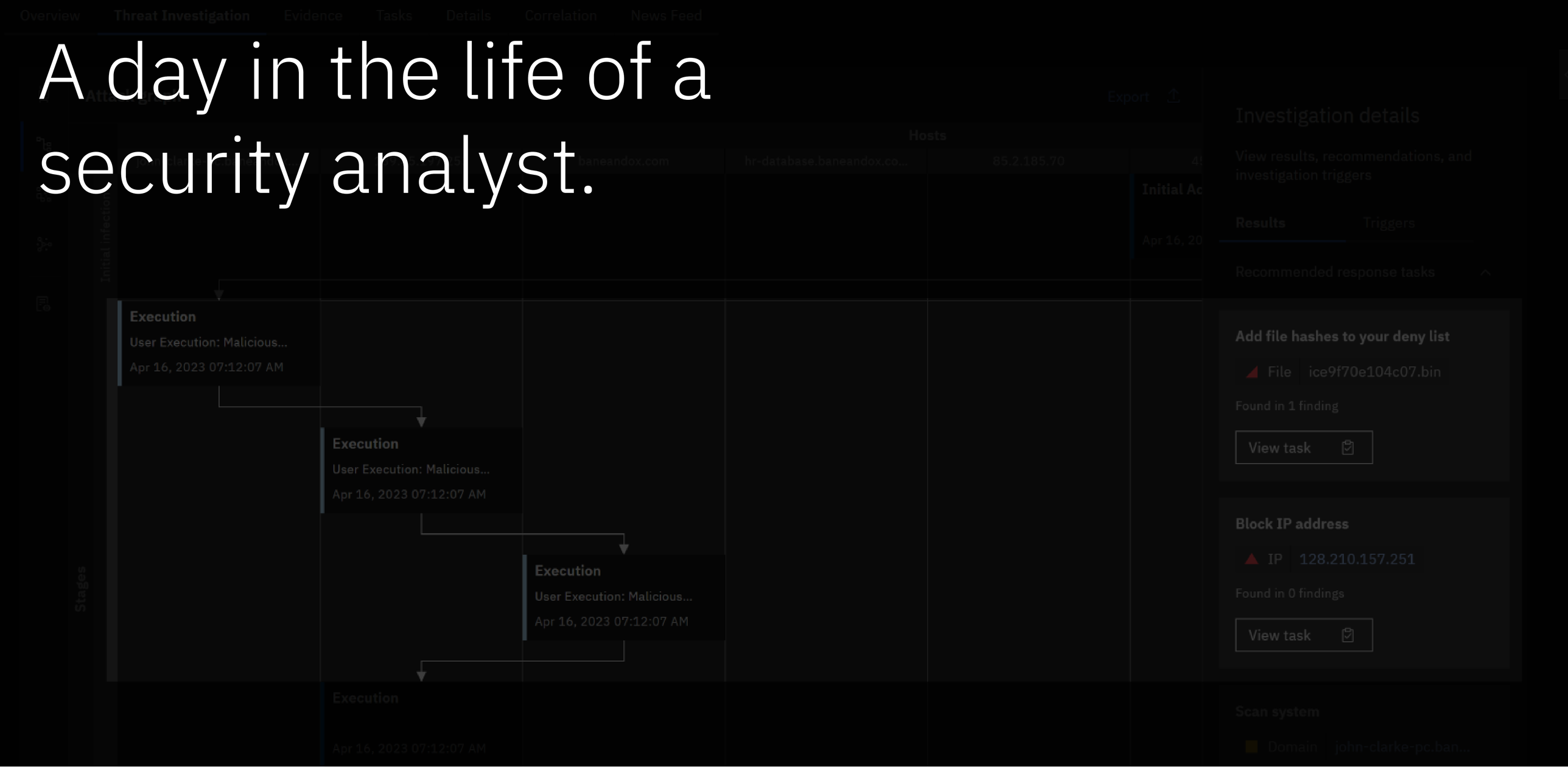
IBM **Security**

IBM

Presentation Agenda

- A day in the life of a security analyst
- L300 demonstration
- Key Takeaways
- How to get more information.

A day in the life of a security analyst.



IBM Security QRadar SOAR UAX vs. standard analyst workflow.

Provide security orchestration, automation, and response at scale.

SaaS delivery

Delivered in AWS, functional across entire tech landscape.

Hybrid cloud

AWS, Azure, IBM Cloud & more.

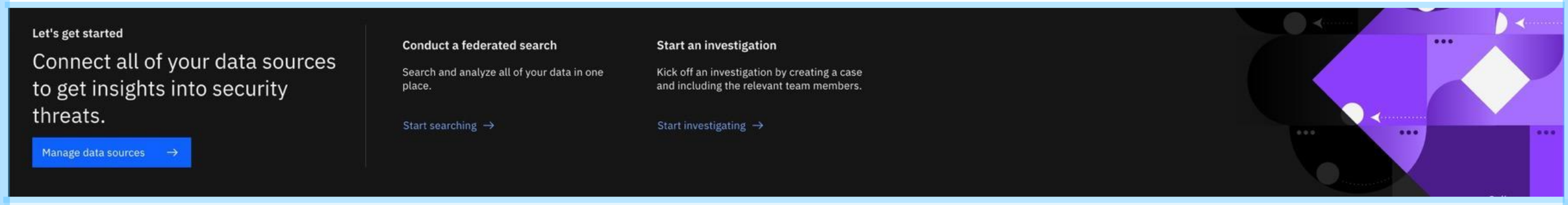
On-premise

Bare metal, Virtualization, Datacenter

Multi-tenant Support

Multi-tenant support

Optimized for multi-tenant MSSP deployment model



Case Management

AI & Automation

Dynamic Playbooks

FS

Federated Search

Single Pane of Glass

Unified Analyst Experience

Cut the confusion of disparate security solutions.

Accelerate incident response times

reddot winner 2022

Manual workflows brings inefficiencies

Security analyst's typical workflow complexity

8 tools/panes of glass

19 steps

~10 hours response time

Triage

1 Review open incidents
2 Classify highest priority
3 Start Triage
4 Start investigation

Investigation

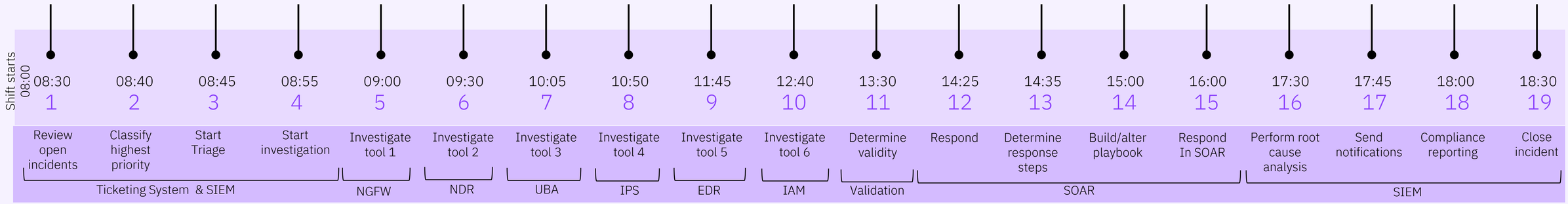
5 Tool 1 NGFW
6 Tool 2 NDR
7 Tool 3 UBA
8 Tool 4 IPS
9 Tool 5 EDR
10 Tool 6 IAM
11 Determine validity

Response

12 Respond
13 Build/alter playbook
14 Determine response steps
15 Respond In SOAR

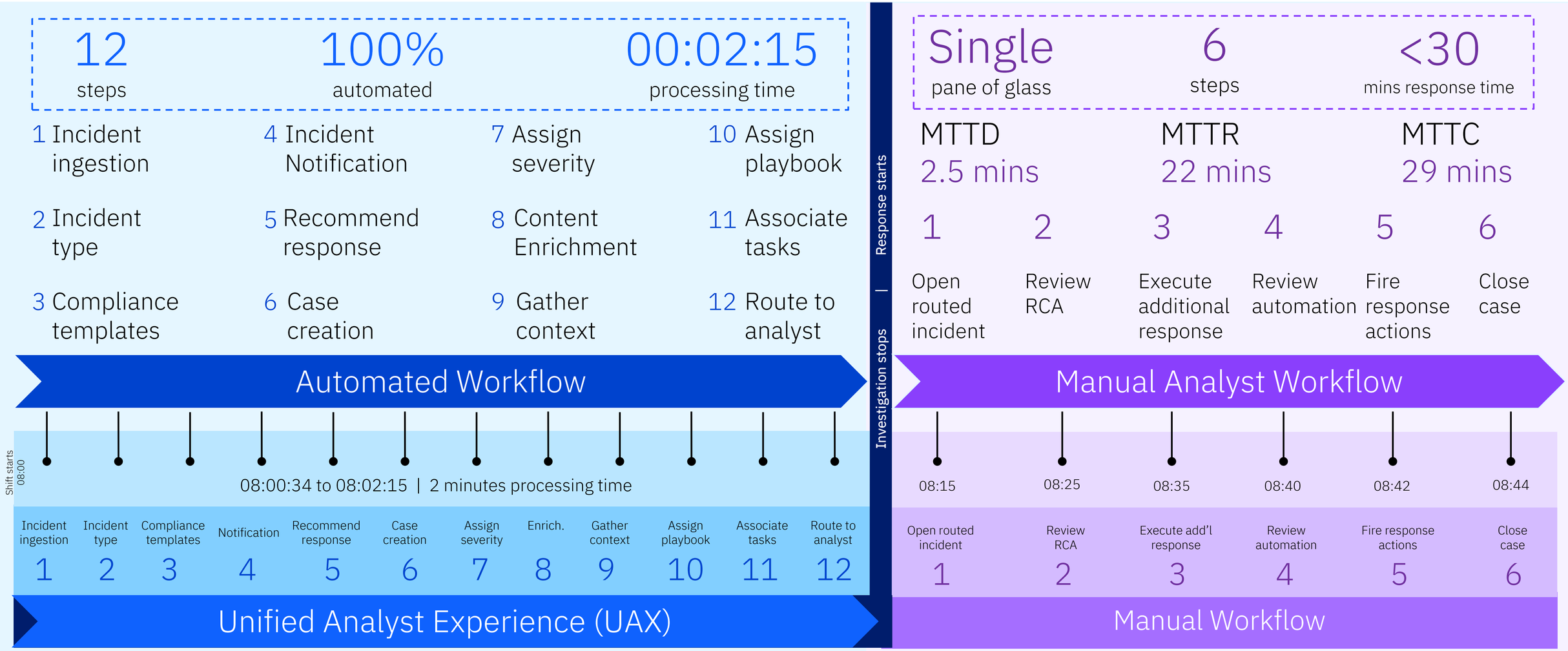
Closure

16 Perform root cause analysis
17 Send notifications
18 Compliance reporting
19 Close incident

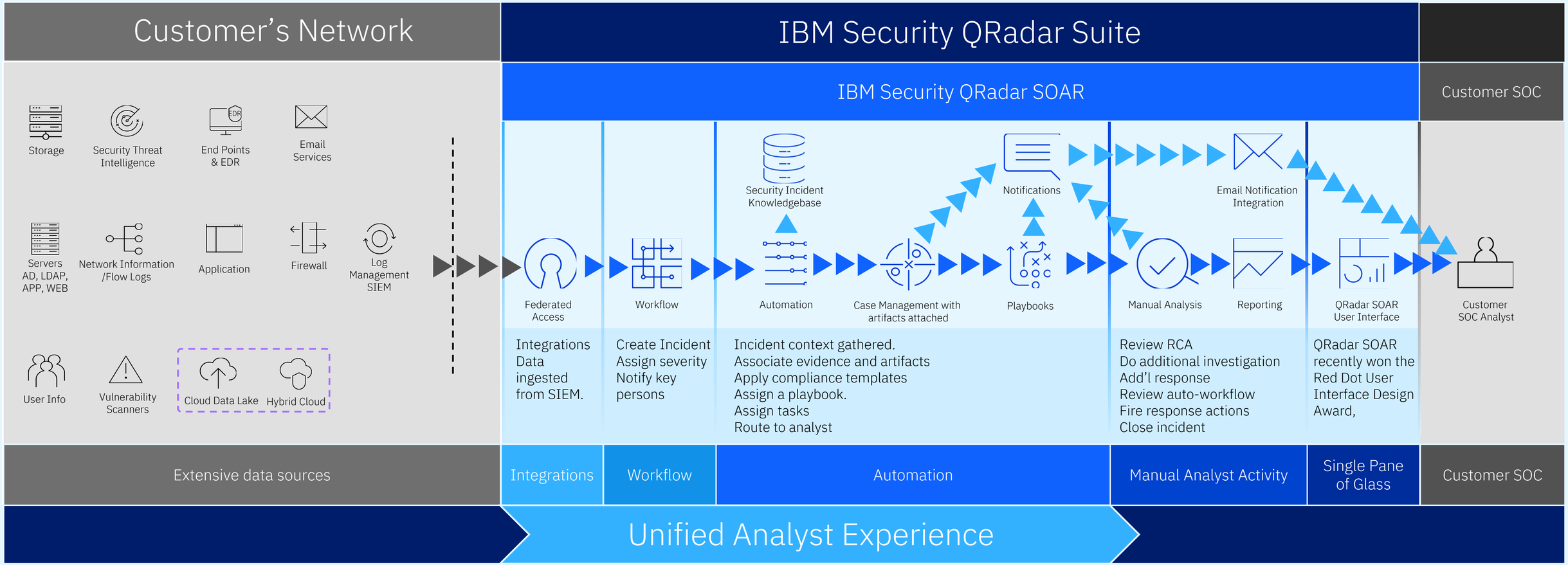


Automated workflows brings efficiencies

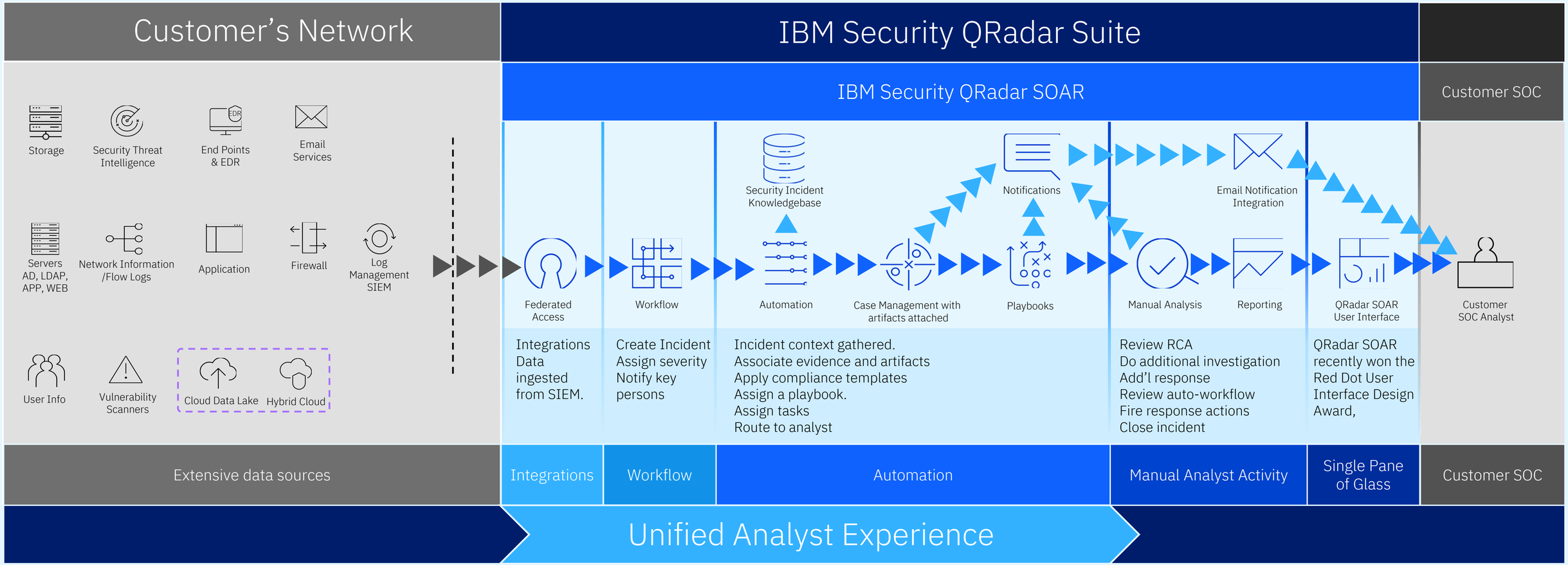
Security analyst's workflow using QRadar SOAR with Unified Analyst Experience (UAX)



Automation powered by IBM Security QRadar SOAR?



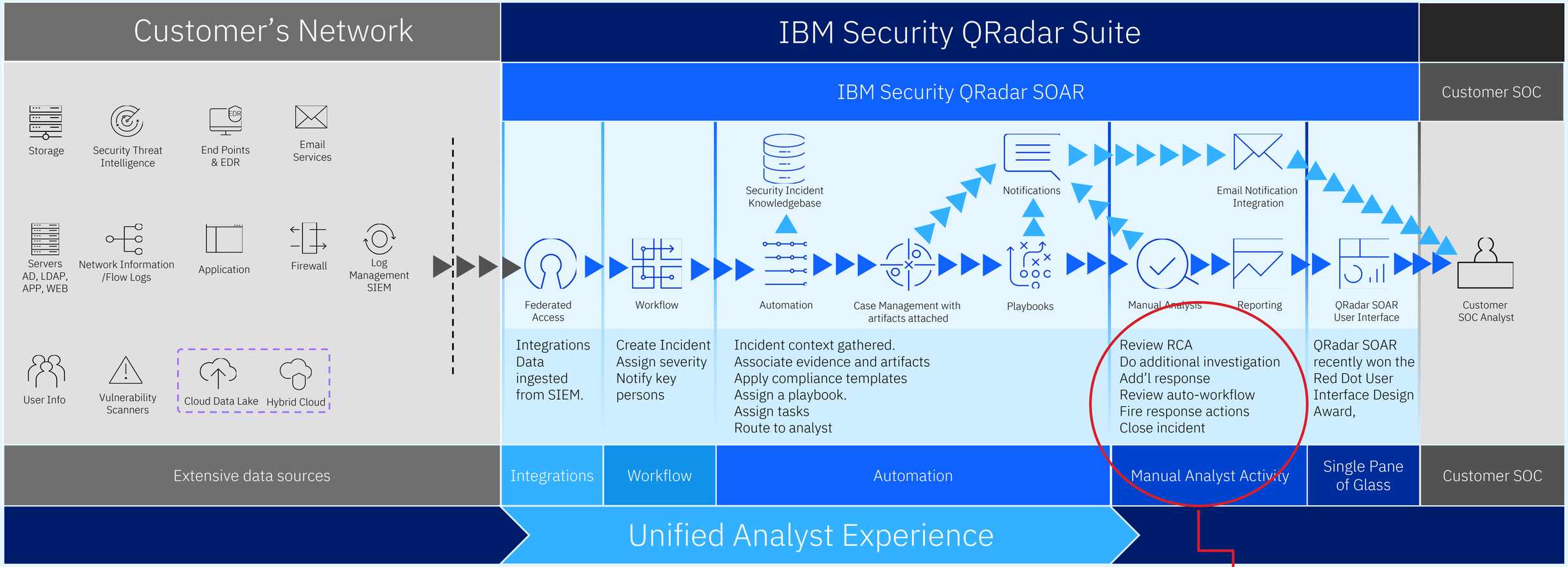
Automation powered by IBM Security QRadar SOAR?



QRadar SOAR processes 12 steps with AI and automation in just 2.5 minutes

Traditional SOC workflow and processes took ~10 hours to remediate

Automation powered by IBM Security QRadar SOAR?



Traditional SOC workflow
~10 hours to remediate

Thousands of integrations at the center of our ecosystem.

300+ integrations specifically built for QRadar SOAR

Open source and open community

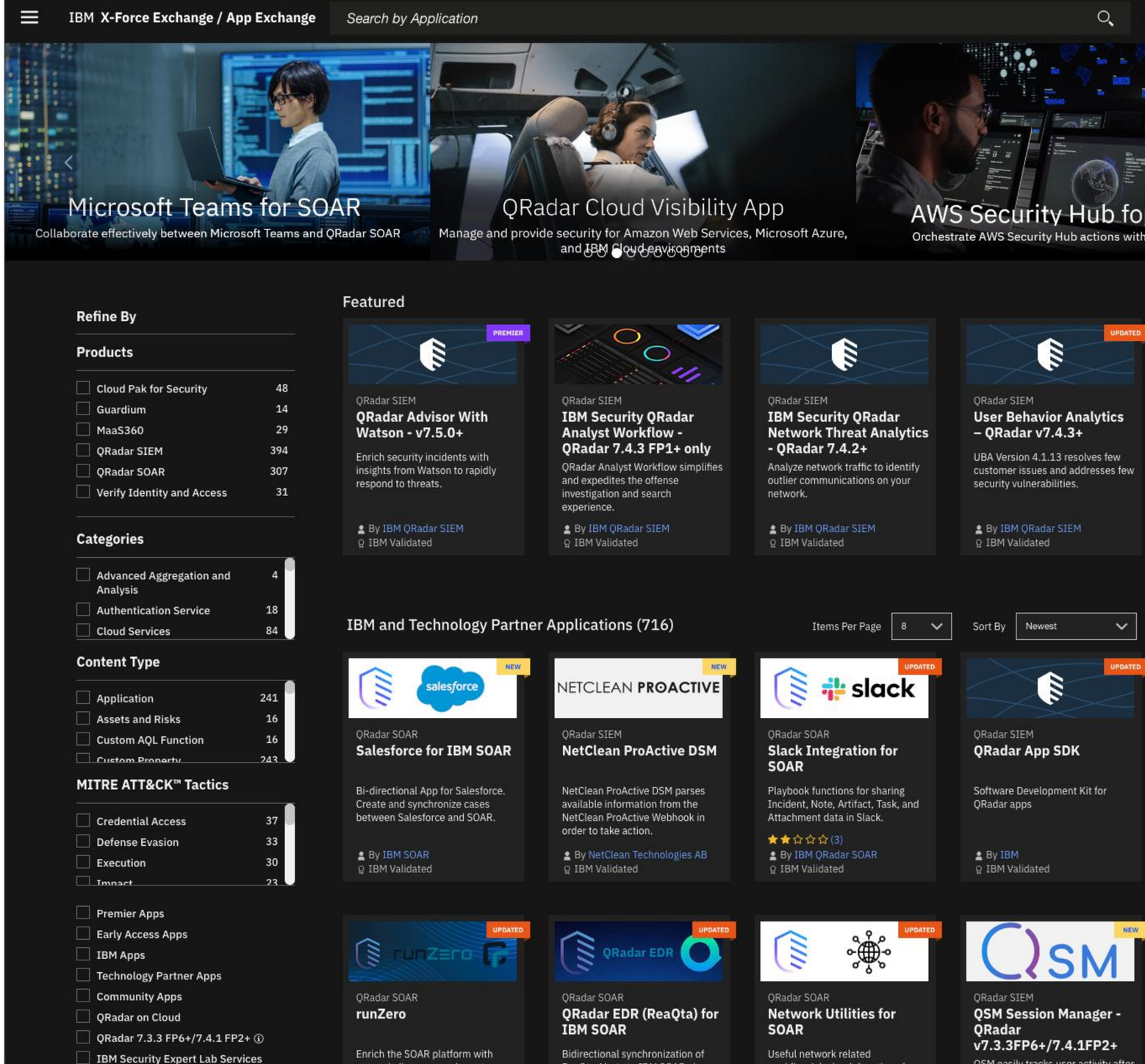
MITRE ATT&CK™

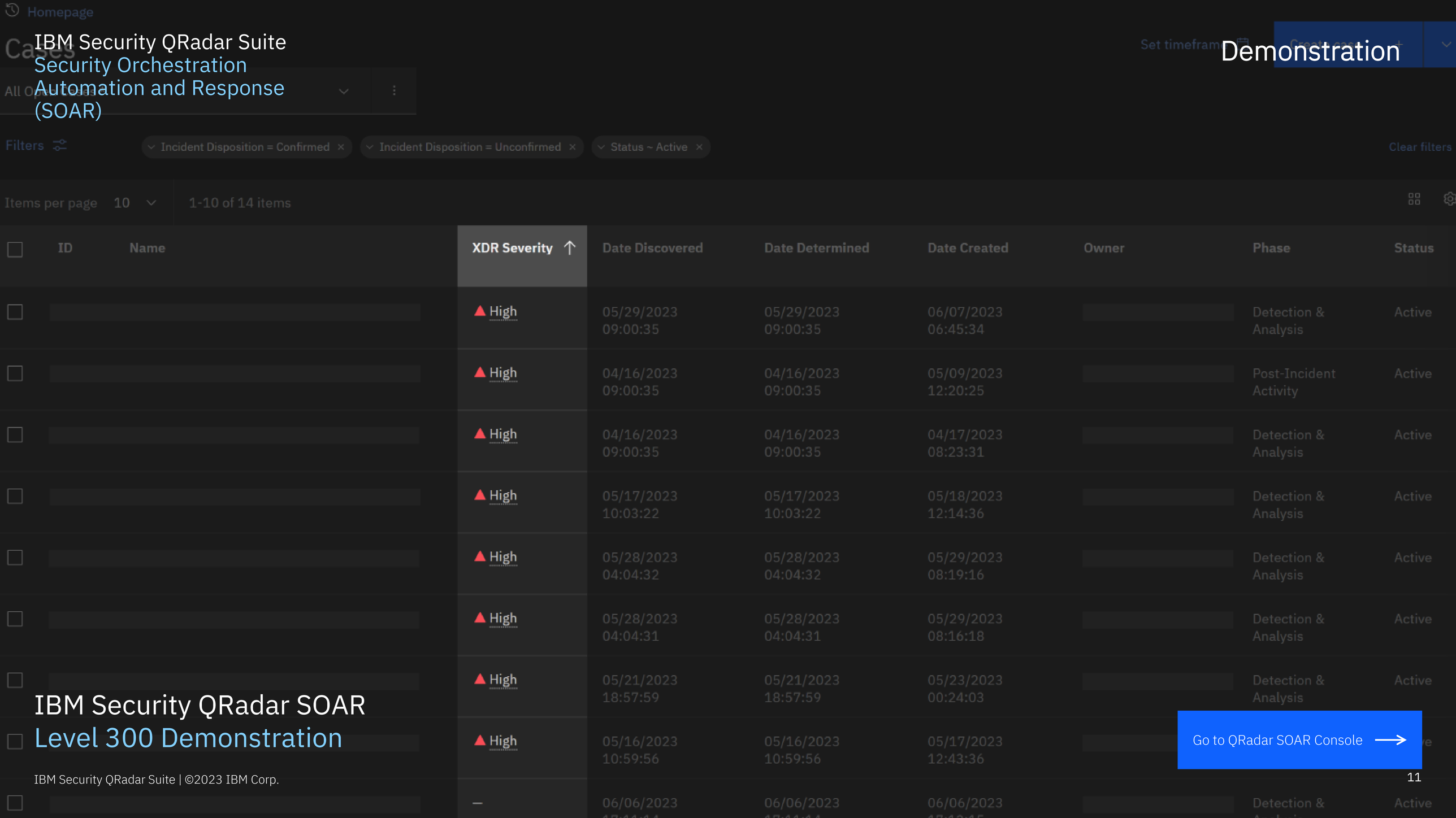
OPEN CYBERSECURITY ALLIANCE

fido™ ALLIANCE

Open Cybersecurity Schema Framework

quad9





IBM Security QRadar Suite
Security Orchestration Automation and Response (SOAR)

Demonstration

IBM Security QRadar SOAR
Level 300 Demonstration

Go to QRadar SOAR Console →

Key Takeaways

AI and automation

QRadar SOAR uses AI and automation to identify anomalous threats and act on them. Stopping known and unknown threats alike.

Breach response

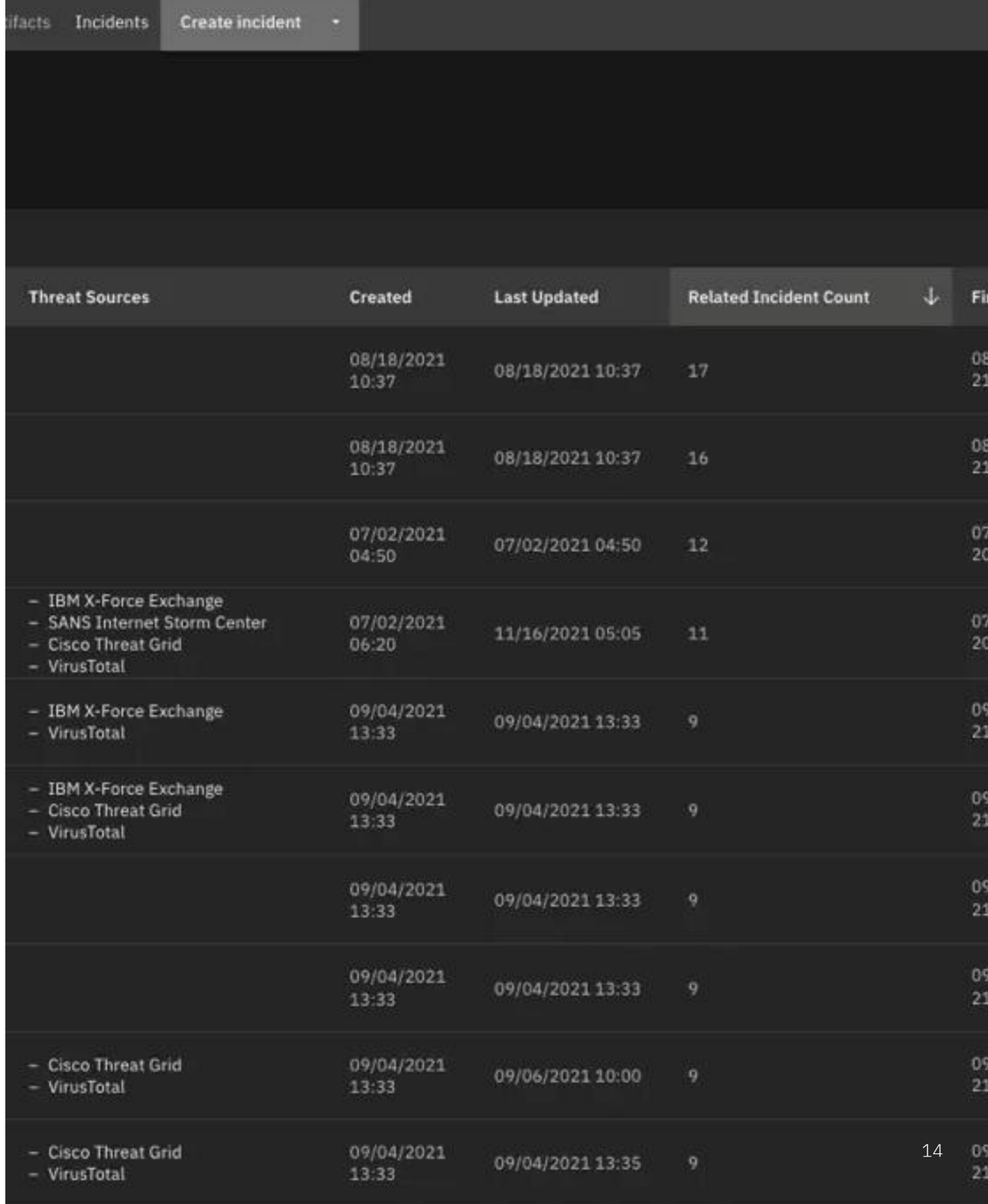
Respond to privacy breaches by integrating privacy reporting tasks into incident response playbooks. Easily address 200+ compliance regulations.

Unified Analyst Experience

The game changing feature that enables analysts to detect and respond to threats in minutes vs days, all in a single pane of glass.

Playbook Designer

QRadar SOAR's playbook designer is a winner of the red dot award for user interface design and ease of use.



Accelerate security operations

Book a deep dive with an IBM rep to learn about the IBM Security QRadar Suite products.

Experience

Request an IBM Security QRadar SOAR demo to see the power of QRadar for yourself.

Request a SOAR demo

Join

The QRadar SOAR Community to keep up with the latest QRadar news and announcements.

IBM Security Community

Read

IBM Security QRadar SOAR and QRadar SIEM Integration. Download the solution brief.

Download the Solution Brief


IBM