

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.

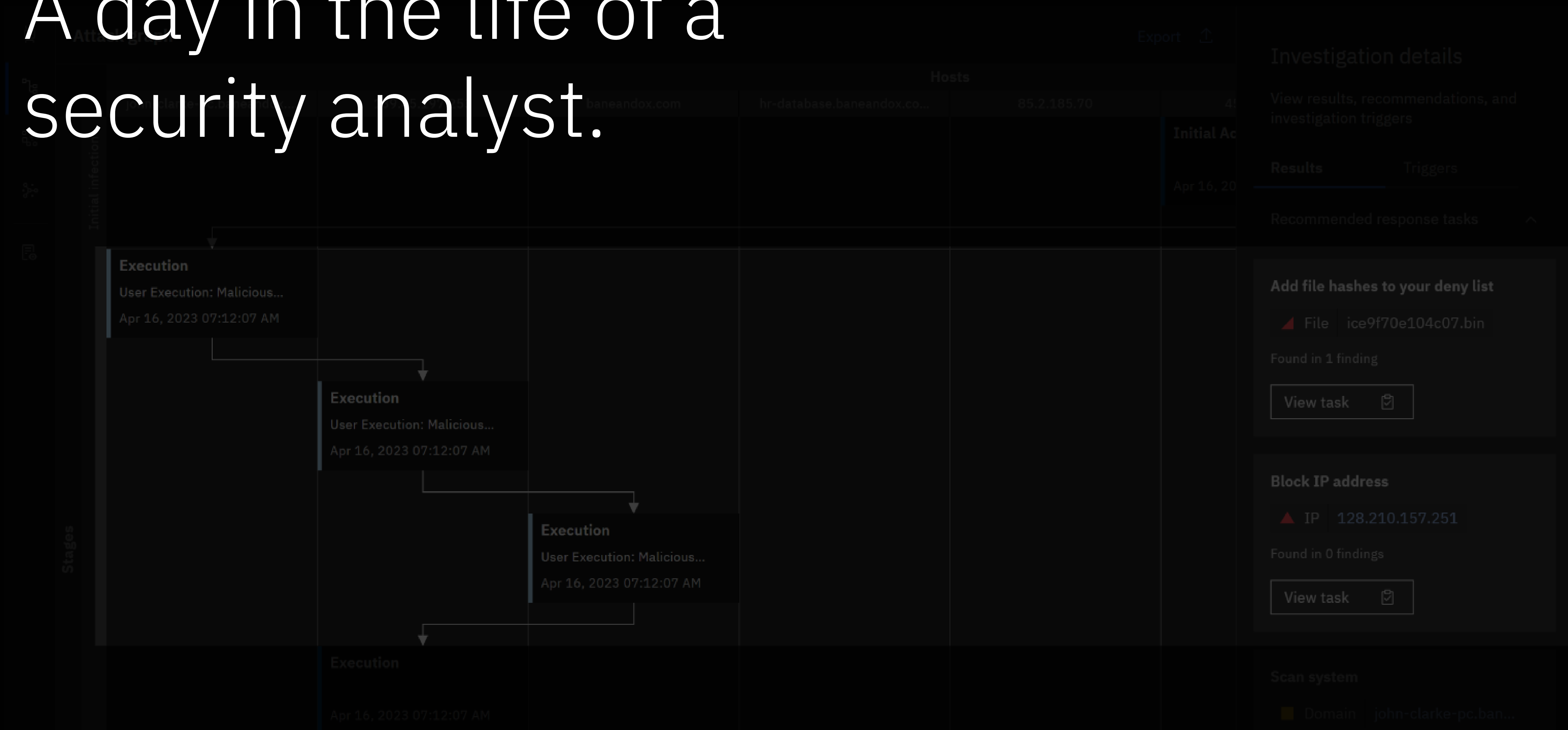
IBM Security



Presentation Agenda

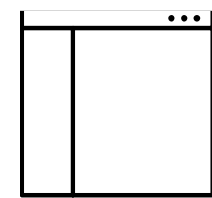
- A day in the life of a security analyst
- L300 demonstration
- Key Takeaways
- How to get more information.

A day in the life of a security analyst.



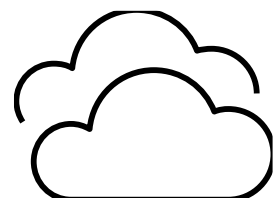
IBM Security QRadar SOAR UAX vs. standard analyst workflow.

Provide security orchestration, automation, and response at scale.



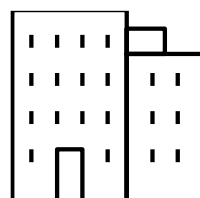
SaaS delivery

Delivered in AWS, functional across entire tech landscape.



Hybrid cloud

AWS, Azure, IBM Cloud & more.



On-premise

Bare metal, Virtualization, Datacenter



Multi-tenant support

Optimized for multi-tenant MSSP deployment model

Let's get started

Connect all of your data sources to get insights into security threats.

Manage data sources →

Conduct a federated search

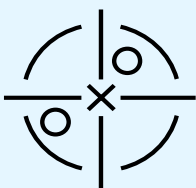
Search and analyze all of your data in one place.

Start searching →

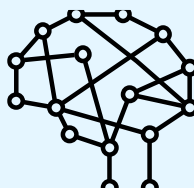
Start an investigation

Kick off an investigation by creating a case and including the relevant team members.

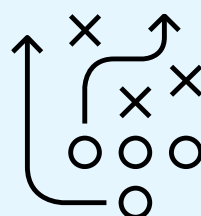
Start investigating →



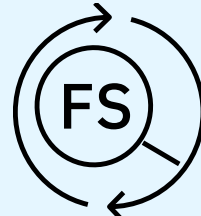
Case Management



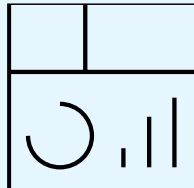
AI & Automation



Dynamic Playbooks

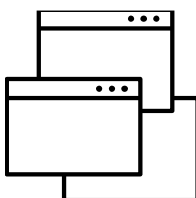


Federated Search

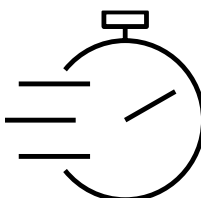


Single Pane of Glass

Unified Analyst Experience



Cut the confusion of disparate security solutions.



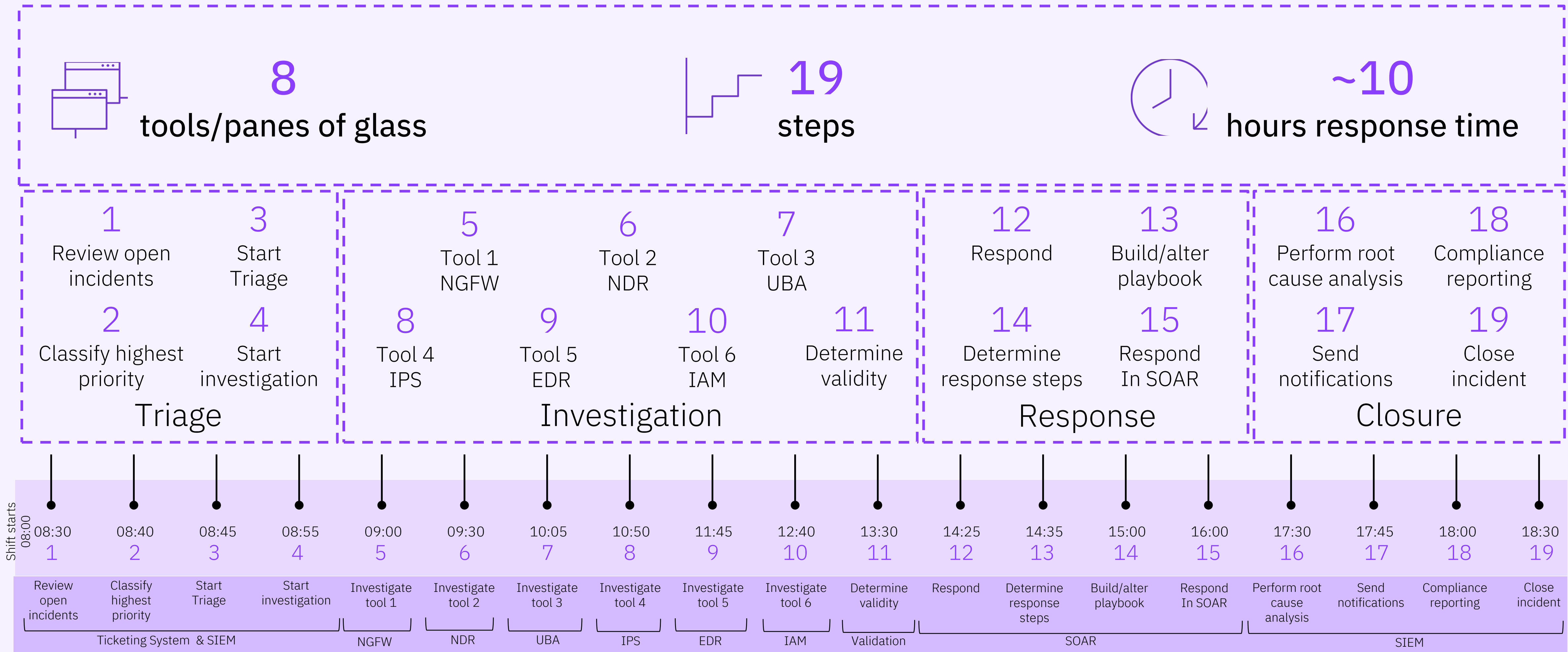
Accelerate incident response times



reddot winner 2022

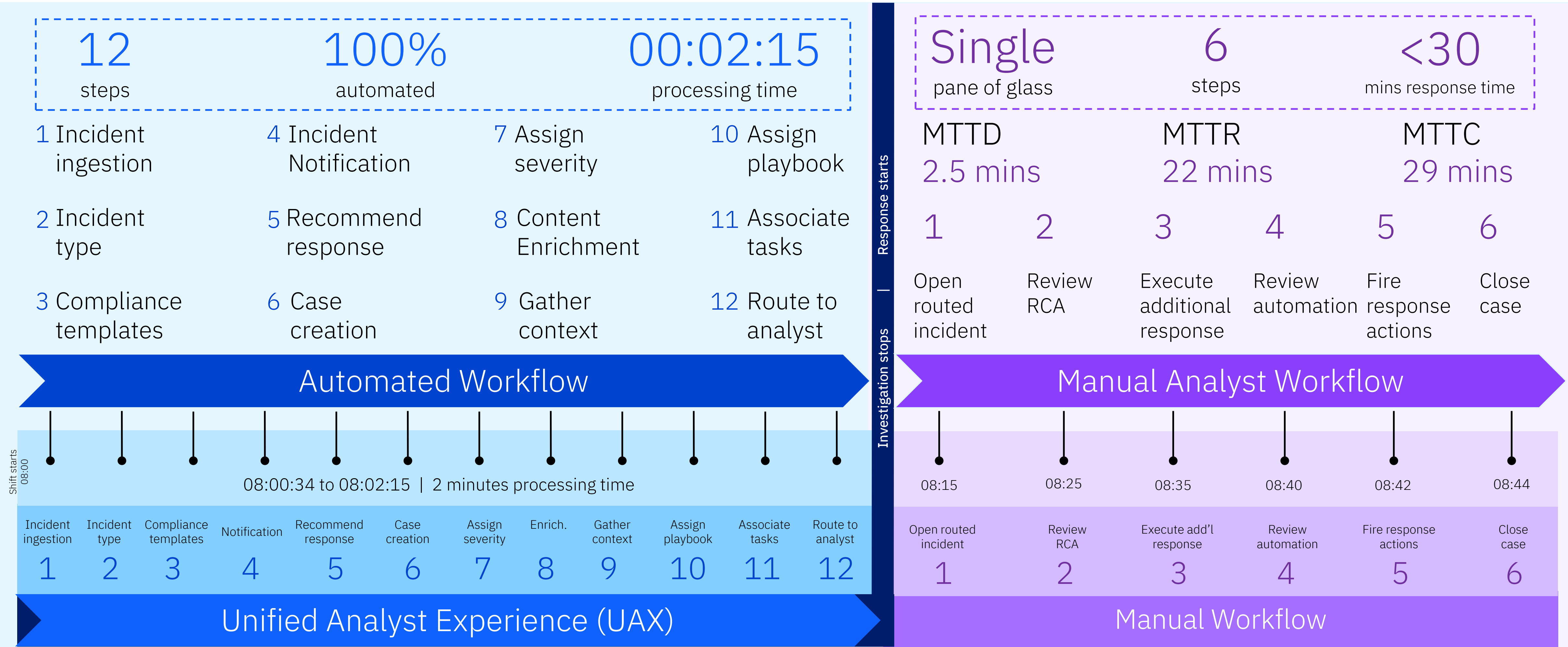
Manual workflows brings inefficiencies

Security analyst's *typical workflow complexity*

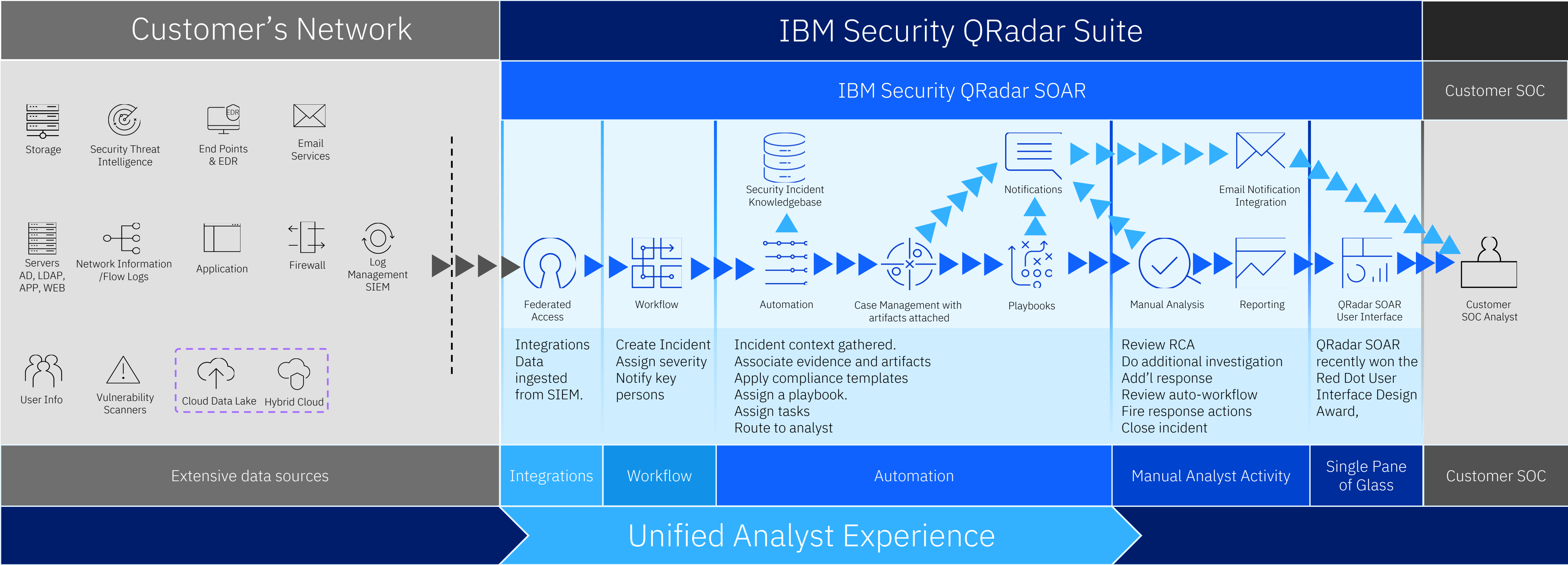


Automated workflows brings efficiencies

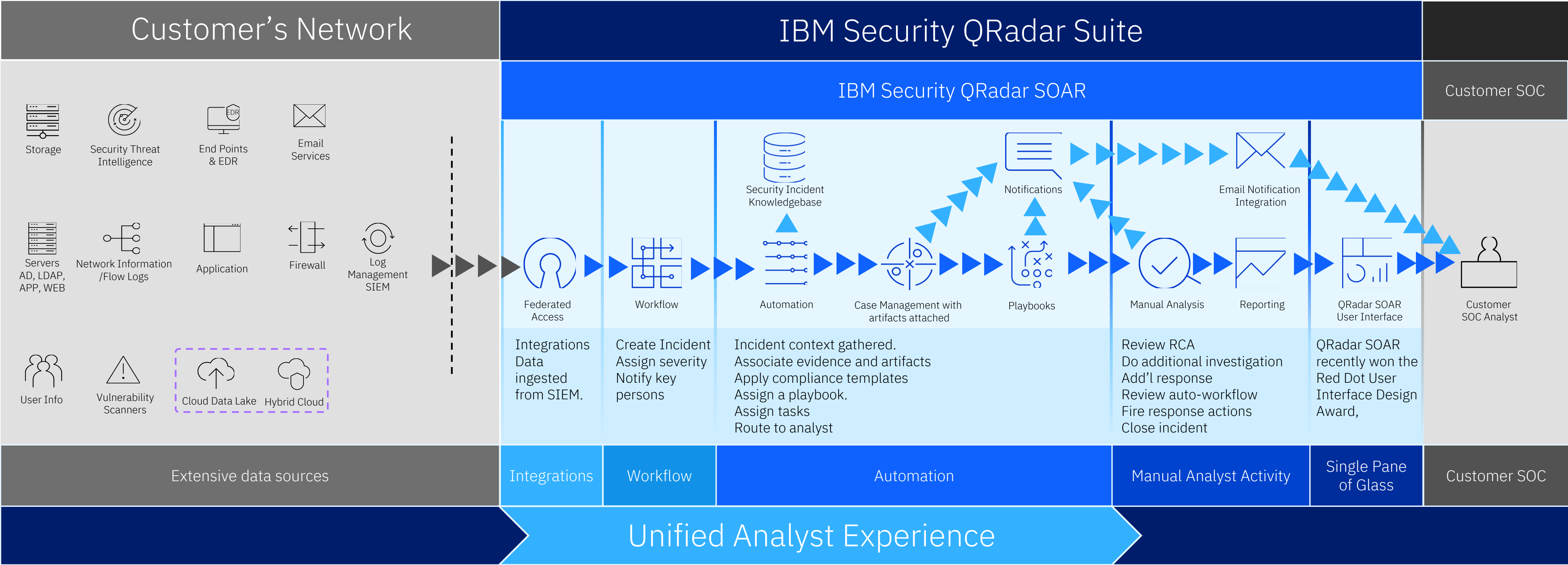
Security analyst's workflow using QRadar SOAR with [Unified Analyst Experience \(UAX\)](#)



Automation powered by IBM Security QRadar SOAR?

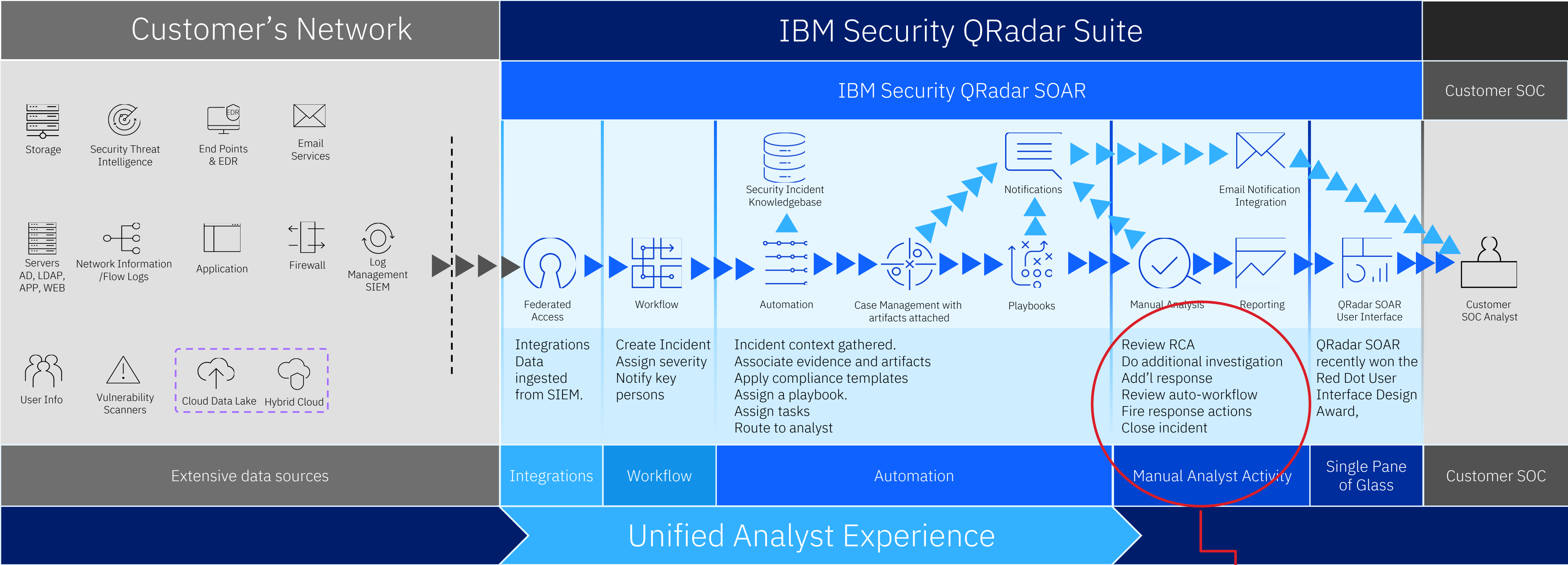


Automation powered by IBM Security QRadar SOAR?



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



IBM X-Force Exchange / App Exchange Search by Application

Microsoft Teams for SOAR Collaborate effectively between Microsoft Teams and QRadar SOAR

QRadar Cloud Visibility App Manage and provide security for Amazon Web Services, Microsoft Azure, and IBM Cloud environments

AWS Security Hub for IBM Cloud Environments Orchestrate AWS Security Hub actions with IBM Cloud Environments

Refine By

Products

<input type="checkbox"/> Cloud Pak for Security	48
<input type="checkbox"/> Guardium	14
<input type="checkbox"/> MaaS360	29
<input type="checkbox"/> QRadar SIEM	394
<input type="checkbox"/> QRadar SOAR	307
<input type="checkbox"/> Verify Identity and Access	31

Categories

<input type="checkbox"/> Advanced Aggregation and Analysis	4
<input type="checkbox"/> Authentication Service	18
<input type="checkbox"/> Cloud Services	84

Content Type

<input type="checkbox"/> Application	241
<input type="checkbox"/> Assets and Risks	16
<input type="checkbox"/> Custom AQL Function	16
<input type="checkbox"/> Custom Property	243

MITRE ATT&CK™ Tactics

<input type="checkbox"/> Credential Access	37
<input type="checkbox"/> Defense Evasion	33
<input type="checkbox"/> Execution	30
<input type="checkbox"/> Impact	23

Featured

QRadar SIEM QRadar Advisor With Watson - v7.5.0+ PREMIER

Enrich security incidents with insights from Watson to rapidly respond to threats.

By IBM QRadar SIEM IBM Validated

QRadar SIEM IBM Security QRadar Analyst Workflow - QRadar 7.4.3 FP1+ only

QRadar Analyst Workflow simplifies and expedites the offense investigation and search experience.

By IBM QRadar SIEM IBM Validated

QRadar SIEM IBM Security QRadar Network Threat Analytics - QRadar 7.4.2+

Analyze network traffic to identify outlier communications on your network.

By IBM QRadar SIEM IBM Validated

QRadar SIEM User Behavior Analytics - QRadar v7.4.3+ UPDATED

UBA Version 4.1.13 resolves few customer issues and addresses few security vulnerabilities.

By IBM QRadar SIEM IBM Validated

IBM and Technology Partner Applications (716)

Items Per Page 8 Sort By Newest

NEW **salesforce**

QRadar SOAR Salesforce for IBM SOAR

Bi-directional App for Salesforce. Create and synchronize cases between Salesforce and SOAR.

By IBM SOAR IBM Validated

NEW **NETCLEAN PROACTIVE**

QRadar SIEM NetClean ProActive DSM

NetClean ProActive DSM parses available information from the NetClean ProActive Webhook in order to take action.

By NetClean Technologies AB IBM Validated

UPDATED **slack**

QRadar SOAR Slack Integration for SOAR

Playbook functions for sharing Incident, Note, Artifact, Task, and Attachment data in Slack.

★★★★☆ (3)

By IBM QRadar SOAR IBM Validated

UPDATED

QRadar SIEM QRadar App SDK

Software Development Kit for QRadar apps

By IBM IBM Validated

UPDATED **runZero**

QRadar SOAR runZero

Enrich the SOAR platform with

UPDATED **QRadar EDR (ReaQta) for IBM SOAR**

Bidirectional synchronization of

UPDATED **Network Utilities for SOAR**

Useful network related

NEW **QSM**

QRadar SIEM QSM Session Manager - QRadar v7.3.3FP6+/7.4.1FP2+

QSM easily tracks user activity after

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

Filters

Incident Disposition = Confirmed

Incident Disposition = Unconfirmed

Status ~ Active

Clear filters

Items per page: 10

1-10 of 14 items

	ID	Name	XDR Severity	Date Discovered	Date Determined	Date Created	Owner	Phase	Status
<input type="checkbox"/>			<div><div></div>High</div>	05/29/2023 09:00:35	05/29/2023 09:00:35	06/07/2023 06:45:34		Detection & Analysis	Active
<input type="checkbox"/>			<div><div></div>High</div>	04/16/2023 09:00:35	04/16/2023 09:00:35	05/09/2023 12:20:25		Post-Incident Activity	Active
<input type="checkbox"/>			<div><div></div>High</div>	04/16/2023 09:00:35	04/16/2023 09:00:35	04/17/2023 08:23:31		Detection & Analysis	Active
<input type="checkbox"/>			<div><div></div>High</div>	05/17/2023 10:03:22	05/17/2023 10:03:22	05/18/2023 12:14:36		Detection & Analysis	Active
<input type="checkbox"/>			<div><div></div>High</div>	05/28/2023 04:04:32	05/28/2023 04:04:32	05/29/2023 08:19:16		Detection & Analysis	Active
<input type="checkbox"/>			<div><div></div>High</div>	05/28/2023 04:04:31	05/28/2023 04:04:31	05/29/2023 08:16:18		Detection & Analysis	Active
<input type="checkbox"/>			<div><div></div>High</div>	05/21/2023 18:57:59	05/21/2023 18:57:59	05/23/2023 00:24:03		Detection & Analysis	Active
<input type="checkbox"/>			<div><div></div>High</div>	05/16/2023 10:59:56	05/16/2023 10:59:56	05/17/2023 12:43:36			Active
<input type="checkbox"/>			—	06/06/2023 17:11:11	06/06/2023 17:11:11	06/06/2023 17:12:15		Detection & Analysis	Active

Set timeframe

Go to console

IBM Security QRadar SOAR
Level 300 Demonstration

IBM Security QRadar Suite | ©2023 IBM Corp.

Go to QRadar SOAR Console

11

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

