The Future of the Modern SOC to address the emerging Cyber Threats

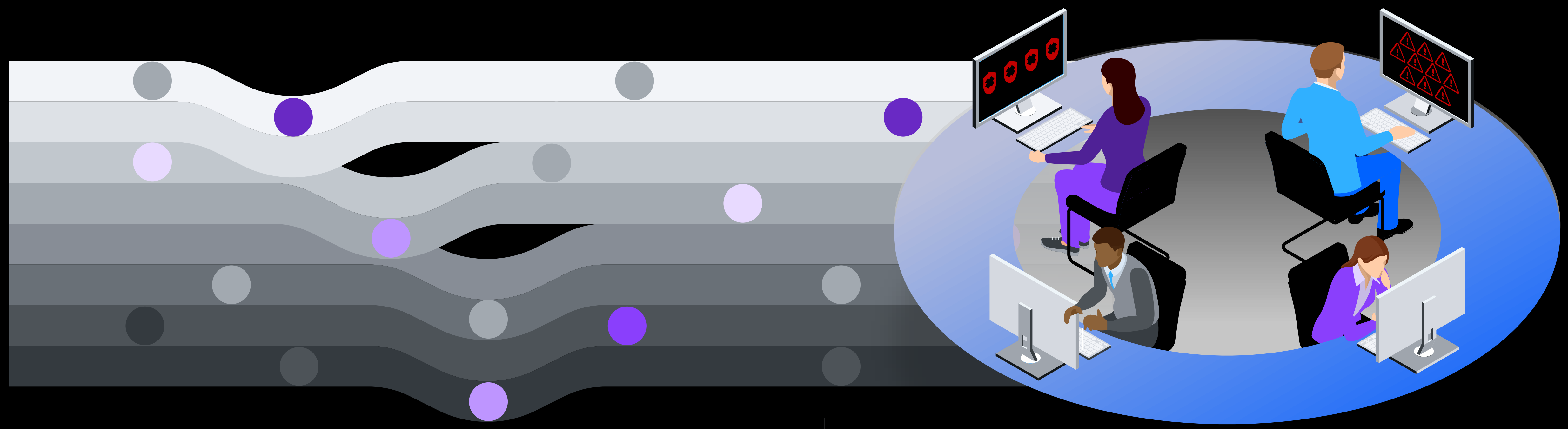
George Mavrovitis, Technical Sales, IBM

Iraklis Mathiopoulos, Chief of Service Delivery

OBRELA

Security operations needs major improvement

The move to cloud and IT modernization has expanded the attack surface, creating increased security complexity



Poor visibility
2 out of 3 organizations’ external attack surface has expanded in the last year[2]

Disconnected tools
80% of organizations use at least 10 disparate solutions to manage security hygiene[2]

Keeping up with attackers
29% of security operations processes are immature and need reengineering before they can be automated[1]

Information overload
52% of security environments have become more difficult to manage over the last two years[2]

51% of organizations struggle to detect and respond to advanced threats[1]

Transformation is needed

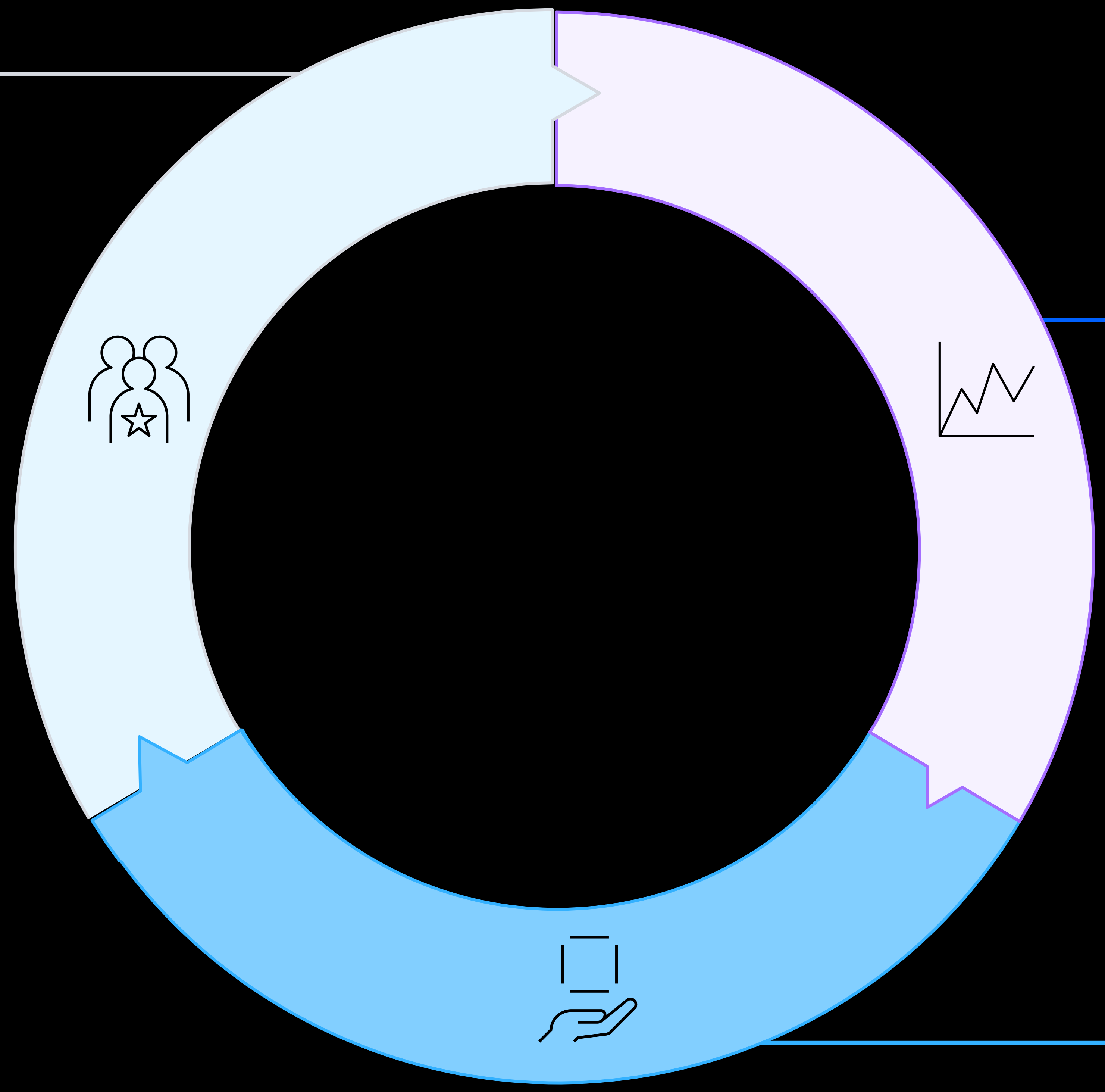
Current

Technology Focused

Dependent on specialized expertise

Proprietary Systems

Future



Analyst Focused

Connected workflows with common UX

Scale with enterprise automation and AI

Leverage AI to manage repetitive manual security tasks

Accelerate with Open

Interoperability with multi-vendor tools and clouds.

Our differentiation

Security that moves with your business

Greater Scale

1. Open Security Architecture

The world's largest cybersecurity ecosystem with 900+ out-of-the-box integrations and extensions[1], and a hybrid architecture built on Red Hat OpenShift

Greater Speed

2. Cybersecurity AI & Automation

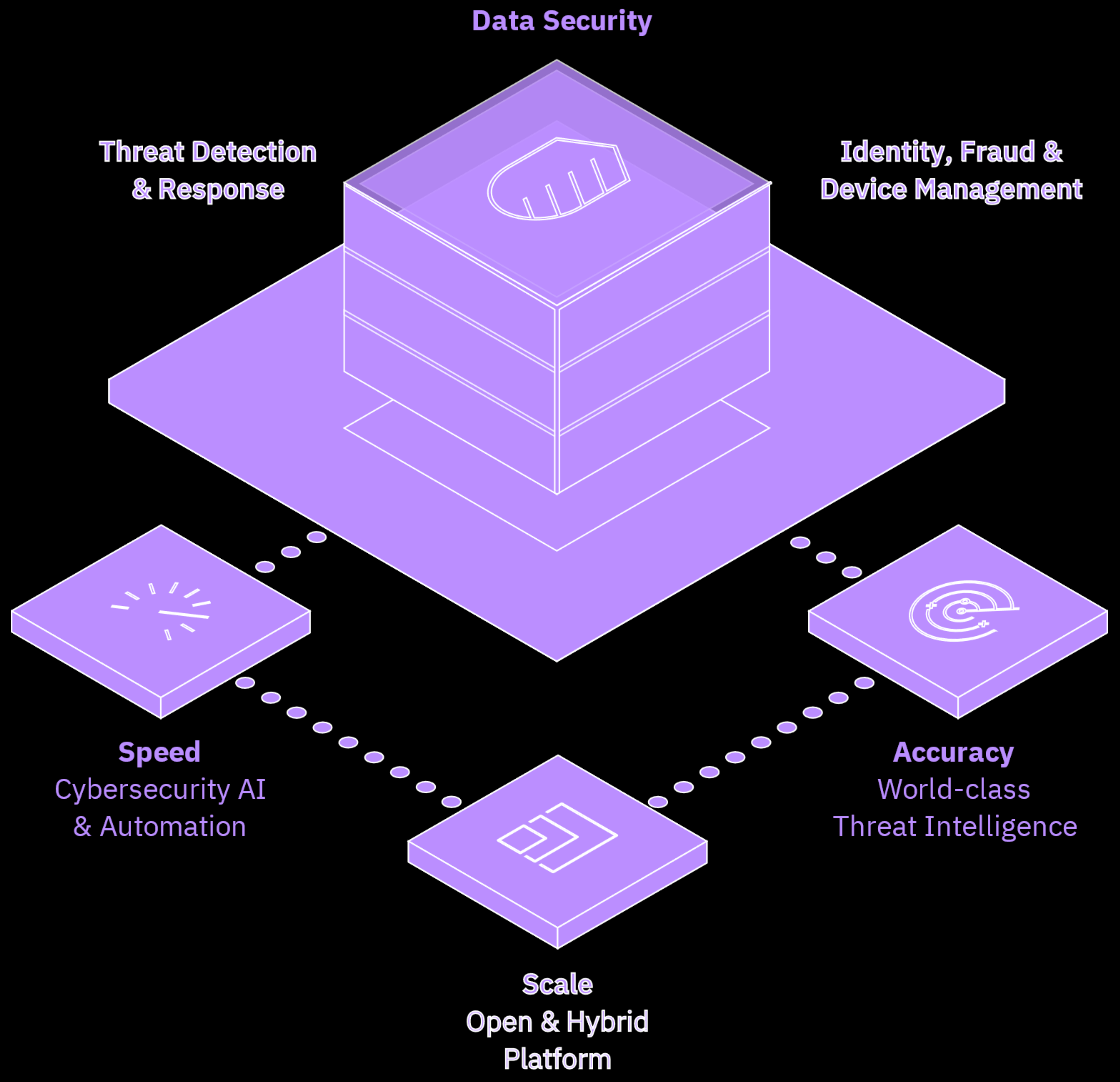
AI-powered actions, automations, and a common user experience that have been shown to speed investigations and triage by 55% in the first year[2]

Greater Accuracy

3. World-class Threat Intelligence

Unique insights on emerging threats and business risk using Randori's attacker's perspective and X-Force insights from monitoring 150B+ events/day

IBM **Security**


Data Security
Threat Detection & Response
Identity, Fraud & Device Management
Speed
Cybersecurity AI & Automation
Accuracy
World-class Threat Intelligence
Scale
Open & Hybrid Platform

Envisioning the future with Generative AI

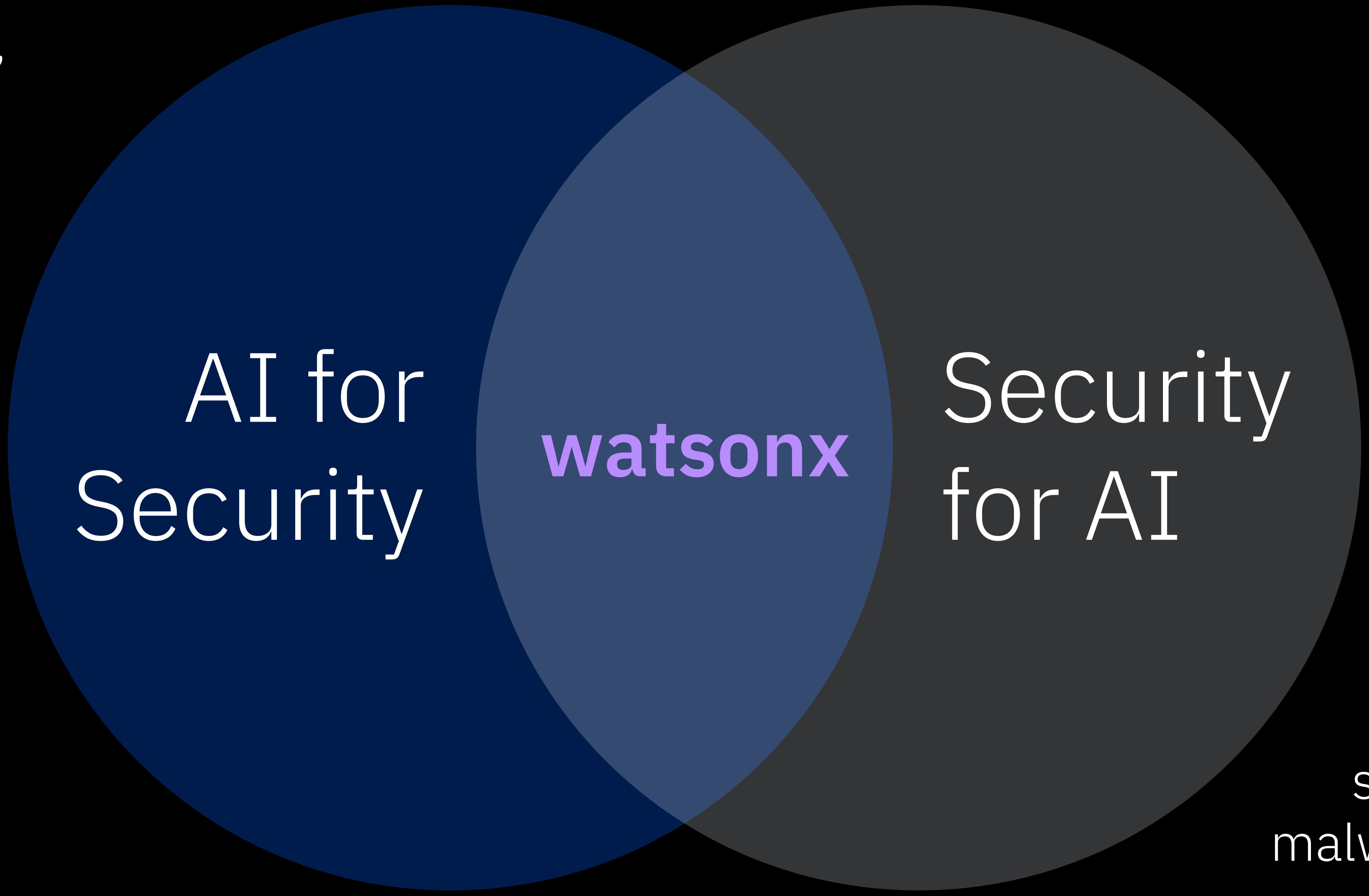
IBM’s cybersecurity and AI strategy

Productivity gains from foundation models and generative AI will reduce human bottlenecks in security

AI will manage repetitive security tasks such as summarizing alerts and log analysis, freeing teams to tackle strategic problems

AI will generate security content (detections, workflows, policies) faster than humans, expediting implementation and adjusting to changing security threats in real-time

AI will learn and create active responses that optimize over time, with abilities to find all similar incidents, update all affected systems, and patch all vulnerable code



Protecting foundation models, generative AI, and their data sets is essential for enterprise-ready AI

Secure the underlying AI training data by protecting it from sensitive data theft, manipulation, and compliance violations

Secure the usage of AI models by detecting data or prompt leakage, and alerting on evasion, poisoning, extraction, or inference attacks (IBM Adversarial Robustness Toolkit)

Secure against new AI generated attacks such as personalized phishing, AI-generated malware, and fake identities by using behavioral defenses and multi-factor authentication

Designed around the analyst experience

Enable better decisions quickly using a common set of Unified Analyst Experience (UAX) capabilities

Traditional Experience

8+ security UI’s

30+ hours of tool training

2+ days of response time

Manual investigation

Unified Analyst Experience

1 common UX

Continuous learning

< 30-minute response time[1]

Automated investigation

– What?

– When?

– Where?

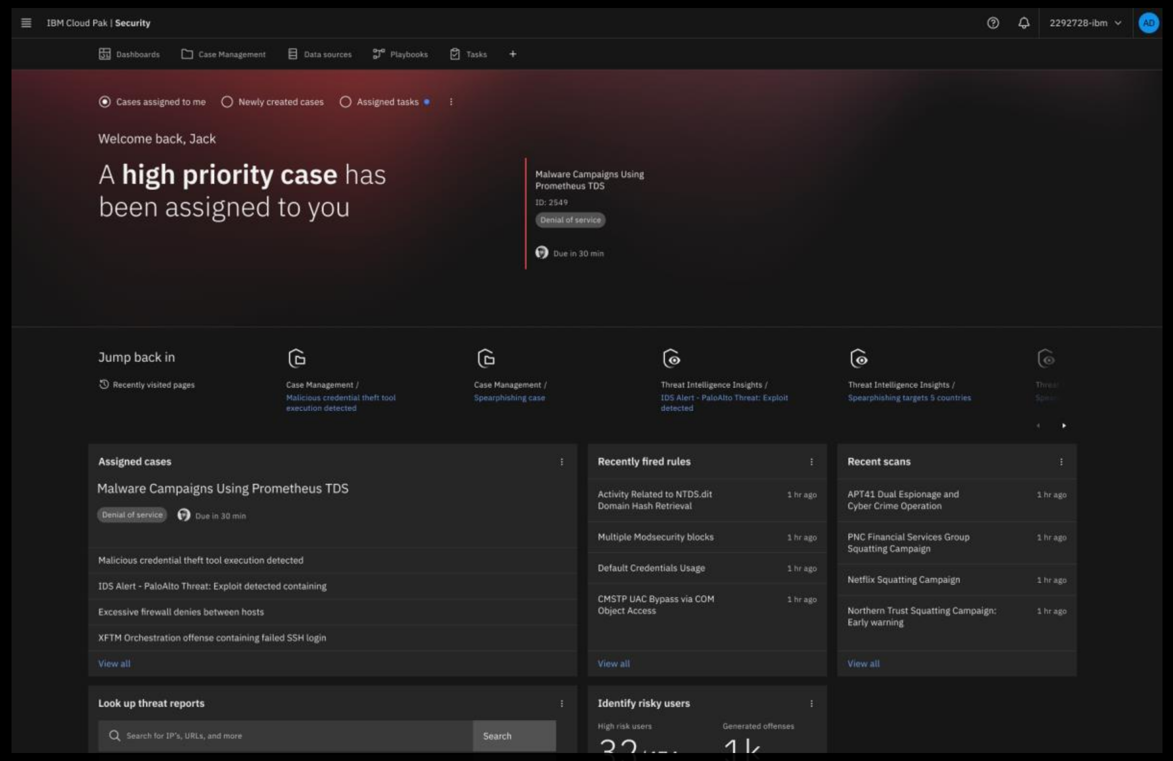
– Who?

– How?

Take action

90%+ analyst time saved on investigating an incident[2]

> “ I equate the UAX to five additional FTEs it was easier to get better data out of my tools with AI, than investing in more people It made my people faster and better at their job.”



Welcome back, Jack

A **high priority case** has been assigned to you

Malware Campaigns Using Prometheus TDS
ID: 2549
Denial of service
Due in 30 min

Jump back in
Recently visited pages
Case Management / Malicious credential theft tool execution detected
Case Management / Spearphishing case
Threat Intelligence Insights / IDS Alert - PaloAlto Threat: Exploit detected
Threat Intelligence Insights / Spearphishing targets 5 countries

Assigned cases
Malware Campaigns Using Prometheus TDS
Denial of service · Due in 30 min
Malicious credential theft tool execution detected
IDS Alert - PaloAlto Threat: Exploit detected containing
Excessive firewall denies between hosts
XFTM Orchestration offense containing failed SSH login
View all

Recently fired rules	
Activity Related to NTDS.dit Domain Hash Retrieval	1 hr ago
Multiple Modsecurity blocks	1 hr ago
Default Credentials Usage	1 hr ago
CMSTP UAC Bypass via COM Object Access	1 hr ago

View all

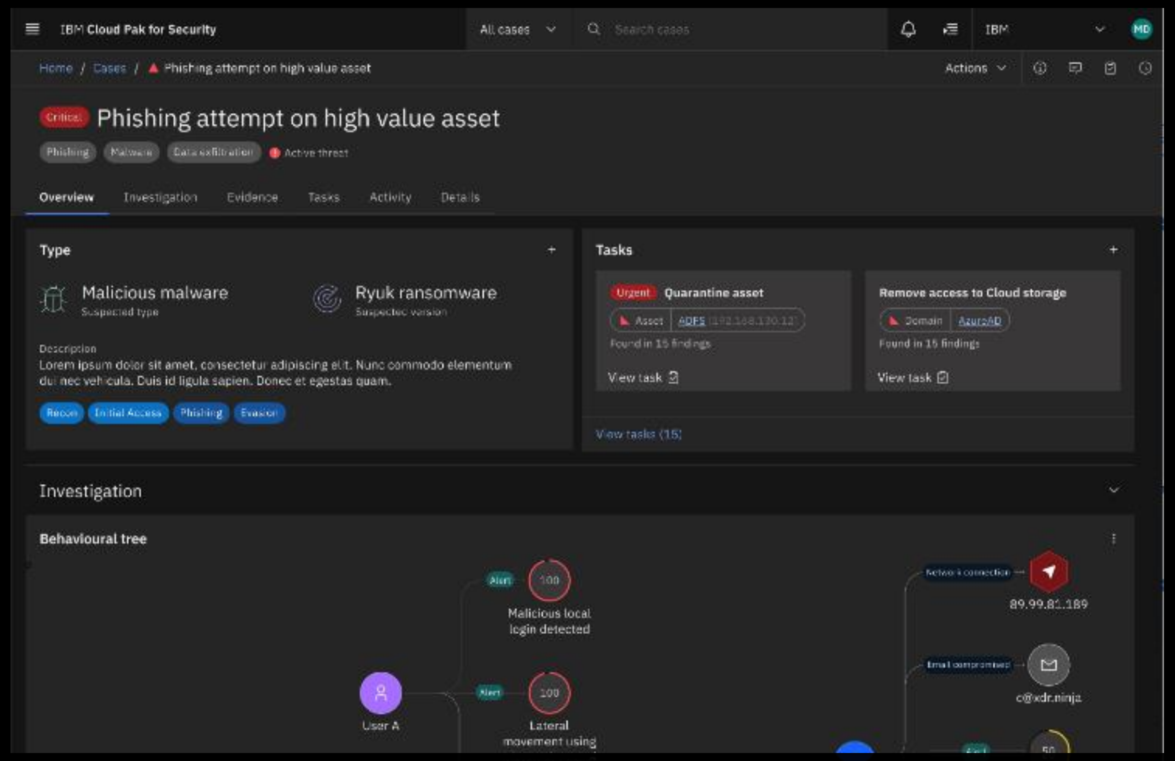
Recent scans	
APT41 Dual Espionage and Cyber Crime Operation	1 hr ago
PNC Financial Services Group Squatting Campaign	1 hr ago
Netflix Squatting Campaign	1 hr ago
Northern Trust Squatting Campaign: Early warning	1 hr ago

View all

Look up threat reports
Search for IP’s, URLs, and more
Search

Identify risky users
High risk users
Generated offenses

Enrich, correlate, and prioritize



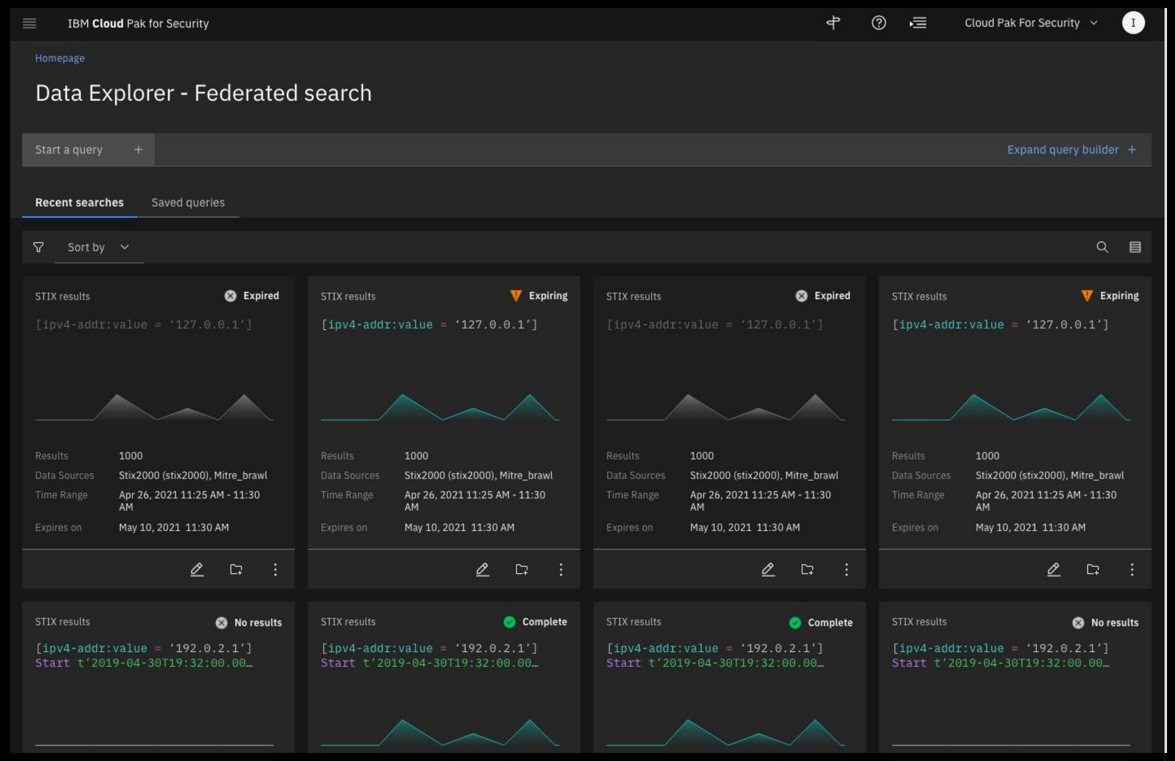
Critical Phishing attempt on high value asset
Phishing · Malware · Data exfiltration · Active threat

Type
Malicious malware — Suspected type
Ryuk ransomware — Suspected version
Description
Lorem ipsum dolor sit amet, consectetur adipiscing elit. Nunc commodo elementum dui nec vehicula. Duis id ligula sapien. Donec et egestas quam.
Recon · Initial Access · Phishing · Evasion

Tasks
Urgent Quarantine asset — Asset ADFS (192.168.130.12) — Found in 15 findings — View task
Remove access to Cloud storage — Domain AzureAD — Found in 15 findings — View task
View tasks (15)

Investigation
Behavioural tree

Automated investigation and response recommendations



Data Explorer - Federated search

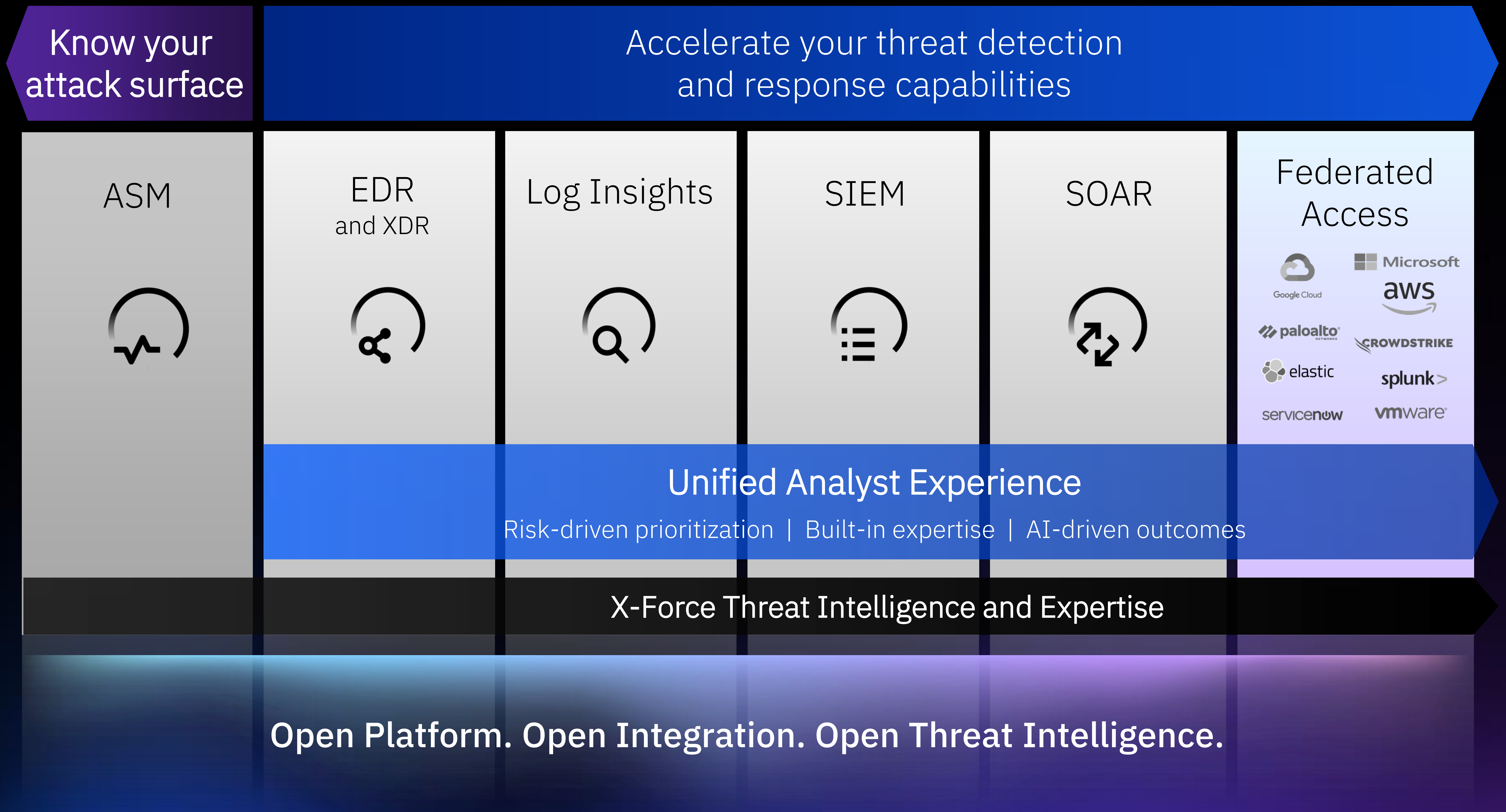
STIX results	STIX results	STIX results	STIX results
Expired	Expiring	Expired	Expiring
[ipv4-addr:value = ‘127.0.0.1’]	[ipv4-addr:value = ‘127.0.0.1’]	[ipv4-addr:value = ‘127.0.0.1’]	[ipv4-addr:value = ‘127.0.0.1’]
Results 1000	Results 1000	Results 1000	Results 1000
Data Sources Stix2000 (stix2000), Mitre_brawl	Data Sources Stix2000 (stix2000), Mitre_brawl	Data Sources Stix2000 (stix2000), Mitre_brawl	Data Sources Stix2000 (stix2000), Mitre_brawl
Time Range Apr 26, 2021 11:25 AM - 11:30 AM	Time Range Apr 26, 2021 11:25 AM - 11:30 AM	Time Range Apr 26, 2021 11:25 AM - 11:30 AM	Time Range Apr 26, 2021 11:25 AM - 11:30 AM
Expires on May 10, 2021 11:30 AM	Expires on May 10, 2021 11:30 AM	Expires on May 10, 2021 11:30 AM	Expires on May 10, 2021 11:30 AM

STIX results	STIX results	STIX results	STIX results
No results	Complete	Complete	No results
[ipv4-addr:value = ‘192.0.2.1’] Start t’2019-04-30T19:32:00.00…	[ipv4-addr:value = ‘192.0.2.1’] Start t’2019-04-30T19:32:00.00…	[ipv4-addr:value = ‘192.0.2.1’] Start t’2019-04-30T19:32:00.00…	[ipv4-addr:value = ‘192.0.2.1’] Start t’2019-04-30T19:32:00.00…

Federated search and threat hunting

Modernize security operations with greater speed and visibility

The evolution of the IBM Security QRadar Suite



Know your attack surface

Accelerate your threat detection and response capabilities

ASM

EDR and XDR

Log Insights

SIEM

SOAR

Federated Access

Unified Analyst Experience

Risk-driven prioritization | Built-in expertise | AI-driven outcomes

X-Force Threat Intelligence and Expertise

Open Platform. Open Integration. Open Threat Intelligence.

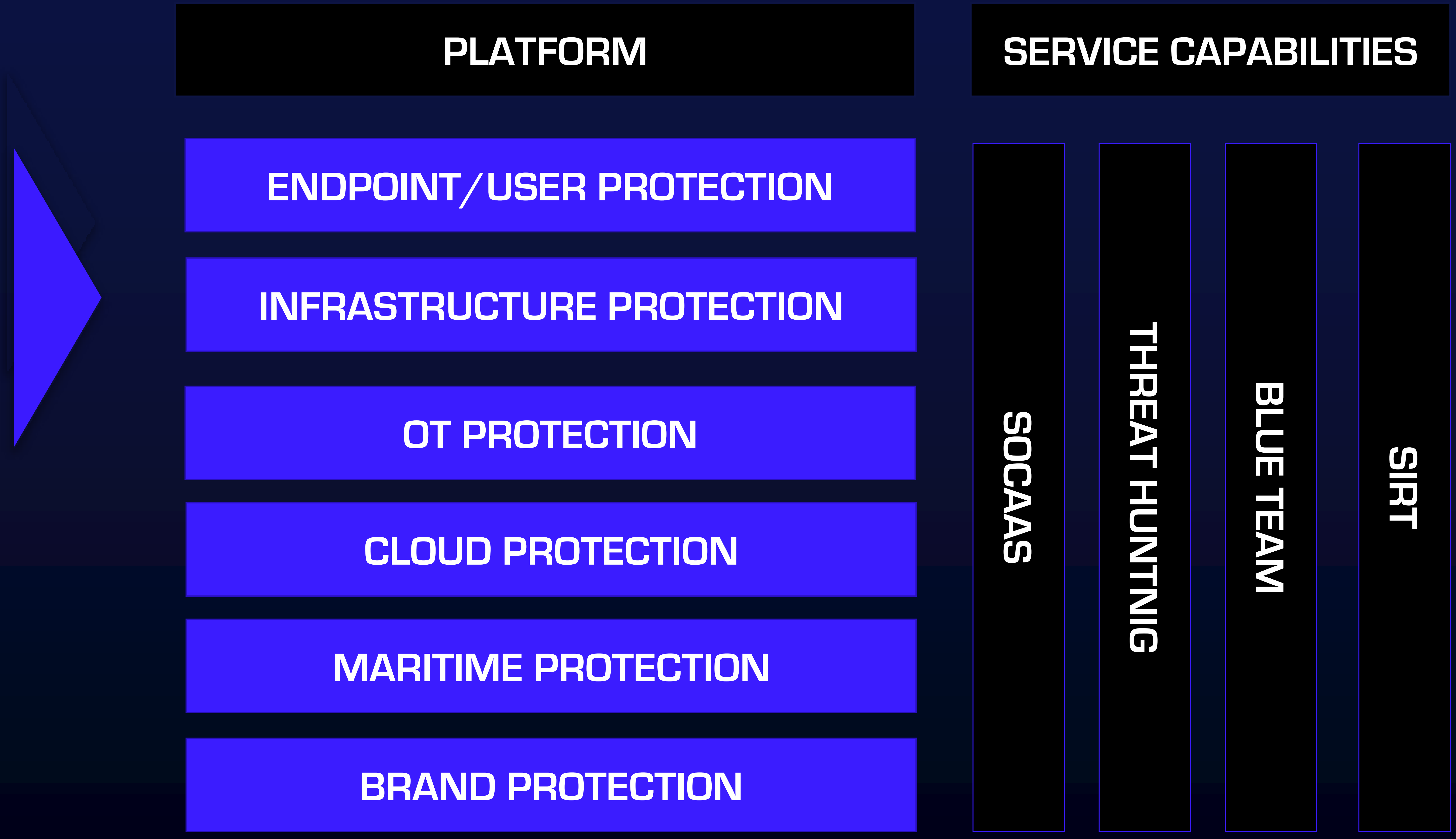
Designed around the analyst experience
Enable better decisions quickly using a common, streamlined, Unified Analyst Experience (UAX)

Gain accurate insights quickly
Streamline workflow with automation and AI designed for analysts, continuously updated threat X-Force threat detection and response expertise

Work with what you already have and expand to where you want to go
Built to meet you where you are using an open modular platform, standards, and ecosystem, with bi-directional integrations including federated search

MDR

MANAGED DETECTION AND RESPONSE



PLATFORM

- ENDPOINT/USER PROTECTION
- INFRASTRUCTURE PROTECTION
- OT PROTECTION
- CLOUD PROTECTION
- MARITIME PROTECTION
- BRAND PROTECTION

SERVICE CAPABILITIES

- SOCAAS
- THREAT HUNTNIG
- BLUE TEAM
- SIRT

SOCAAS

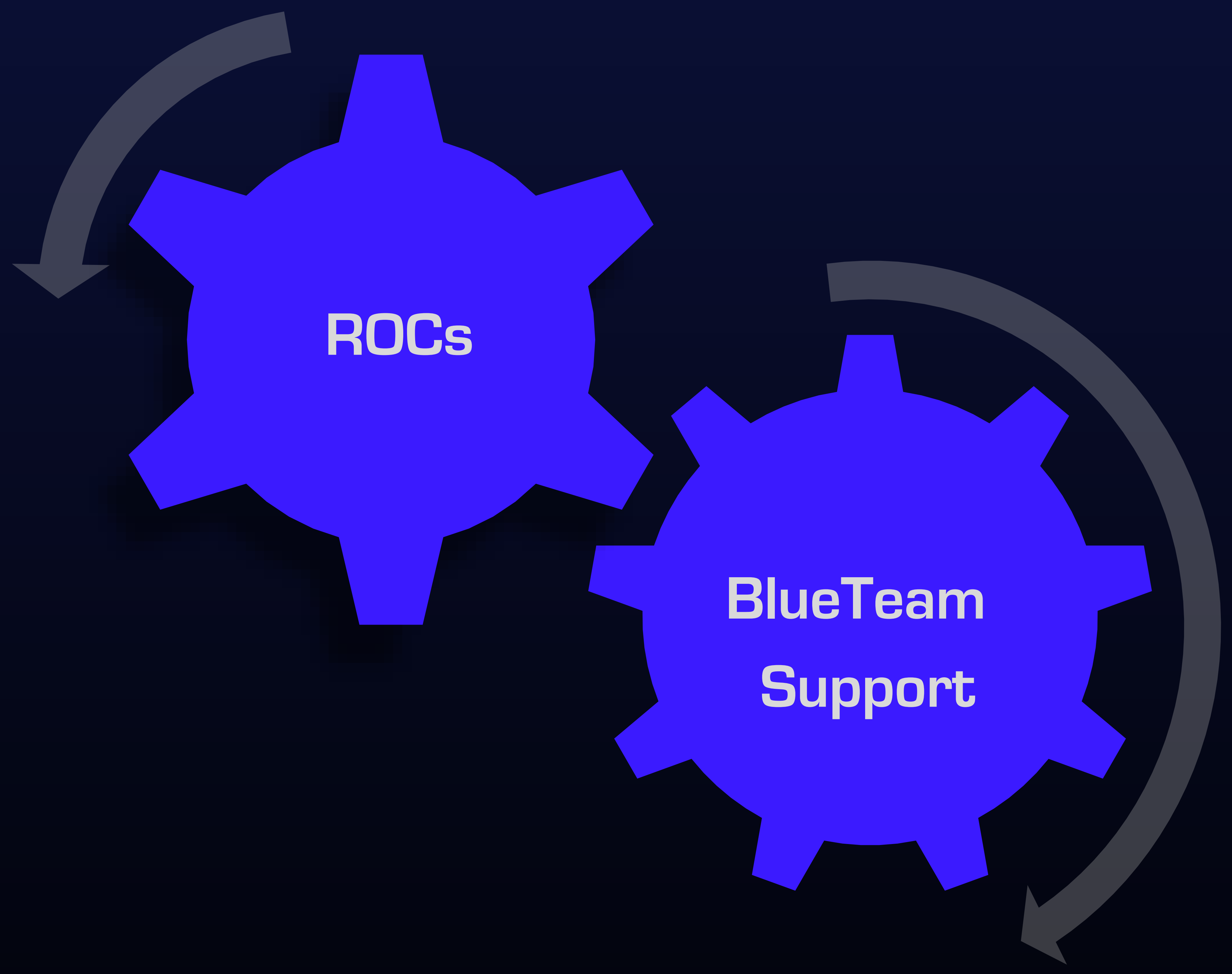
Obrela's SOC-as-a-Service (SOCaaS) delivers real-time situational awareness and protection against cyber threats:

- *Highly experienced security and threat analysts 24/7/365 monitoring*
- *Event management*
- *Reporting*

BLUE TEAM SUPPORT

Supports Global and Regional Resilience Operation Centers (ROCs) with the necessary assistance to ensure effective incident management, escalation, and mitigation:

- *Security Operations Support*
- *Security Posture Assessment*
- *Vulnerability Scanning*
- *Vulnerability Management*
- *Advanced Content Development*
- *Training*



THREAT HUNTING

Combines knowledge, intuition and automation for proactive search of any compromise leveraging advanced analytics and threat intelligence to investigate.

OBRELA's Threat Hunting team actively performs Threat Hunts to identify threat actors and gaps in the organization.

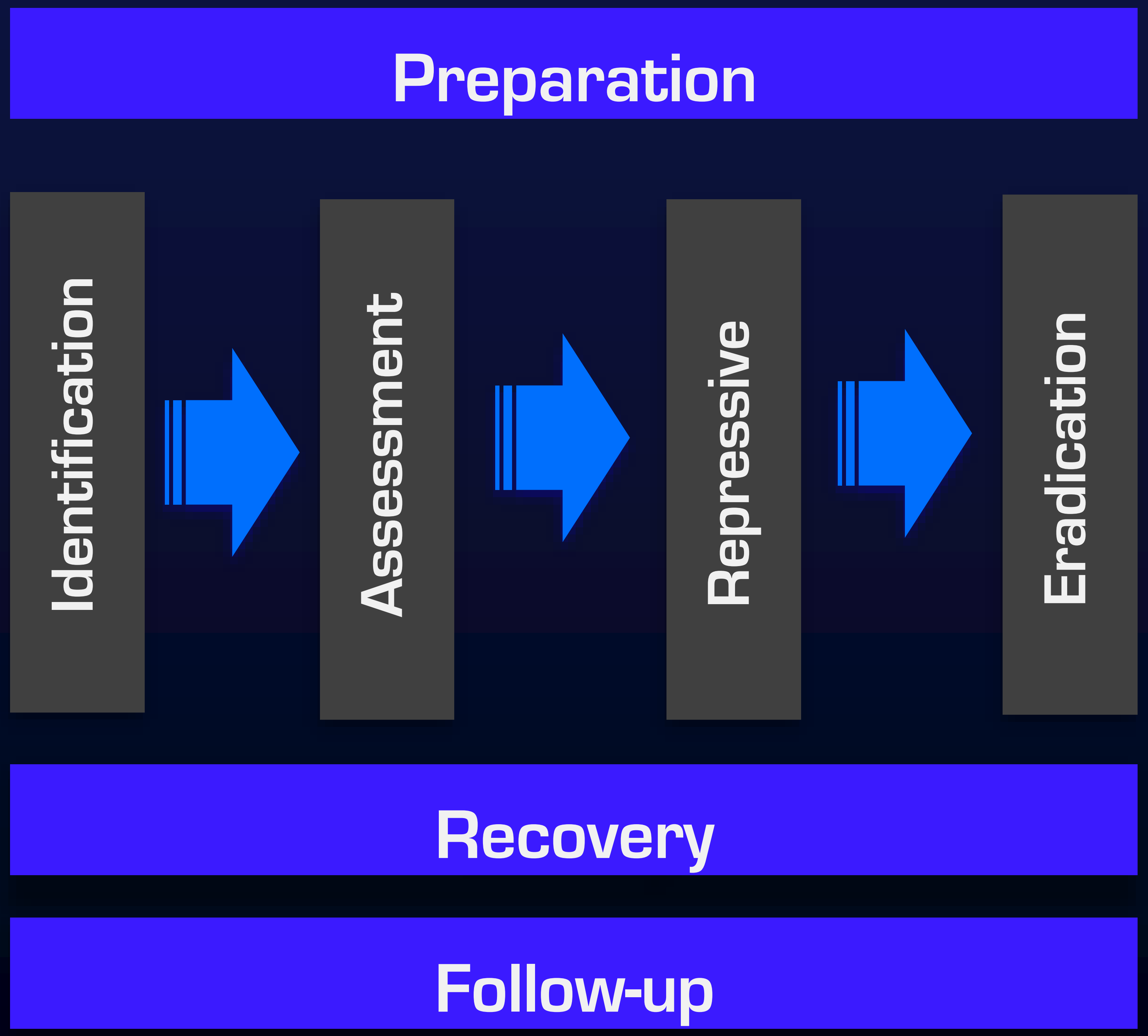
OBRELA's Threat Hunting framework focuses on proactive hypothesis-driven threat profiling and covers:

- *Systematic Based. Following a hypothetical approach, threat hunting cycles to systemically uncover and identify malicious activity or emerging IOCs that are in progress.*
- *Mission Based. Following a reactive approach, threat hunting is actively engaged to "lock" attack behavior and malicious activity that has been reported from threat intelligence or the security operations.*

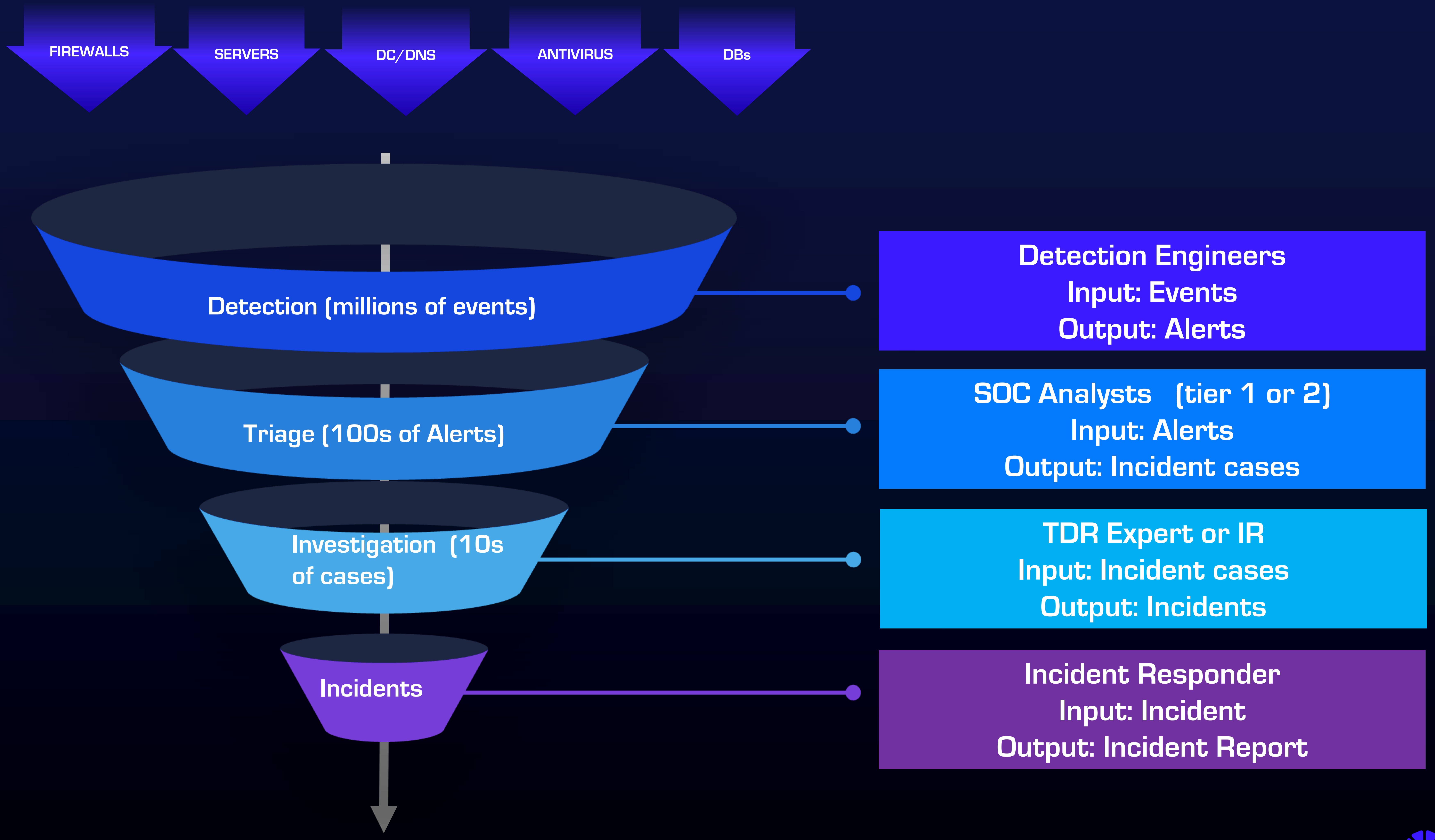
SIRT - INCIDENT RESPONSE

The security incident response team (SIRT) enables the client to perform mitigation/containment of security incidents:

- *Remote Security Incident Support until Closure*
- *Handling Remote Investigation Services Requests*
- *Remote Endpoint Investigation and Malware Analysis*
- *Active Responses/ Playbooks*
- *Domain Takedown*



REAL-TIME THREAT MANAGEMENT



Detection Engineers
Input: Events
Output: Alerts

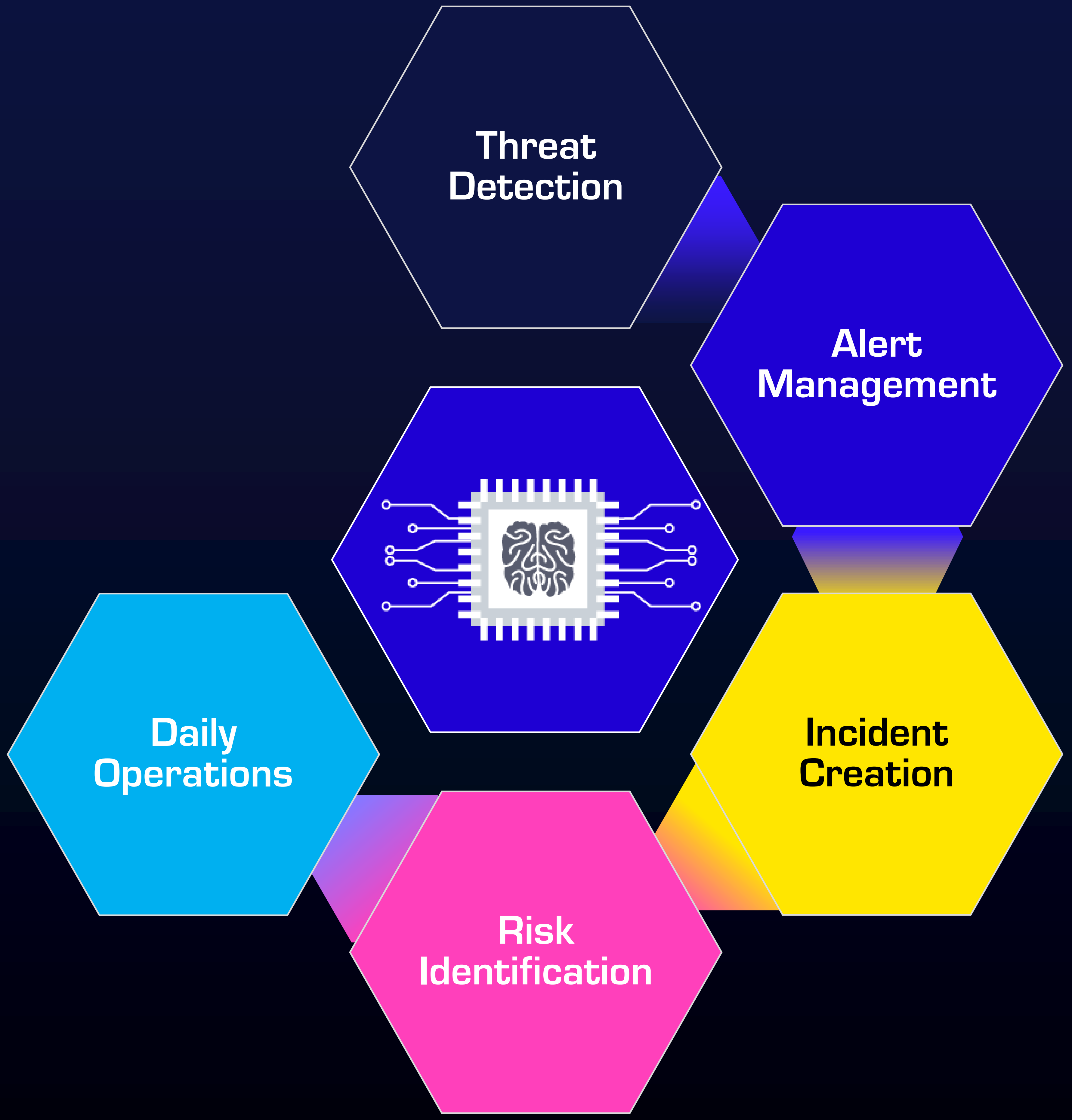
SOC Analysts (tier 1 or 2)
Input: Alerts
Output: Incident cases

TDR Expert or IR
Input: Incident cases
Output: Incidents

Incident Responder
Input: Incident
Output: Incident Report

12 March 2024

AI, LLM & ML CAPABILITIES



- To detect threats that are otherwise undetectable by heuristic approaches
  - By EDRs. UEBA, NDRs, OT, IBM WatsonX
- To reduce alert noise and prioritize alerts on Security Operations Centers
- To speed up investigations and incident creation
- To engage with capabilities offered by Swordfish MRC Risk Analytics
  - Identify materialized business risks
  - What-if scenarios
  - Prioritize threats based on the business impact
- To assist employees securely work using modern toolkits

THE USE OF QRADAR IN THREAT MANAGEMENT

- *Incident Detection and Prioritization*
  - *Our SOC teams focus their efforts on the most critical threats (SLA compliance).*
- *Incident Investigation*
  - *Reduces the time to search through historical data, reconstruct events, and identify the root cause of security breaches*
- *Threat Hunting*
  - *Employs advanced analytics techniques (ML/AI), allows creation of targeted rules and queries in short time.*
- *Use Case Management*
  - *Utilizes content for OBRELA's owned use case library and provides tools for fine tuning. Additionally, it maps the Use Cases to the MITRE Framework*
- *Integration with OBRELA's MDR Technology Stack*
  - *Empower Alert, Incident Management, and SOAR-to-SOAR integration capabilities*

WHY OBRELA

Obrela combines business-focused risk management with threat detection to deliver real-time cyber defense that's ready for everything that comes next.

RISK OVER THREATS

We help identify risks posed by threats, then translate risks into business terms, so customers better understand what's at stake. The biggest threat is not knowing the risk!

PREDICTABILITY OVER UNCERTAINTY

With a centralized view that spans your business and its risks, we prioritize the most important issues in real-time, so you make focused decisions and work with predictability in the face of uncertainty.

VISIBILITY OVER YOUR DIGITAL UNIVERSE

We deliver risk aware operational security consolidating all security data and turning them into actionable intelligence, meaning threats can't hide just because your business grows.

OUR MISSION

WE KEEP YOUR BUSINESS IN BUSINESS

OBRELA

THANK YOU

London | Athens | Dubai | Frankfurt | Riyadh

www.obrela.com