

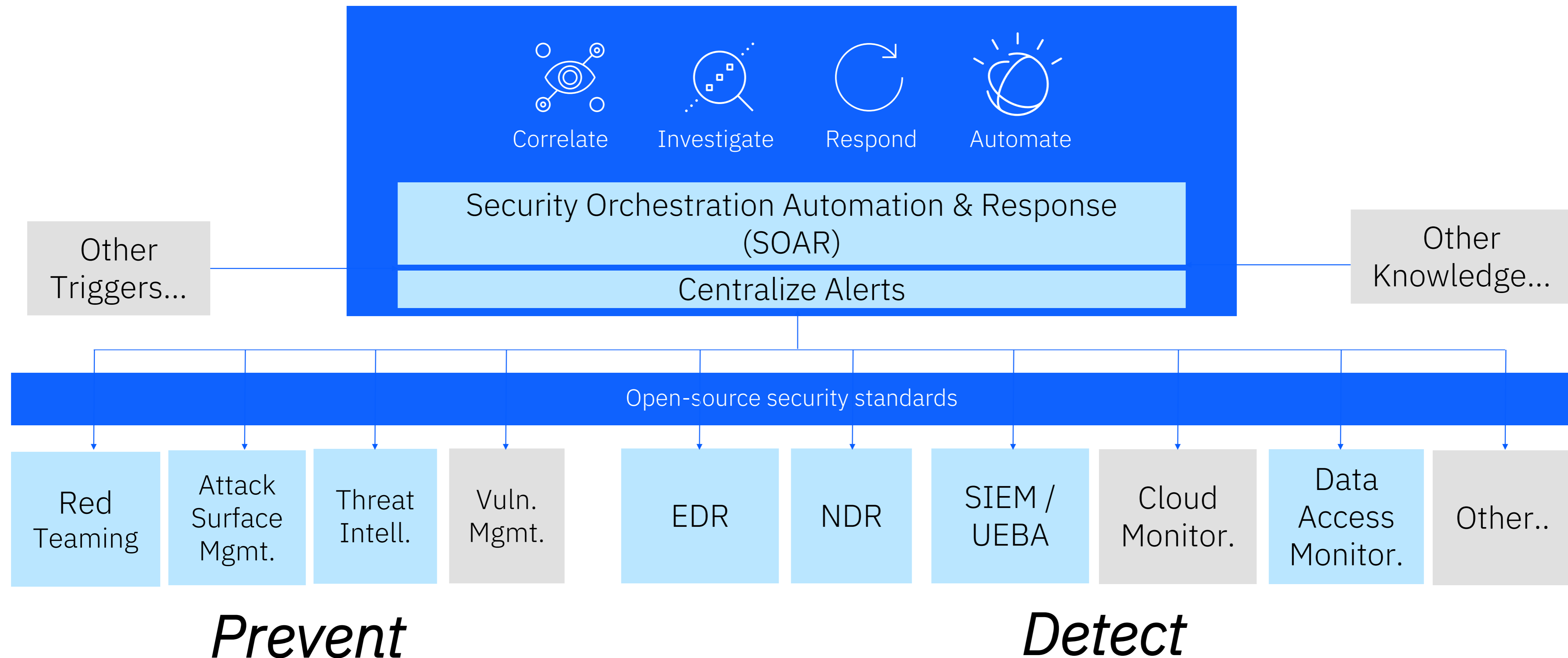
Giulia Caliarì

Security Architect

IBM Technology, IBM ITALIA

Framework for Threat Detection and Incident Response

Analyze and Respond



1 – Leverage Automation, AI and ML to provide immediate understanding of what's going on

- Collect and prioritize alerts

The screenshot displays a 'Risk Scoring Alert' dashboard. At the top, it says 'Top Open Alerts for Today' and 'Risk Score All Open Alerts'. Below this is a search bar. The main area contains eight alert cards arranged in two rows of four. Each card provides the following information: Alert Id, Vendor, Event Name, Risk Score, and Priority. The alert with Alert Id 104070265 is circled in red, highlighting its Risk Score of 0.37 and Medium priority.

Alert Id	Vendor	Event Name	Risk Score	Priority
98321585	CARBONBLACK	"Process mshta.exe was...	0.07	Low
95826705	CROWDSTRIKE	Indicator of Attack	0.1	Low
99529574	QRADAR	CIO_SA: CrowdStrike De...	0.07	Low
99749195	QRADAR	CIO_SA: CrowdStrike De...	0.29	Low
104070265	QRADAR	Unknown Detection Su...	0.37	Medium
107194239	QRADAR	SEV3_IBM_TechnicalAtt...	0.54	Medium
105419673	QRADAR	SEV2_IBM_TechnicalAtt...	0.24	Low
91826802	CARBONBLACK	driverupdate.exe on the ...	0.31	Low

1 – Leverage Automation, AI and ML to provide immediate understanding of what's going on

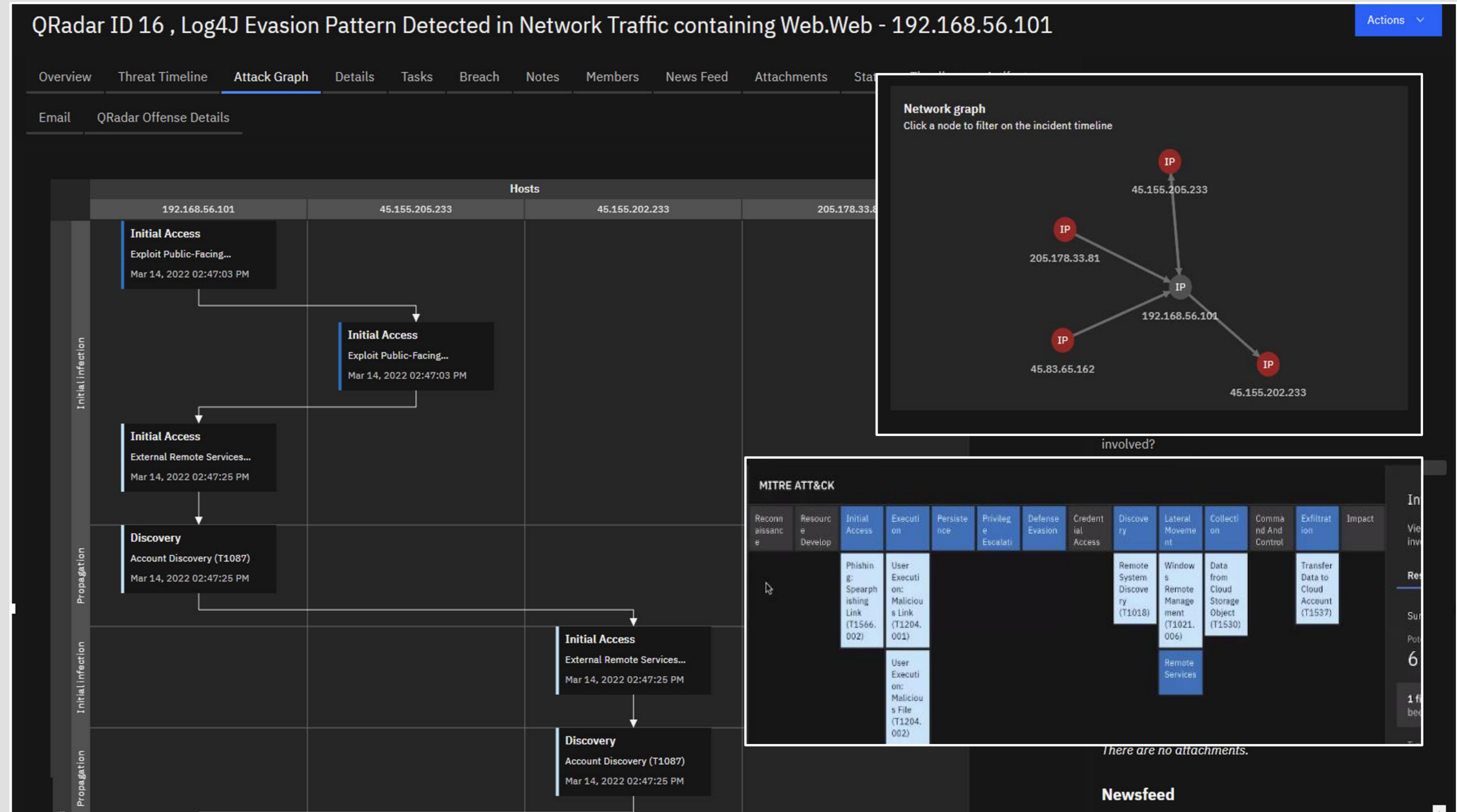
- Collect and prioritize alerts
- Aggregate alerts from multiple sources
- Enrich with telemetry, asset information and Threat Intelligence

The screenshot displays the QRadar interface for a specific case. The title bar reads "QRadar ID 16, Log4J Evasion Pattern Detected in Network Traffic containing Web.Web - 192.168.56.101". The interface is divided into several sections:

- Case details:** Description: "1 events in 2 categories: Log4J Evasion Pattern Detected in Network Traffic containing Web.Web". Owner: Tier 1 Analysts. Last modified: 14 March 2022 16:30:08. Date created: 14 March 2022 15:08:23. Severity: -. Phase: Engage.
- Threat timeline:** Artifacts investigated: 2, MITRE tactics: 4, Findings: 7, Assets involved: 5.
- MITRE ATT&CK Tactics:** Discovery, Execution, Exfiltration, Initial Access (highlighted).
- Artifacts:** IP 192.168.56.101 (2 hits), IP 45.155.205.233 (1 hit).
- Related cases:** Active cases: 3, Matching artifacts: 3. Matches include: "QRadar ID 18, UBA: Potentially Compromised Endpoint containing CMD Spawned on Host - fadams", "Log4j Zero-Day Vulnerability", and "QRadar ID 17, Potential Log4Shell Evasion detected preceded by Potential Log4Shell Base Pattern detected containing HTT...".
- Playbook status:** 1 Playbook (Running).
- Tasks list:** Complete: 1/3, Unassigned: 1. Tasks include "Initial Triage" and "Investigate Network Threats".

1 – Leverage Automation, AI and ML to provide immediate understanding of what's going on

- Collect and prioritize alerts
- Aggregate alerts from multiple sources
- Enrich with telemetry, asset information and Threat Intelligence
- Build threat timeline and graphs
- Map on MITRE Framework



1 – Leverage Automation, AI and ML to provide immediate understanding of what's going on

Zero Effort

- Collect and prioritize alerts
- Aggregate alerts from multiple sources
- Enrich with telemetry, asset information and Threat Intelligence
- Build threat timeline and graphs
- Map on MITRE Framework
- Suggest tactical recommendations

Recommendations
Click Add to case to create a task in the case. Click Dismiss to mark response as dismissed.

▲ **Add file hashes to your deny list**

Add the following file hashes to your deny list: MD5 7e37ab34ecdcc3e77e24522ddfd48... SHA-256 02ef73bd2458627ed7b397ec26ee2...

Reason: A threat intelligence report indicates file ransom.exe is malicious and was found on Domain user-workstation.example.com

The host has an associated finding.

[Add to case](#)
[Dismiss](#)
[Open details](#)

▲ **Block URL**

Block the following URL: URL https://findoutcredit.com

Reason: A threat intelligence report indicates that this URL is malicious and was accessed by an internal host IP user-workstation.example.com

The host has an associated finding.

[Add to case](#)
[Dismiss](#)
[Open details](#)

2 – Orchestrate tech & business activities to resolve incident

- Dynamic workflows guide technical and **business users**
- Provide clear instructions and deadlines
- Enable team collaboration
- Support further analysis, threat hunting and collection of forensic data
- Introduce **automation** whenever possible

The screenshot displays the IBM Security console interface. At the top, it shows the breadcrumb 'Homepage / Cases / Prestige Ransomware Targeting Transportation Industry' and a progress indicator '12% Complete'. Below this, there are filters for 'Owner: 0 selected', 'Status: Active', and 'Selected'. A table lists tasks under three phases: 'Initial', 'Engage', and 'Detect/Analyze'. The 'Detect/Analyze' phase is expanded, showing a task 'Analyze malware-infected systems' with detailed instructions. To the right, a 'Summary' panel provides metadata for the incident, including ID (2311), Phase (Engage), Severity (Low), and Incident Type (Malware/Ransomware). Other panels show 'People' (Created By: cp4sadmin, Owner: cp4sadmin, Members: manager), 'Related Incidents' (No related cases), and 'Attachments' (There are no attachments).

The screenshot shows a workflow diagram for a phishing attack. The main workflow starts with a task 'Microsoft online exchange: set member...' (#1). This task branches into three parallel tasks: 'Attach emi file' (#2), 'Notify public relations department' (#3), and 'Gather URL threat intel' (#4). Task #2 leads to 'Provide end-user remediation guidance...' (#6) and 'Look for modifications made to system softw...' (#7). Task #4 leads to 'if denise is a member, set address' (#5), which then branches into 'Microsoft online exchange: set member...' (#8) and 'Carbon Blac' (#9). A 'Playbook details' panel on the right provides information about the playbook, including its name 'Phishing attack is very bad', description, status 'Draft', and activation summary 'Reusable'. The panel also lists inputs like 'Recipient email address', 'Sender email address', and 'Subject body', and has a 'Publish playbook' button.

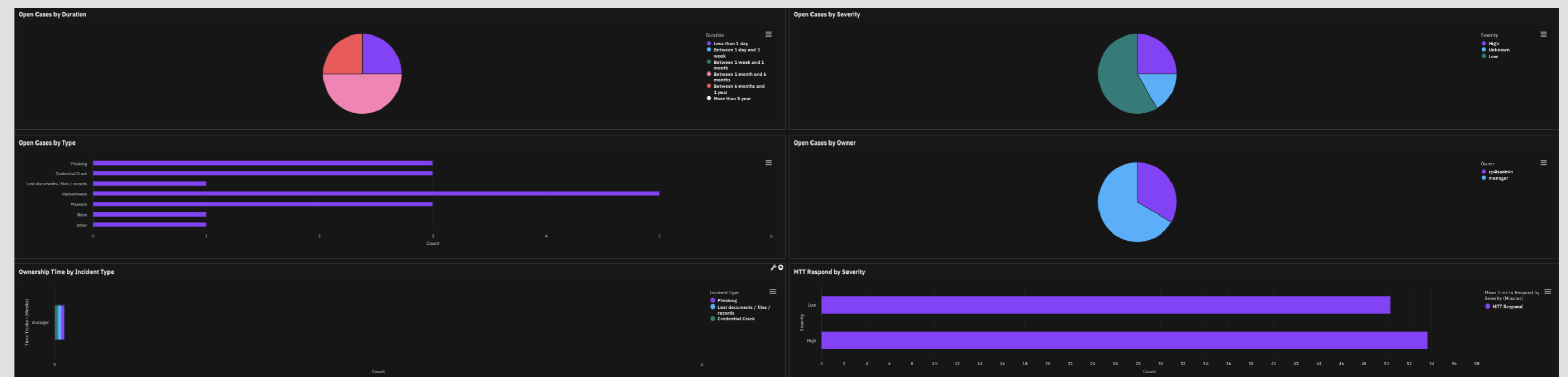
- Trace everything and collect evidences
- Monitor progression of incident resolution
- **Simulation scenarios** to test effectiveness of procedures and preparation of personnel
- **Long-term improvement** of security policies and posture

3 – Inject activities dictated by regulations (ie: data privacy)

- Meet short reporting timeframes for incident/ breach notification
 - Instructions, impact/risk assessment, reporting templates, deadlines, ...
- Cover requirements from multiple regulations at the same time
- Single hub for all breach/incident information as well as a single auditable system of record
- Support other requirements, like GDPR DSAR process
- Measure efficiency of response processes

The screenshot shows a 'Tasks' view for a case titled 'Credential Crack and access to Customer DB'. The interface includes a navigation bar with tabs like Overview, Details, Tasks, Artifacts, Notes, MITRE ATT&CK Details, Tables, Breach, Members, News Feed, Attachments, Stats, Timeline, and Email. A progress bar at the top indicates '0% Complete'. A table lists tasks with columns for Task Name, Instructions, Due Date, Flags, and Actions. The tasks are categorized under 'Respond - (Data Breach - General)', 'Respond - (Data Breach - Authority Notification)', and 'Respond - (Data Breach - Individual Notifications)'. A detailed view of a task shows instructions for GDPR compliance, including a list of required documentation items. On the right, a summary panel provides details such as ID (2594), Phase (Respond), Severity (Low), and Incident Type (Credential Crack).

Task Name	Instructions	Due Date	Flags	Actions
Respond - (Data Breach - General)	GDPR The GDPR requires, that you keep documentation of all breaches, regardless of whether or not the breach needs to be notified to the supervisory authority. If a breach is not notified or if notification was delayed, a justification for your reasoning and decisions, should be documented. Your supervisory authority may request these records as evidence of compliance as part of enforcing GDPR's accountability principle.	05/24/2023 16:53		
Respond - (Data Breach - Authority Notification)	Documentation must include: <ul style="list-style-type: none">• Causes of the breach;• What took place;• Personal data affected;• Effects and consequences of the breach;• Remedial actions taken by controller;• Reasoning for the decision taken (e.g. why	05/12/2023 16:53		
Respond - (Data Breach - Individual Notifications)		05/12/2023 16:53		



Thank you

© 2023 International Business Machines Corporation
IBM and the IBM logo are trademarks of IBM Corporation, registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on [ibm.com/trademark](https://www.ibm.com/trademark). This document is current as of the initial date of publication and may be changed by IBM at any time. Statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only. THIS DOCUMENT IS DISTRIBUTED "AS IS" WITHOUT ANY WARRANTY, EITHER EXPRESS OR IMPLIED. IN NO EVENT, SHALL IBM BE LIABLE FOR ANY DAMAGE ARISING FROM THE USE OF THIS INFORMATION, INCLUDING BUT NOT LIMITED TO, LOSS OF DATA, BUSINESS INTERRUPTION, LOSS OF PROFIT OR LOSS OF OPPORTUNITY. Client examples are presented as illustrations of how those clients have used IBM products and the results they may have achieved. Actual performance, cost, savings or other results in other operating environments may vary. Not all offerings are available in every country in which IBM operates. It is the user's responsibility to evaluate and verify the operation of any other products or programs with IBM products and programs. The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

