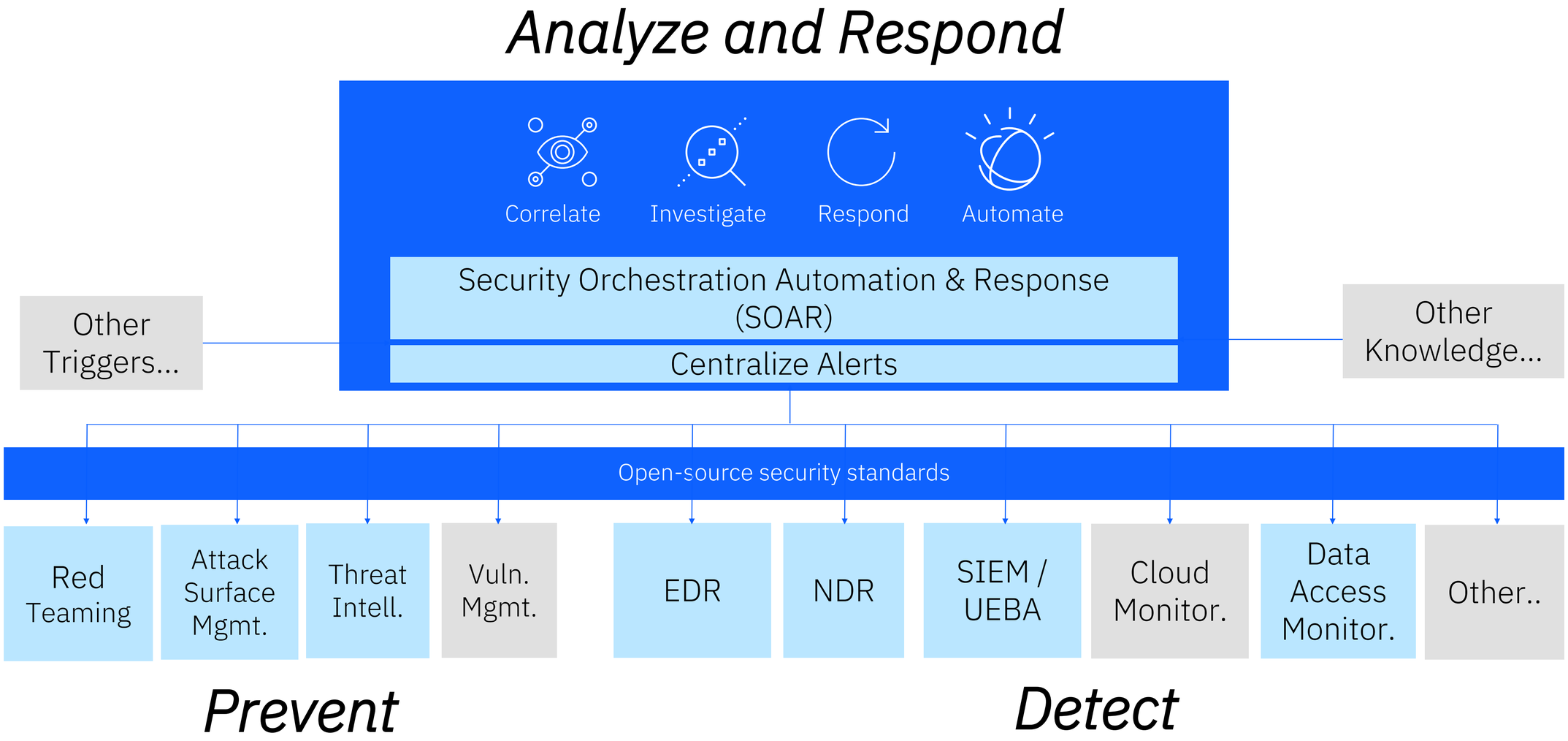
Giulia Caliari

Security Architect
IBM Technology, IBM ITALIA

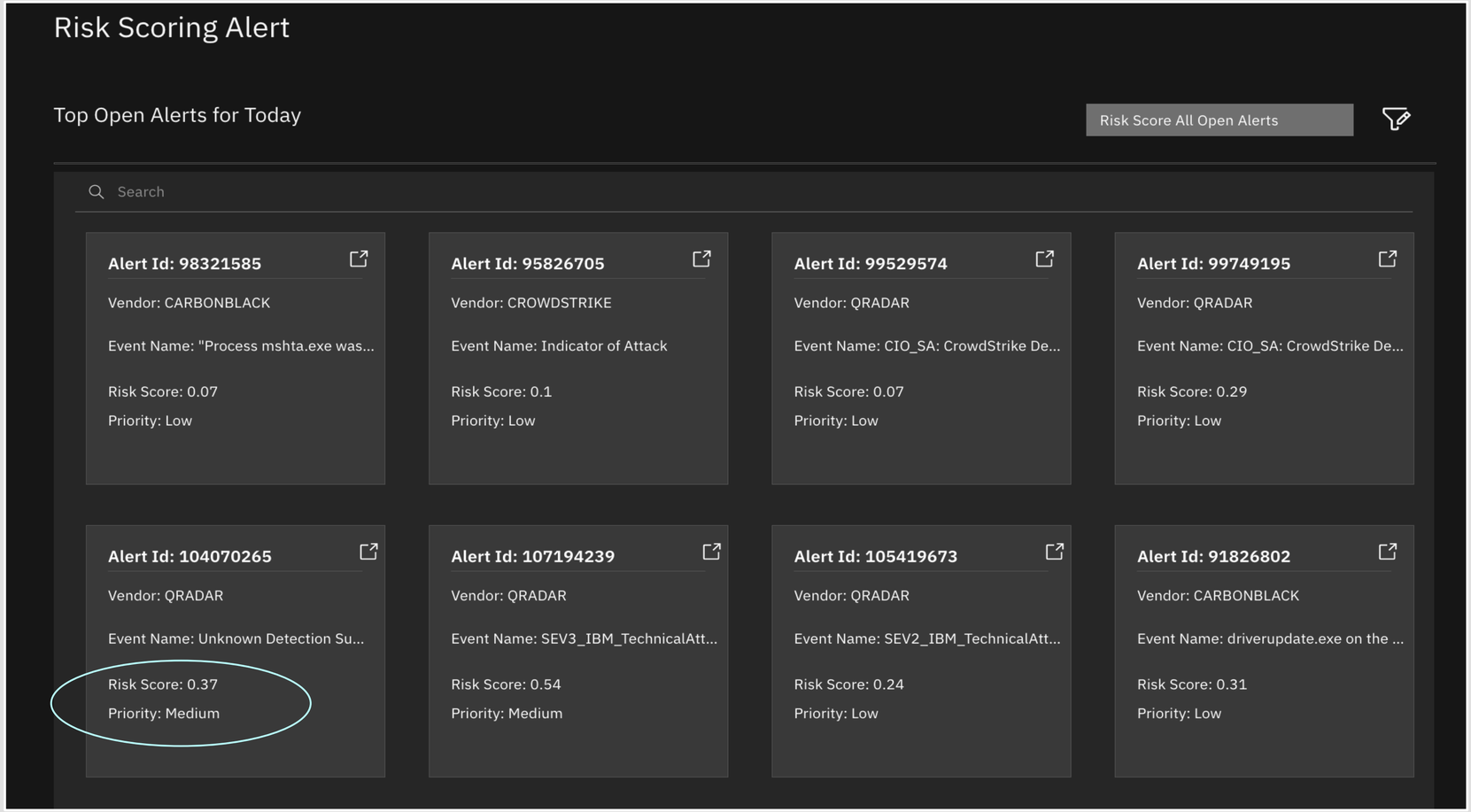
IBM **Security**

Framework for Threat Detection and Incident Response



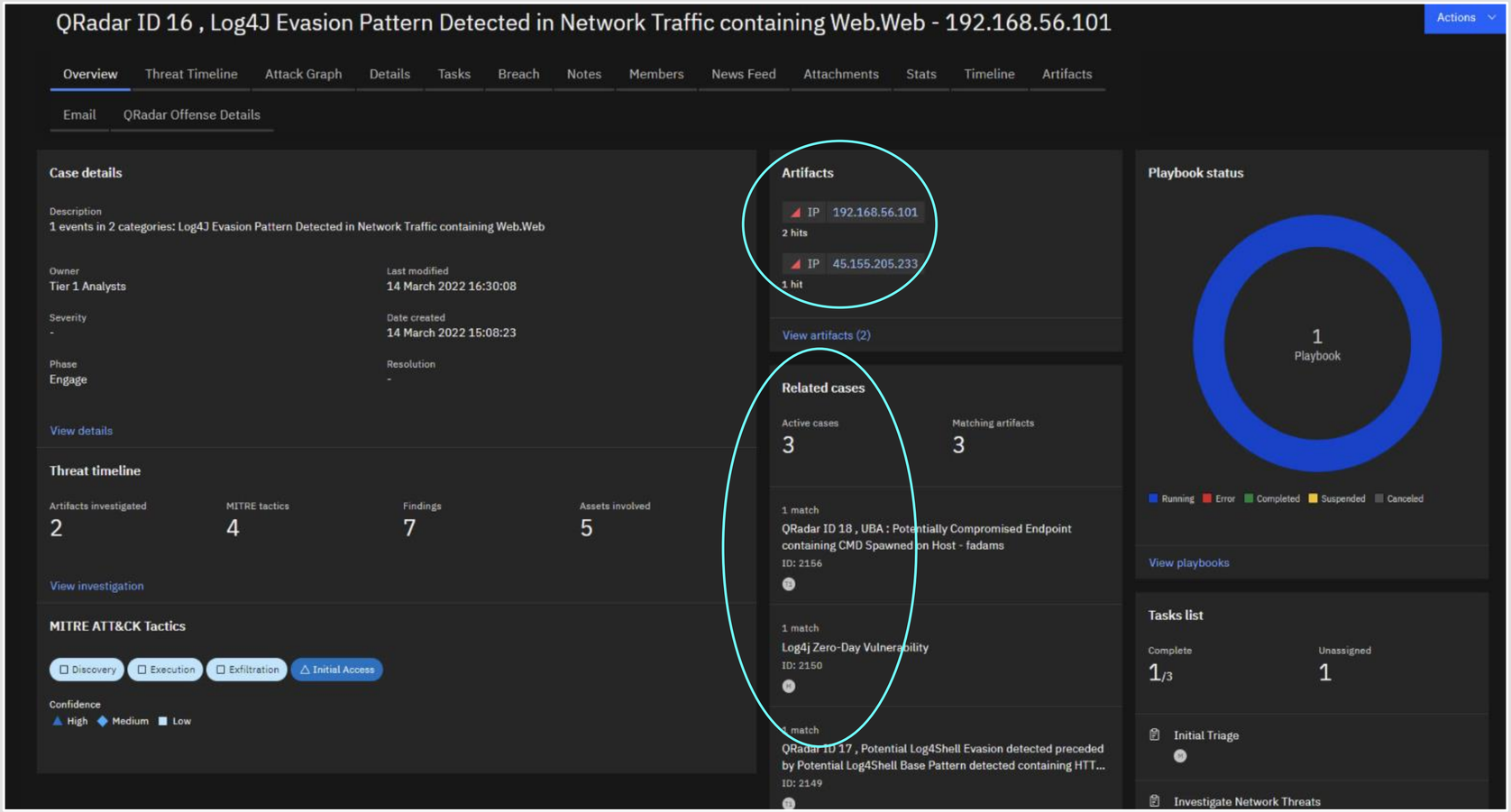
1 – Leverage Automation, AI and ML to provide immediate understanding of what's going on

- Collect and prioritize alerts



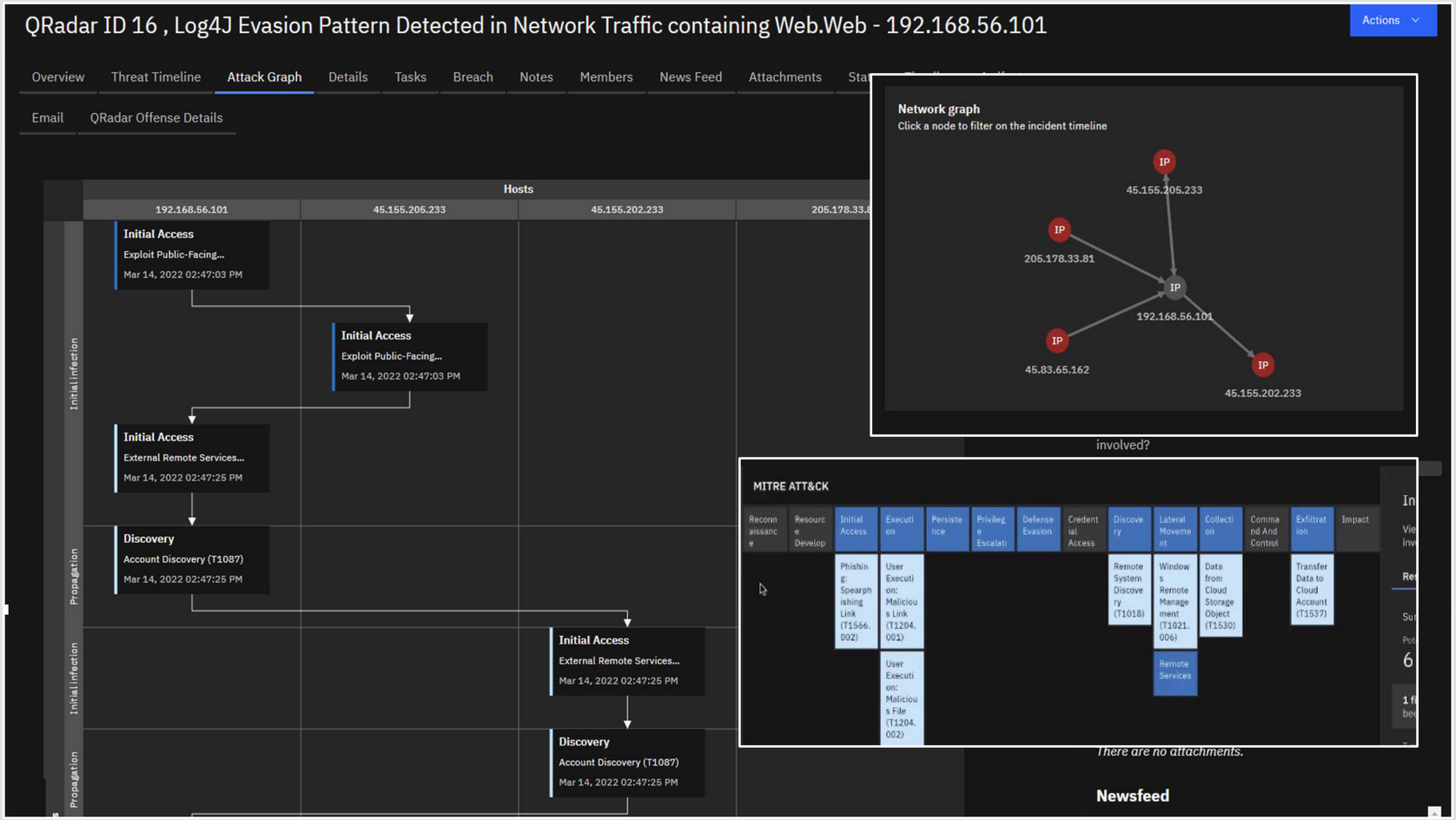
1 – Leverage Automation, AI and ML to provide immediate understanding of what's going on

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



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

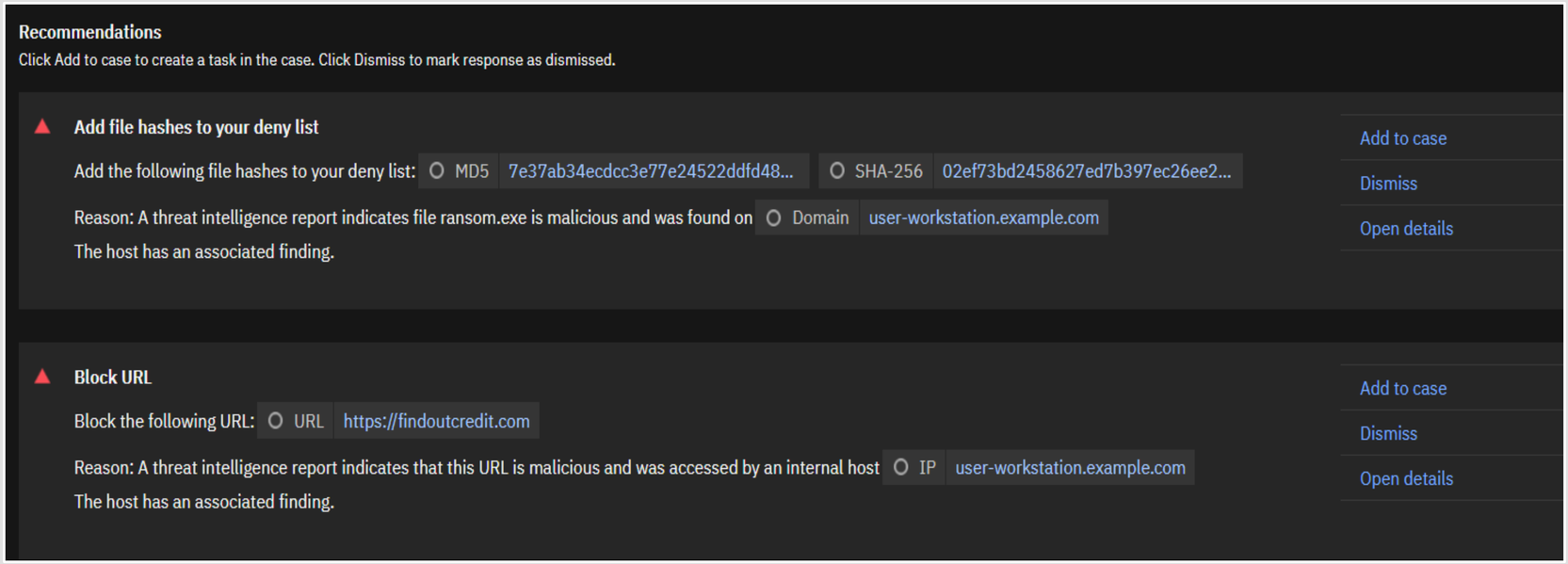
- Collect and prioritize alerts
- Aggregate alerts from multiple sources
- Enrich with telemetry, asset information and Threat Intelligence
- Build threat timeline and graphs
- Map on MITRE Framework



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

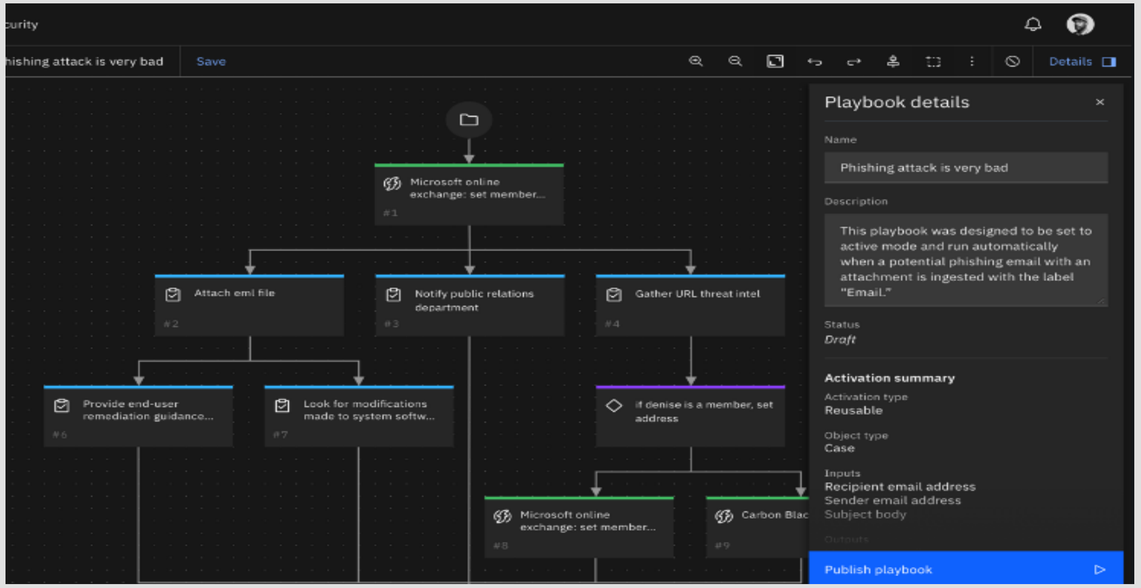
Zero Effort

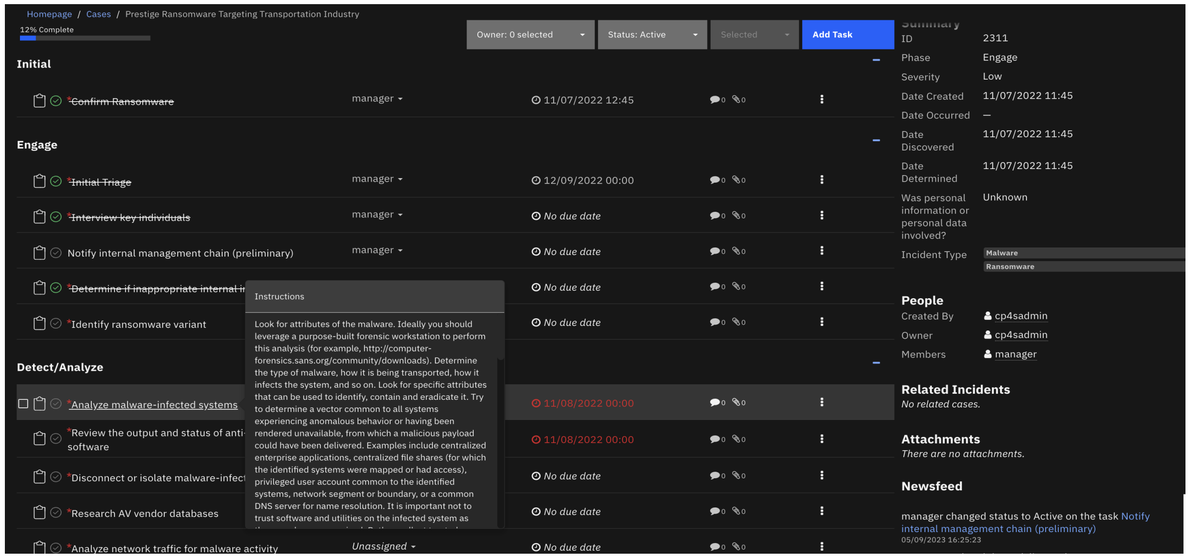
- Collect and prioritize alerts
- Aggregate alerts from multiple sources
- Enrich with telemetry, asset information and Threat Intelligence
- Build threat timeline and graphs
- Map on MITRE Framework
- Suggest tactical recommendations



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

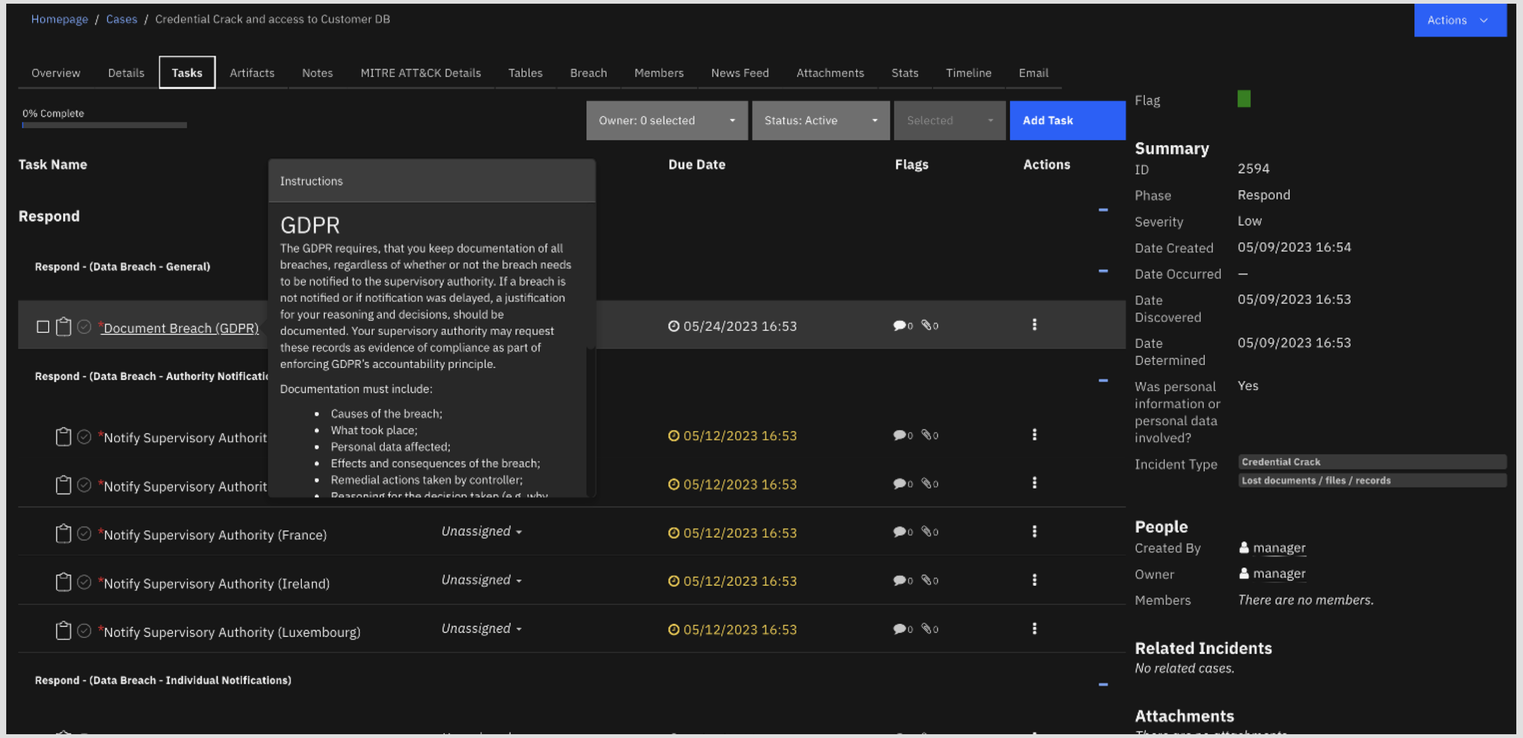


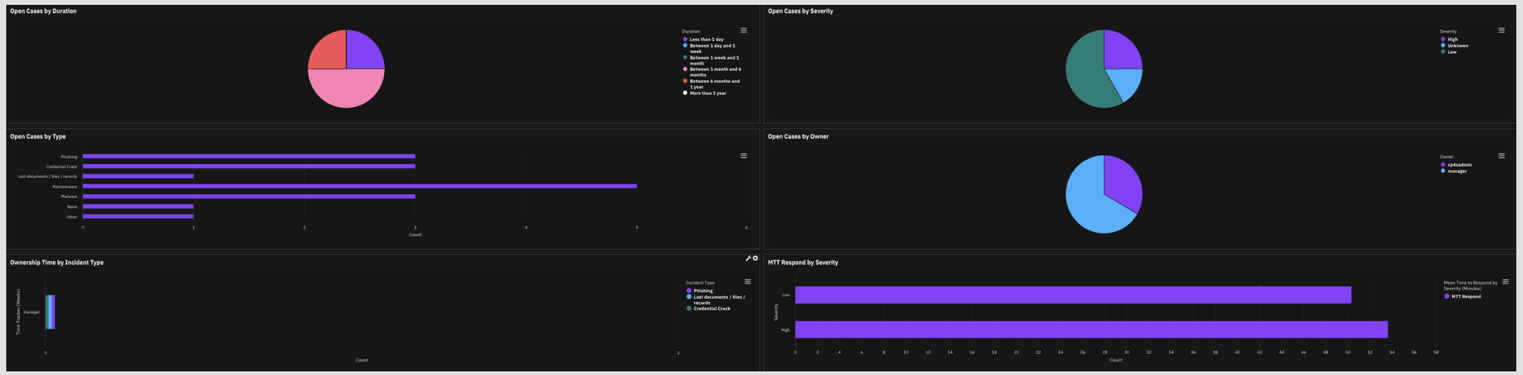


- Trace everything and collect evidences
- Monitor progression of incident resolution
- Simulation scenarios to test effectiveness of procedures and preparation of personnel
- Long-term improvement of security policies and posture

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





Thank you