

*“Consolidated Security Platforms
Are the Future”*

IBM way for integration and management of cyber security data

Emil Melamed

Customer Success Manager Architect IBM

The Challenge

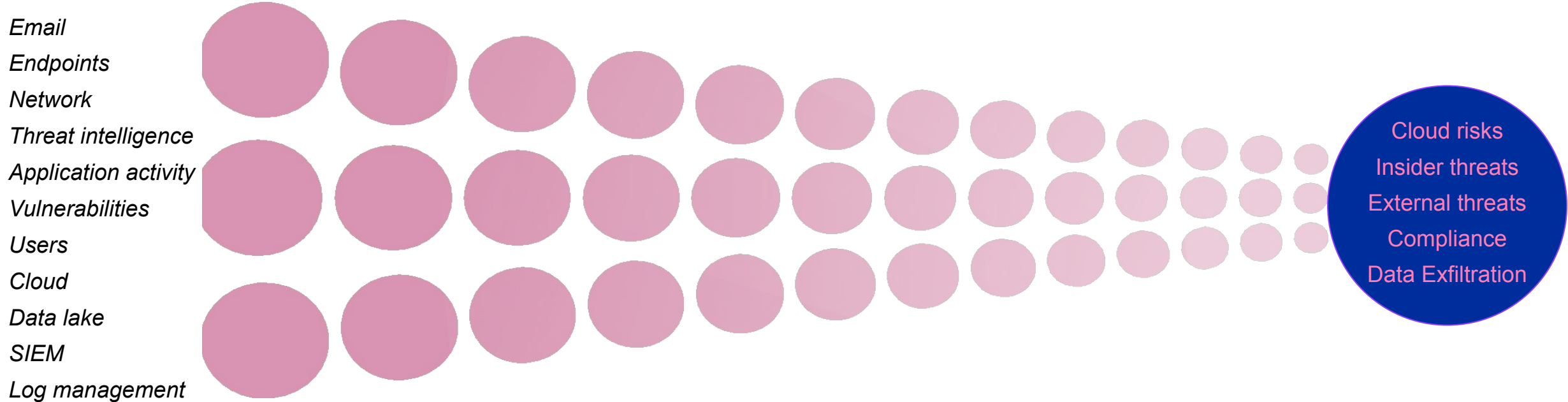
- Find all IOCs for the threat
- Search all data sources for threats, patterns, IOCs, and more
- Build the case attributes and prepare the playbook for incident response (quarantine the infection, isolate resources, escalation reports, etc.)
- Orchestrate the tasks from the playbook



A top-down view of a cluttered workbench or toolbox. The scene is filled with a wide variety of tools and hardware. In the foreground, several screwdrivers with different handle materials (wood, plastic, metal) and colors (red, black, blue) are prominent. There are also several pairs of pliers, some with long handles, and various wrenches. A large, cylindrical brush with a dark handle is positioned in the upper center. The background shows more tools, including what appears to be a red toolbox or container, and various metal rods, bolts, and nuts. The overall impression is one of a well-used, multi-tool environment.

60% of companies use 25+ unique security products, and
44% engage with 10+ vendors

The complexity of threat management



SOC
analysts
need help
with...

Visibility

- Normalization
- Categorization
- Enrichment
- Operationalize data at rest
- Network, endpoint, cloud, user and application

Detection

- MITRE ATT&CK®
- Models
- Behavior chaining
- Global threat intelligence

Investigation

- AI
- Link analysis
- Data mining
- Supervised learning
- Unstructured data analysis
- Federated search

Response

- Dynamic playbooks
- Automation
- Orchestration
- Privacy breach reporting

IBM Cloud Pak for Security

An open multicloud platform to gain security insights, take action faster, and modernize your architecture



Modular security capabilities

Threat Management

Data Security

Identity & Access Management


Open Security Ecosystem


Platform services

- Data connection
- Asset enrichment
- Case management
- Orchestration
- Automation
- Development tools

Open and integrated hybrid multicloud platform

SIEM tools EDR tools Cloud repositories Data lakes Database protection Network protection Additional point solutions


On premise


Hybrid Cloud


Multicloud

Case Management Security Orchestration, Automation, and Response (SOAR)

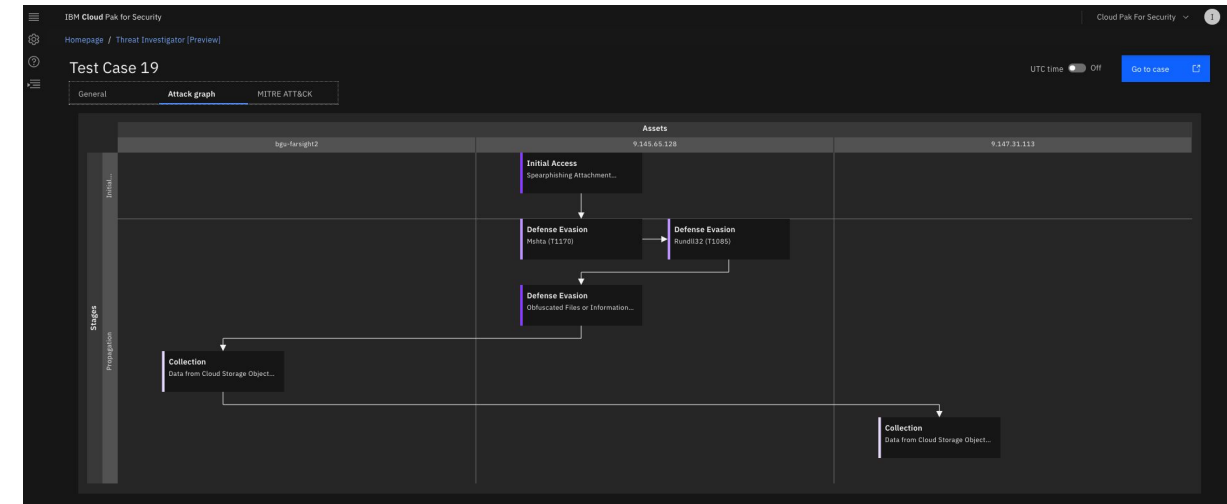
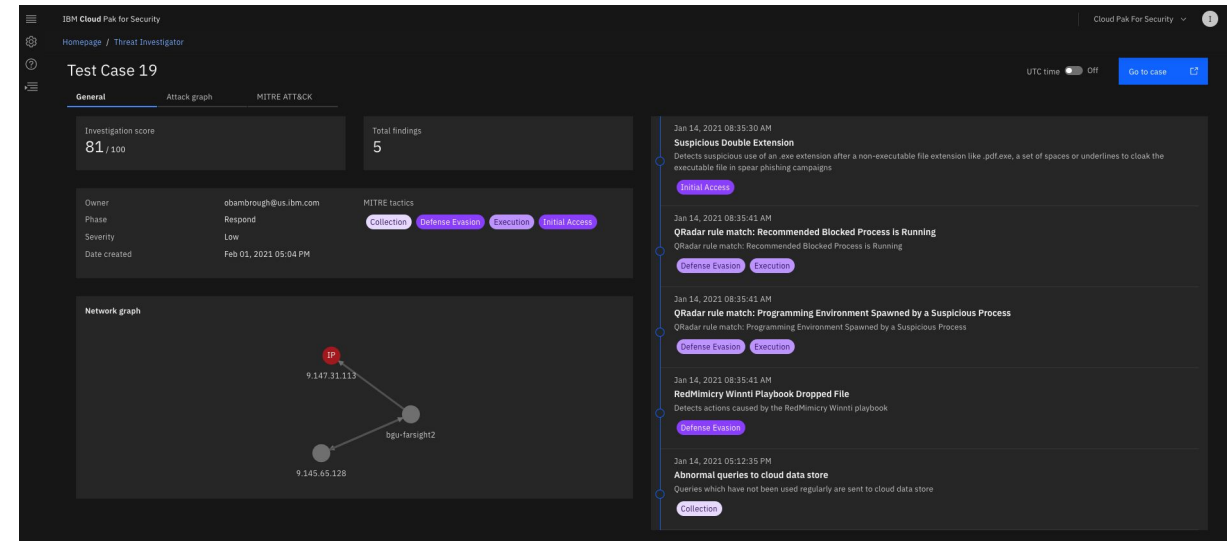
- Reduce time to respond to and remediate complex cyber threats by automating incident response processes
- Streamline and automate manual and repetitive tasks
- Guide and execute investigation and response actions consistently with robust case management and tasks, leveraging visual process techniques from lean manufacturing
- Drive investigations across the organization via simple point-and-click deployment of 160+ third-party integrations
- Customize and extend dynamic playbooks through a visual workflow editor

The screenshot displays a SOAR interface with a dark theme. At the top, a 'Cases' dashboard shows filters for 'All cases' (46), 'Unassigned' (2), and 'My cases' (3). A search bar and a 'Create case' button are also visible. Below the dashboard, there are cards for 'New (4)' and 'In progress (42)' cases. One case card is titled 'X-Force IRIS Finds New TTPs on POS Network Intrusion' and another is 'MuddyWater APT Expansion of Operations and Latest Activity'. A detailed view of a case titled 'APT41 Dual Espionage and Cyber Crime Operation' is shown in the foreground. This view includes a description, tabs for 'Details', 'Tasks', 'Notes', 'Members', 'News Feed', 'Attachments', 'Stats', 'Timeline', 'Artifacts', 'AWS IAM', and 'Analyze'. The 'Artifacts' tab is active, showing a network diagram with nodes for 'IP Address 67.229.97.229', 'User: Malware Case', 'Malware MD5 Hash 846c0b52184facb', 'AWS IAM User Name Daniel.Jones', 'APT41 Dual Espionage and Cyber Crime Operation', and 'IP Address 192.168.0.8'. A 'Timeline' view is also visible at the bottom of the case details. On the right side of the case view, there is a 'Summary' section with fields for ID, Phase, Severity, Date Created, Date Occurred, Date Discovered, and Incident Type. Below this is a 'People' section with 'Created By', 'Owner', and 'Members'. A 'Related Incidents' section lists other cases, and an 'Attachments' section is empty. A 'Newsfeed' section shows a list of recent actions performed by 'Mark A Neumann'. At the bottom right, there are buttons for 'Generate Case Report' and 'Download Case History Report'.

Threat Investigator

Automated alert investigation driving faster more consistent and accurate responses

- AI driven threat priorities
- Search all your data sources for evidence automatically
- Understand the source and impact of the attack so you can respond effectively
- Create a timeline view of the attack so you know what has happened and when it happen
- Map investigations to MITRE ATT&CK tactics and techniques



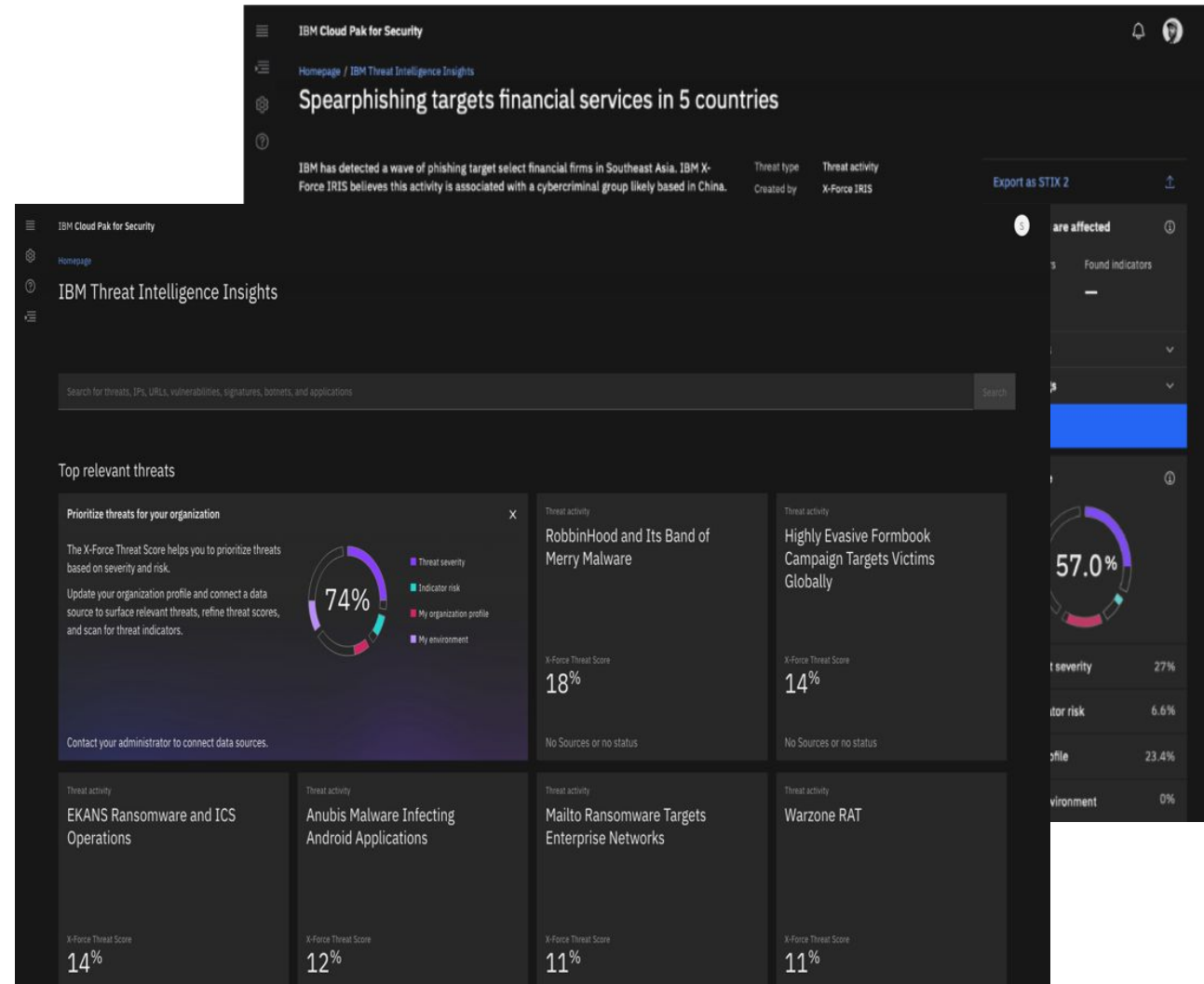
The screenshot displays the 'MITRE ATT&CK' table for 'Test Case 19'. The table maps the observed attack events to specific MITRE tactics and techniques.

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Spearghaling Attachment	PowerShell Command-Line Interface			Mimicry Hunk32 Hunk32 Obfuscated Files or Information				Data from Cloud Storage Object			

Threat Intelligence Insights

Prioritized, actionable threat intelligence

- Gain global threat intelligence through reports with contextual information curated by the IBM X-Force team
- Prioritize threats with the X-Force Threat Score, based on relevance, severity, penetration, impact and environmental sightings
- Identify and act on threats active in the environment with “Am I Affected”—continuous, automated searches across data sources; cases created automatically for active threats
- Leverage investments in 3rd-party threat intelligence feeds through a simple single configuration screen and enrich information throughout the platform



STIX — the Structured Threat Information eXpression

TAXII — the Trusted Automated Exchange of Intelligence Information

- Exchange cyber threat intelligence (CTI)
- Prepare and respond to upcoming attacks
- Automated threat exchange
- Integrate into existing tools and products



Thank you