Automatic Threat Investigation

Making the Forest from the Trees

IBM

Prof. Yaron Wolfsthal

Head, IBM Cyber Security Center of Excellence
Beer Sheva, Israel

May 13, 2021 – FIWARE Cybersecurity Day

Speaker Info

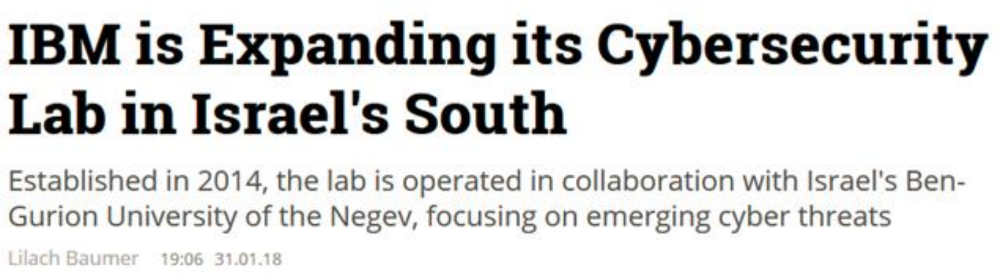
IBM Research Lab

Cyber Security Center of Excellence

Innovation arm for IBM:

- AI-based security analytics
- Threat Management
- Cloud security
- Exploring new solutions and architectures

IBM Cloud Pak for Security



IBM is Expanding its Cybersecurity Lab in Israel's South

Established in 2014, the lab is operated in collaboration with Israel's Ben-Gurion University of the Negev, focusing on emerging cyber threats

Lilach Baumer 19:06 31.01.18

Challenges of the Modern SOC

- Flood of alerts
- Shortage of qualified staff
- Too many tools, too many technologies
- Increasing threat landscape

Threat Management Lifecycle
The Investigation Bottleneck

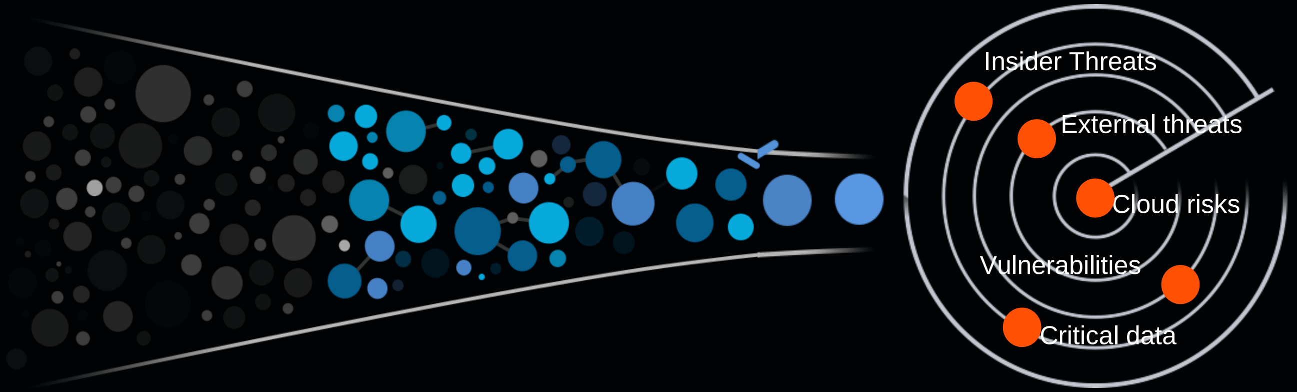
Monitor

Detect

Investigate

Respond

Endpoints
Network
Users
Threat Intelligence
Email
Vulnerabilities
Application activity
Cloud



Insider Threats
External threats
Cloud risks
Vulnerabilities
Critical data

Incident Investigation
Not an Easy Task

Is it an ongoing attack?

What systems where affected?

Did I lose any data?

Where did the attacker infiltrate from?

Did the attacker achieve persistence?

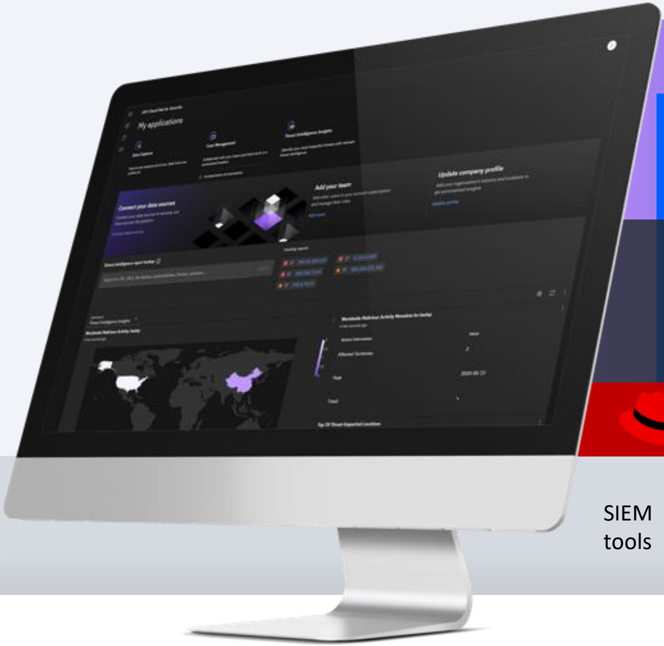
Who is the attacker?

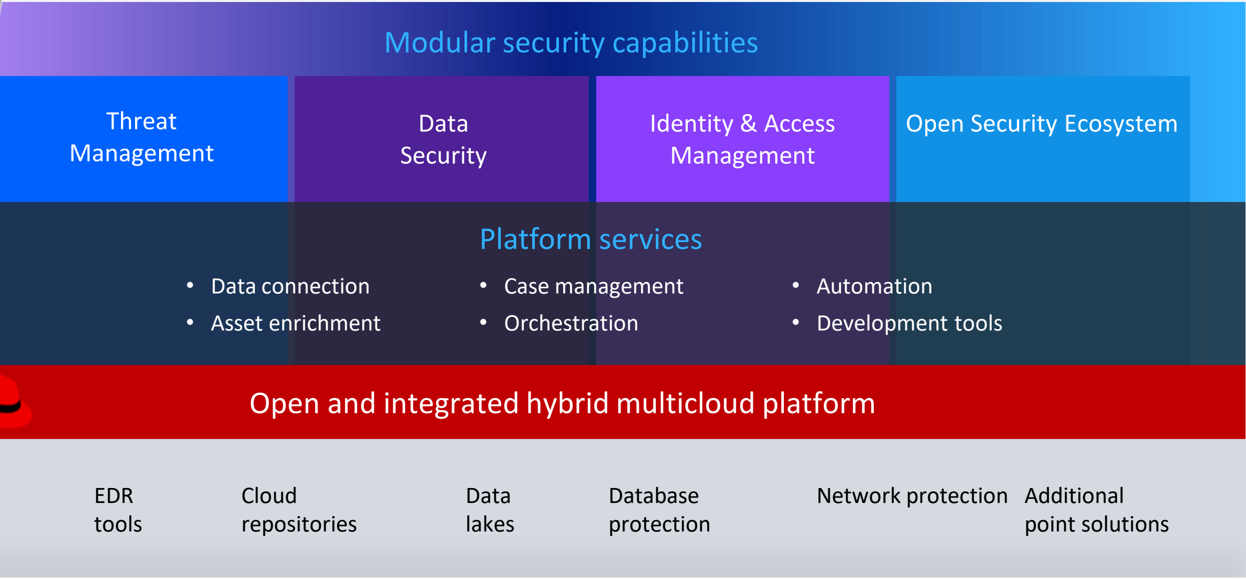
What is he after?

What tools does he use?

IBM Cloud Pak for Security

An open multicloud platform to gain security insights and take fast action





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

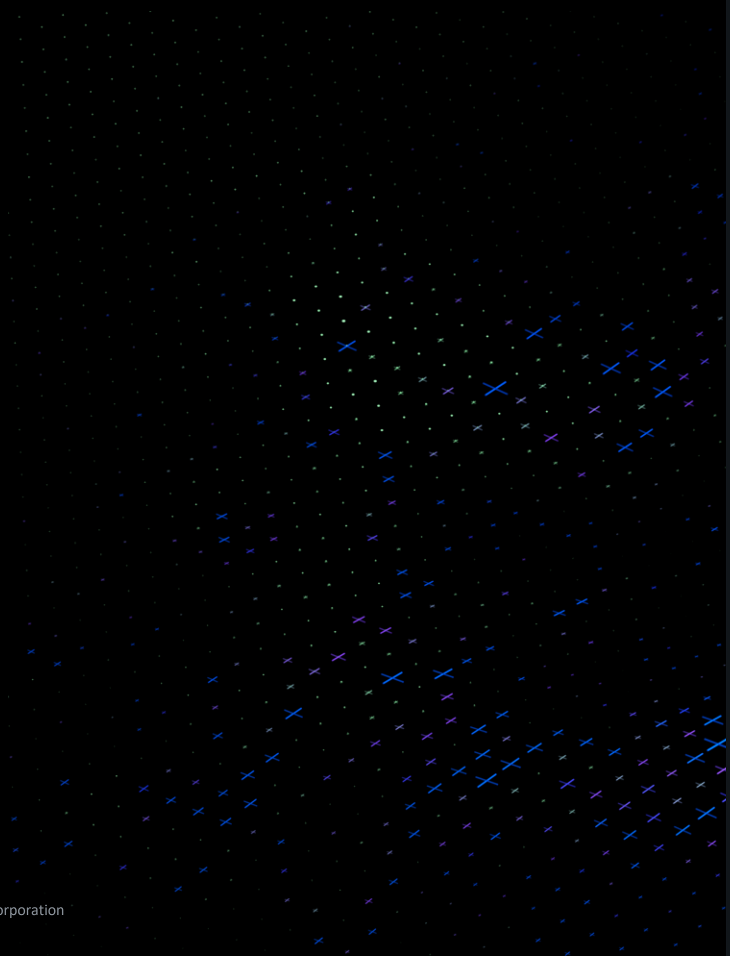
SIEM tools | EDR tools | Cloud repositories | Data lakes | Database protection | Network protection | Additional point solutions

On premise

Hybrid Cloud

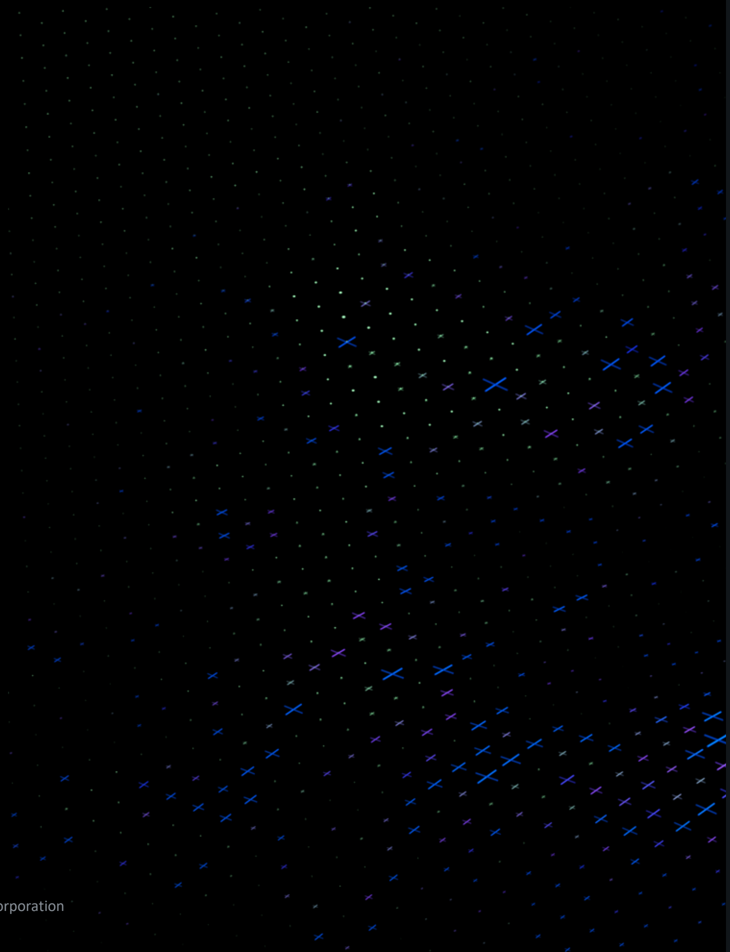
Multicloud

Remember Modern SoC?



Security Event
Security Event
Security Event
Security Event
Security Event
Security Event
Security Event
Security Event
Security Event
Security Event

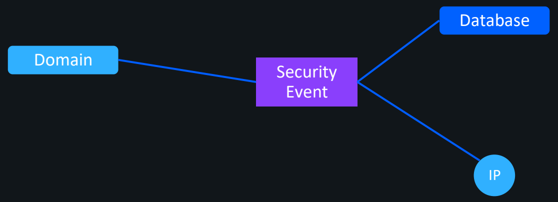
Automatic investigation



Security Event

Automatic investigation

Data representation and linkage

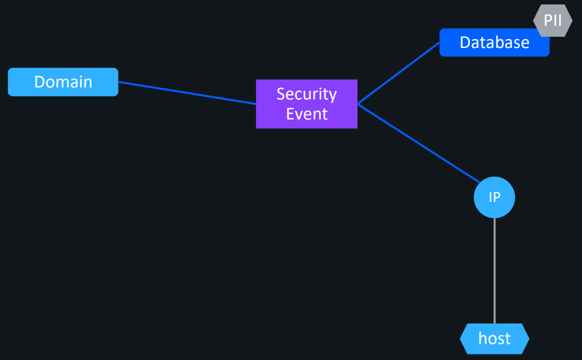


STIX MITRE | ATT&CK IBM Cloud Pak for Security

Automatic investigation

Data representation and linkage

Environment context



STIX

MITRE | ATT&CK®

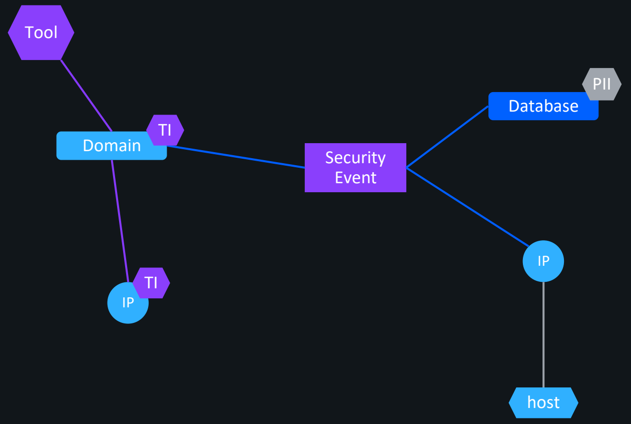
IBM Cloud Pak for Security

Automatic investigation

Data representation and linkage

Environment context

Threat intelligence integration



STIX

MITRE | ATT&CK®

IBM Cloud Pak for Security

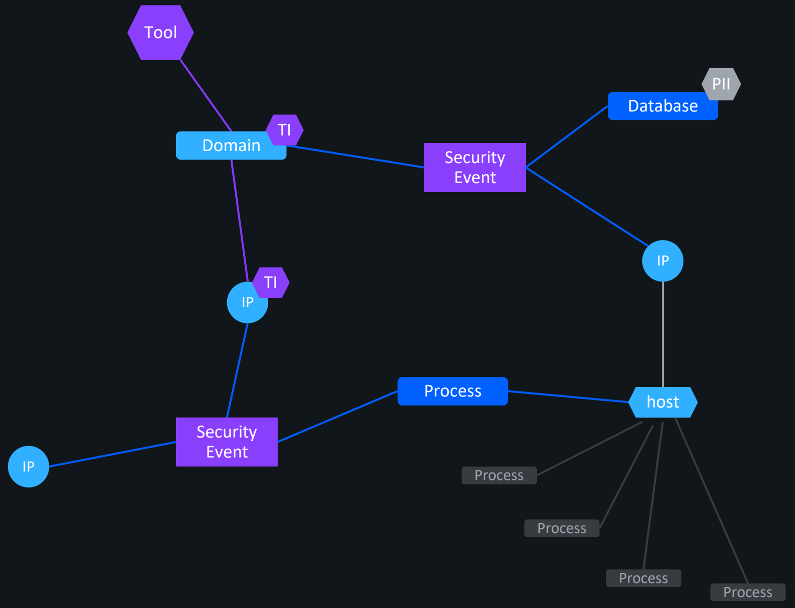
Automatic investigation

Data representation and linkage

Environment context

Threat intelligence integration

Forensics investigation



STIX

MITRE | ATT&CK®

IBM Cloud Pak for Security

Automatic investigation

Data representation and linkage

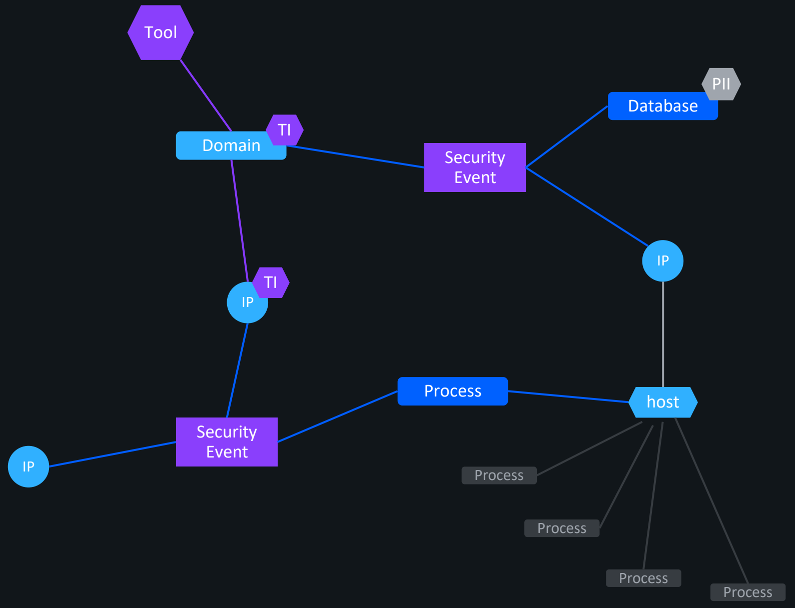
Environment context

Threat intelligence integration

Forensics investigation

Domain knowledge

Smart risk assesment



STIX

MITRE | ATT&CK®

IBM Cloud Pak for Security

Automatic investigation

Data representation and linkage

Environment context

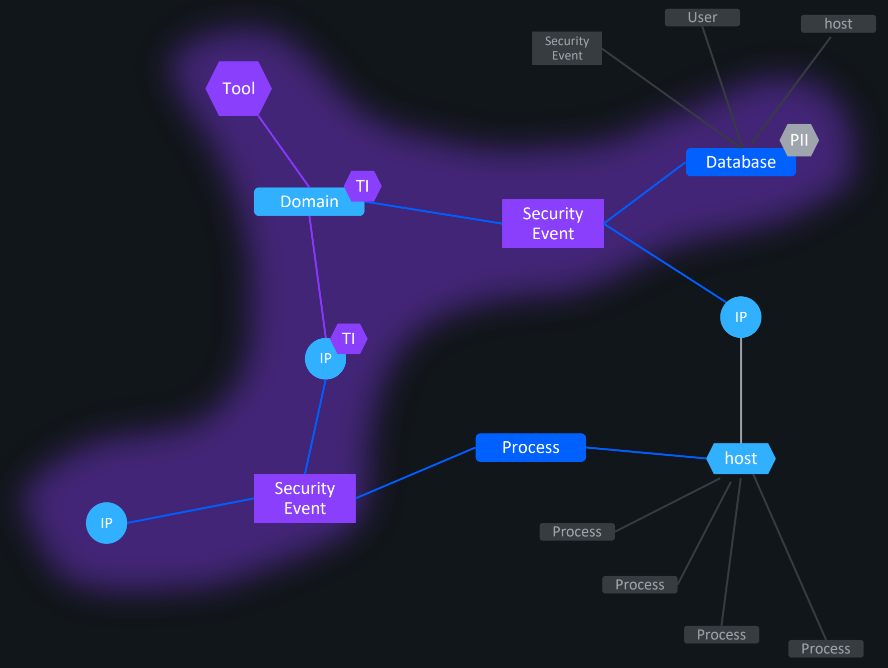
Threat intelligence integration

Forensics investigation

Domain knowledge

Smart risk assesment

Attack kill chain reasoning



Query Optimization

Machine Learning

Graph Theory

Belief Networks

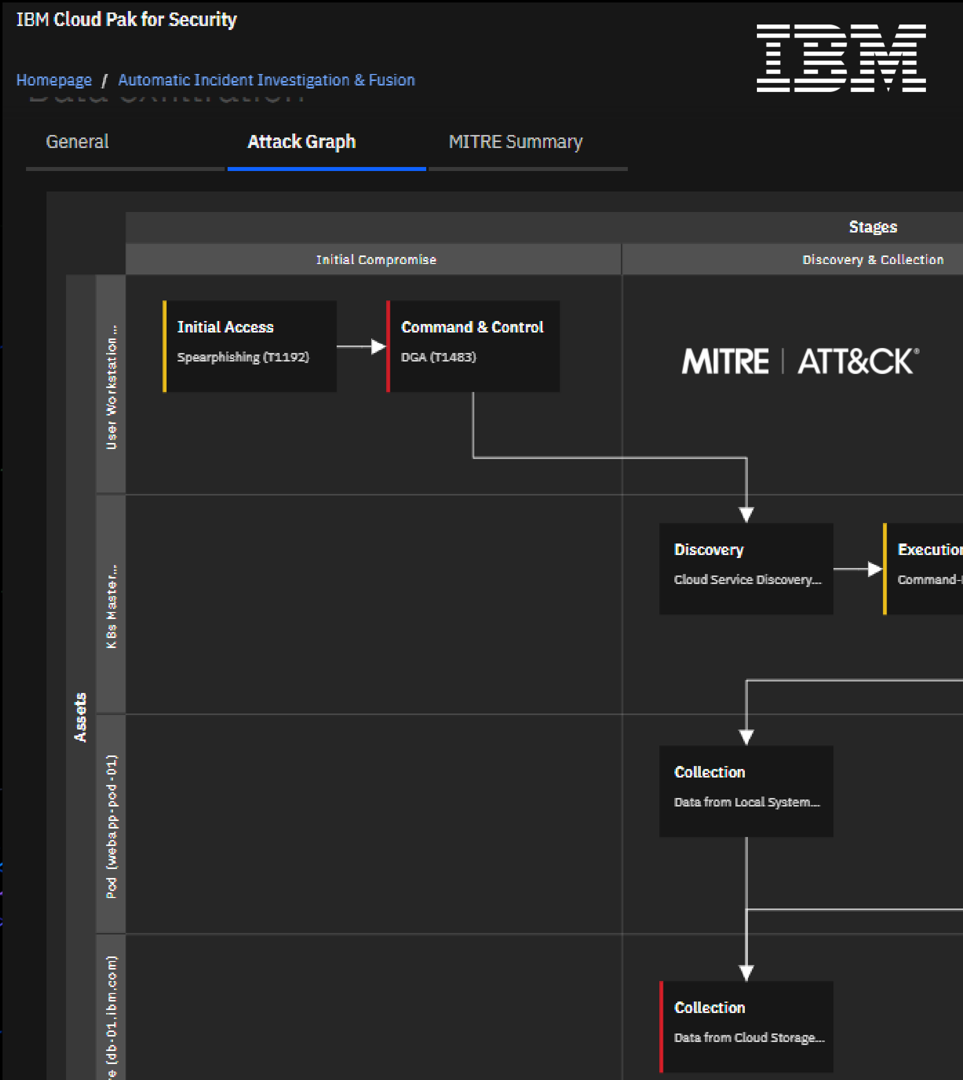
STIX

MITRE | ATT&CK®

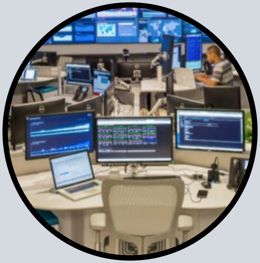
IBM Cloud Pak for Security

Automatic investigation

- Data representation and linkage
- Environment context
- Threat intelligence integration
- Forensics investigation
- Domain knowledge
- Smart risk assesment
- Attack kill chain reasoning
- Sofware / tools classification
- Threat actor classification
- Assistive interactive investigation



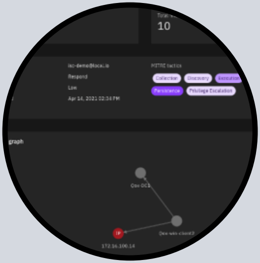
Automatic Threat Investigation: Summary



Improve the efficiency of the SOC by automating incident investigation

Access alerts and data from different security products in one place

Map alerts to Industry standard MITRE ATT&CK Tactics Techniques & Procedures



Present what happened in a clear and intuitive way to the analyst

Utilize AI to suggest what happened, what needs to be done and how to triage it all

Looking for collaborations

Q&A

Contact us

https://research.ibm.com/haifa/ccoe