CP4S Hackathon Use Case: Diamond Model of Intrusion Analysis

Use Case - High level description

Energy company Nuclearplant is target by a cyber attack

1. Suspicious activity has been detected accessing sensitive company data , indicating a possible cyber attack

2. Critical PII data access discovery triggers an alert in Guardium

3. Alert is handled in Guardium and event forwarded to QRadar SIEM

4. Event analysis and correlation is processed in QRadar and an offense is created

5. Offense is forwarded by QRadar to CP4S for incident response processing

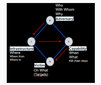
6. Analysis of the incident is handled in CP4S based on the „Diamond Model for Intrusion Analysis"

Use Case - Infrastructure

Use Case - Additional information on Diamond Model

IBM W7-2 methodology with Diamond model

Who : Which person or application generated the action
What: What action was performed
When: When did the event happened (absolute and relative time)
Where: On which object it happened?
Where From: From which object was the action initiated
Where To: Which object was the target of the action
On What: Which object was impacted
+
With Whom: Who were the collaborators in the activity
Why: Goal of the activity


Who
What
When
Where
Where From
Where To
On What
With Whom
Why
Actor
Victim
Infrastructure
Capability
Adversary
Event
Process
Cyber Observable
Cyber Intelligence
Cyber Attack
Cyber Forensics
Cyber Vulnerability
Cyber Weakness
Cyber Exploit
Cyber Deception
Course of Action
Cyber Resilience
Cyber Hygiene
Cyber Threat Intelligence
Cyber Situational Awareness
Cyber Threat Management
Cyber Risk Management
Cyber Resource Management
Cyber Supply Chain Management
Cyber Dependency Management
Cyber Workforce Management
Cyber Security Architecture
Cyber Security Engineering
Cyber Security Testing
Cyber Security Training
Cyber Security Education
Cyber Security Awareness
Cyber Security Governance
Cyber Security Compliance
Cyber Security Audit
Cyber Security Assessment
Cyber Security Monitoring
Cyber Security Detection
Cyber Security Response
Cyber Security Recovery
Cyber Security Forensics
Cyber Security Analytics
Cyber Security Intelligence
Cyber Security Threat Intelligence
Cyber Security Threat Management
Cyber Security Risk Management
Cyber Security Resource Management
Cyber Security Supply Chain Management
Cyber Security Dependency Management
Cyber Security