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"

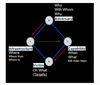
Use Case - Infrastructure

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

Maps intuitively to the Diamond Model of Intrusion Analysis:
http://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf


Who
What: Offense
When
Where
Adversary
Infrastructure
Where From
Where To
Capability
On What: Victim
Why
Goals
Capabilities
Methodology
Core Features
Meta-Features
Extension
Core Relations
Meta-Relations
Extension Relations
Core Meta-Relations
Extension Meta-Relations
Core Extension Relations
Meta-Extension Relations
Core Meta-Extension Relations
Core Meta-Extension Relations
Core