cerc 2021
THE 3RD CYBERSECURITY EDUCATION & RESEARCH CONFERENCE

Securing Critical Infrastructure

Ahmad Al-Sharif

Senior Cybersecurity Engineer

Diyar United Company - Kuwait

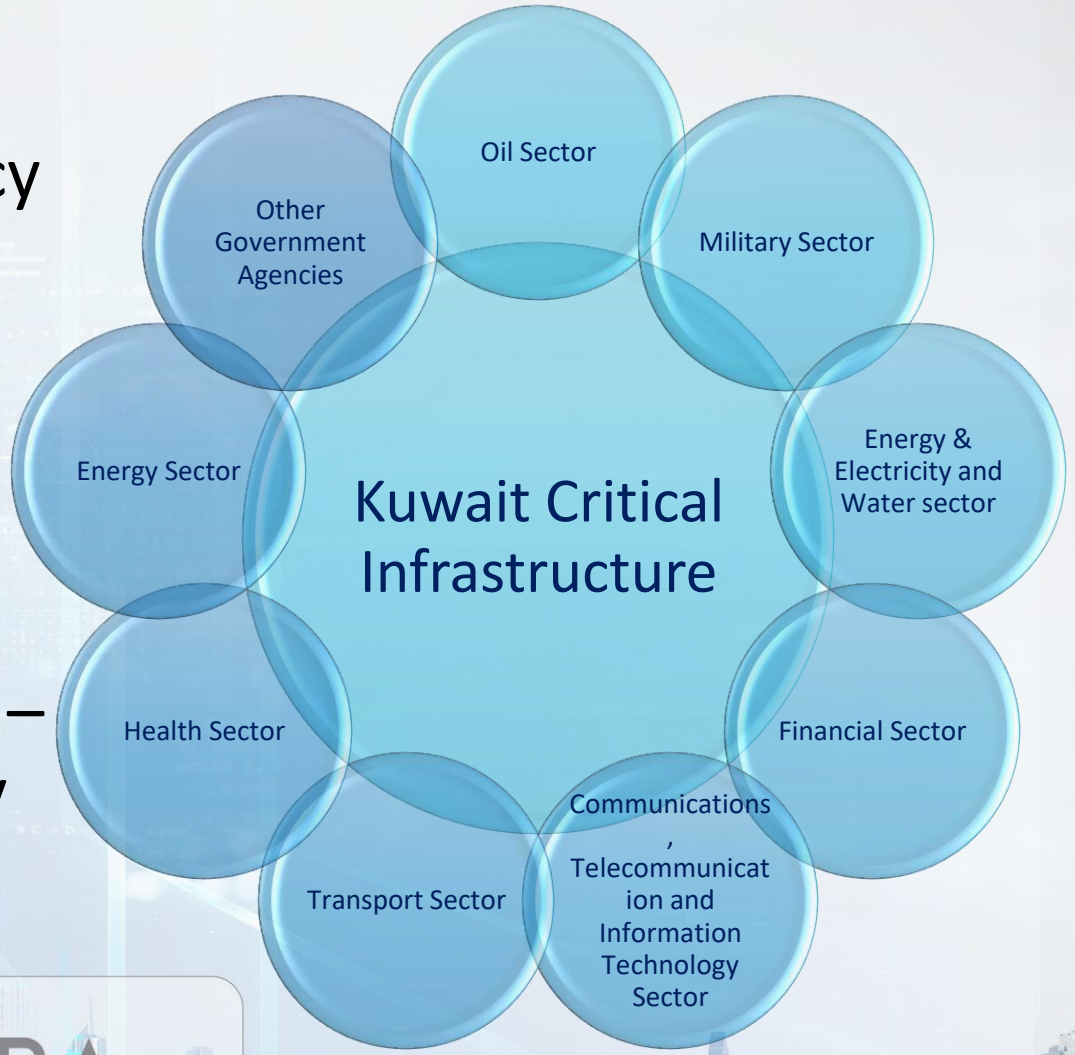
British Embassy Kuwait
GREAT BRITAIN & NORTHERN IRELAND
KUWAIT COLLEGE OF SCIENCE & TECHNOLOGY كلية الكويت للعلوم والتكنولوجيا
جامعة الكويت KUWAIT UNIVERSITY
CITRA
COMMUNICATION & INFORMATION TECHNOLOGY REGULATORY AUTHORITY

Let's face it, we're humans

- *"Rules are meant to be broken, and are too often for the lazy to hide behind"* – General MacArthur

Know your Critical Infrastructures

- The Cybersecurity & Infrastructure Agency (CISA) – US, identifies 16 critical sectors
- The Centre for the Protection of National Infrastructure (CPNI) – UK, identifies 13 critical sectors
- The Communication and Information Technology Regulatory Authority (CITRA) – Kuwait, as per the National Cybersecurity Strategy 2017-2020, identifies 9 critical sectors



Know your Critical Infrastructure

cerc 2021
THE 3RD CYBERSECURITY EDUCATION & RESEARCH CONFERENCE

- Common sectors
  - Information Technology
    - Data Centers
    - Disaster Recovery sites
  - Finance Departments
  - Threat and Risk Management Departments
  - SCADA Systems
    - Oil & Gas
    - Water Treatment
  - HIS Systems
    - Hospitals

British Embassy Kuwait
GREAT BRITAIN & NORTHERN IRELAND
KUWAIT COLLEGE OF SCIENCE & TECHNOLOGY كلية الكويت للعلوم والتكنولوجيا
جامعة الكويت KUWAIT UNIVERSITY
CITRA
COMMUNICATION & INFORMATION TECHNOLOGY REGULATORY AUTHORITY

How to manage

- Security Operations Center (SOC) and Security Information and Events Management (SIEM)
- Physical Security UEBA
  - Access points
  - Door points
  - Human Motion DB?
- SCADA UEBA
- HIS UEBA

User and Entity Behavior Analytics (UEBA)

- This is a multi-tiered use case in SIEMs
- One tier acts as the basis/trend
- The second tier processes the differences based on the first tier
- The basis/trend's timeline is dependent on the use case required
  - Process anomalies usually range between a week to a month
  - Access anomalies should usually range between two weeks and a month
  - Sensors anomalies should range between 1 and 5 hours

How to manage UEBA use cases

- SCADA/HIS system to be integrated with SIEM
- **Modify** the SCADA system to log user accesses to terminals as well as audit operations
- HIS audits are a default as per HIPAA compliancy
- Since systems differ, and according to the SIEM platform, accommodate username mnemonics with users
- Build specific behavioral analytics use cases
- SOC is a real-time operation. Eyes on screen are for live events being triggered according to specific use cases.

Case 1: GM's Office

- Employee tries accessing the GM's floor/office
- Access card denied
- Employee tries opening the door, door locked
- Employee forces the door open, the door opens (brute force)
- Employee enters and vandalizes the office or steals something
- The next day, GM notices something wrong, and they check the security camera footage.

Case 1: Applying UEBA and SOC

- Employee follows a constant trend, accessing certain areas throughout the month or specified time range
- Accessing the GM's office/floor triggers two alarms here:
  - Timing is different than that of base trend
  - Location is different that that of base trend
- Brute forcing the door open triggers two alarms:
  - Sensor is down (normal alarm)
  - Sensitive area sensor is down (normal alarm)
- SOC would see that two alarms were raised following each other. Triage would show the relationship. Prompt escalation to mitigate vandalism and/or theft with physical security personnel

Case 2: Water Treatment Factory

- Let's imagine having a disgruntled employee working in a water treatment factory.
- Employee at day T, becomes agitated, accesses the waste water tank system, and changes the amount of chlorine added into the waste water.
- Employee then changes pH level of waste water accepted
- This water is then pumped out into the sea or lake, killing marine life.
- After weeks of investigations; it is found that disgruntled employee changed the chlorine and acceptance levels of the waste water tank.

Case 2: Applying UEBA and SOC

- Waste water tank sensors should be applied into a UEBA
- First alarm trigger would be the UEBA use case triggering for a changed sensor rating
- Second alarm trigger would be to an operator accessing a non faulty unit (normal alarm)
- Third alarm trigger would be the UEBA use case triggering for a unit acceptance trend
- At any point in time, a SOC escalation of any of the alarms raised would trigger a response to resolve the issue

Case 3A: Hospital Registration Desk

1. Appointment scheduling managed by employees
2. Appointment number 3 has been booked for insured patient G.
3. Employee signs out and signs in with an elevated user's account.
4. Employee adds non-insured patient D's information as a dependent of patient G.
5. Employee signs out of elevated user's account, and signs back to their account
6. Employee adds another appointment for patient G
7. Employee changes patient G's initial appointment, and adds patient D (now a dependent)
8. Employee calls patient G, and confirms change of appointment, blaming the system as being slow during the initial appointment booking and the slot taken through another employee

Case 3A: Applying UEBA and SOC

- Impersonation step (point 3)
  - UEBA will trigger for the impersonation that occurred
  - A secondary alarm could be triggered if applied in the environment, which includes concurrent sign in's specifically over terminals (NAC integrations)
- HIPAA Breach (point 4)
  - This could be detected by a normal non-UEBA alarm
  - UEBA use cases can be applied for authorized personnel.
  - It is highly recommended to keep both types of alarms for these as there can be a huge number of false positives
- Duplicate appointments (point 6)
  - According to the hospital terms. This could be applicable in some scenarios. This would be considered as a normal alarm
- Social Engineering (point 8)
  - Although this is undetectable by a SOC or UEBA use cases, warrants security awareness to patients are a requirement. Patient G can take further actions according to the awareness bulletins

Case 3B: Patient Files

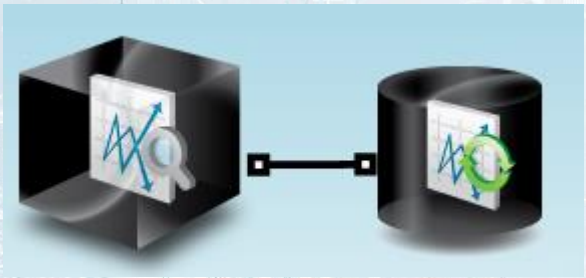
- Doctor is performing an approved statistical study on their patients
- Doctor doesn't have time to perform this statistical study during working hours.
- Hospital administrators blocked the usage of external storage (including cloud)
- Doctor requires patient data files to complete study. The doctor exports patients' medical records to their workstation
- Doctor emails these files after compressing them into 10, 10MB files, to be able to send them via email

Case 3B: Applying UEBA and SOC

- UEBA application on HIS audit
  - Triggers on doctor accessing multiple patient data within a certain time period
  - Triggers according to time frame in which doctor is accessing the system
- Exporting of patient medical record (MRI)
  - Normal alarm (prone to false positives due to nature of action)
  - UEBA triggers for multiple MRI exports within a time frame through one user
- Email Exfiltration
  - Normal alarm, with action taken to quarantine such emails
  - Some SIEMs/SOARs allow taking action on certain systems through an API when an alarm triggers.

Sample: UEBA Process Anomaly

Trend Baseline (Rule 1)
Primary Criteria = Process/Service Restarted/Restarting/Started/Starting/Startup or Shutdown Activity = Process/Service Stopped/Stopping
All Log Sources
Group By = User Origin
Data Fields = Process Name
Time and Schedule Live Time Period = 7 days Evaluation Frequency = 0mins Evaluation Schedule = Always Active



Expressions and Results
1. HistogramSimilarity(live:Process, baseline:Process) < 0.5 2. UniqueCount(live:Process) >= 5 3. UniqueCount(baseline:Process) >= 5
Results = 1 and 2 and 3

Trend Monitor (Rule 2)
Primary Criteria = Process/Service Restarted/Restarting/Started/Starting/Startup or Shutdown Activity = Process/Service Stopped/Stopping
All Log Sources
Group By = User Origin
Data Fields = Process Name
Time and Schedule Live Time Period = 7 days Baseline Time Period = 7 days Evaluation Frequency = 1 hour Evaluation Schedule = Always Active