Contribution ID: **514** Type: **Interactive Content Presentation**

The Nuclear SIEM

This paper will discussthe need for devices to capture Industrial Control System (ICS) communication-based data within the architecture of a Nuclear Power Plant (NPP)in order to detect, investigate, or mitigate cyber-events. Furthermore, this paper will discuss requirements and design principles for such a mechanism.
Communication flows within NPPsare based upon security zones implementing the requirements of security levels. The five security levels within the IAEA's example implementation in the Nuclear Security Series Draft on Computer Security Techniques for Nuclear Facilities (NST047)[1] are described to cover, based on a graded approach to addressing the consequences of compromise, protection systems (Security Level 1), operational control systems (Security Level 2), supervision real time systems (Security Level 3), technical data management systems (Security Level 4) and other systems (Security Level 5) [1].
In this regard, typically Security Levels 1, 2 and 3 form the ICS part of a nuclear power plant (Operational Technology - "OT"), while Security Levels 4 and 5 form the business portion of a NPP facility (Information Technology - "IT").
This architecture contains various devices to record different sets of data for different purposes. A Process Historian collects information about the underlying physical processes and makes them available for operators. Usually this Process Historian is situated on a zone within Security Level 3. This historian must store the data for somegivenamount of time. A Plant Historian stores the information about the underlying physical process for the whole duration of a power plant's operation. This data mostly serves analysts and system engineers. Such a Plant Historian resides on a zone underneath Security Level 4 and needs to be able to store data for a prolonged amount of time while ensuring the integrity of the data.
The business portion of the facility architecture often resideswithin a Security Information and Event Management (SIEM). TheSIEM is tasked with collecting data about the IT processes within the zones comprising Security Level 4 and 5, as well as storing and analyzing this data. Data collected here is not so much concerned with the physical process, but instead "IT-Data". Examples include the various properties of network communications or the state of the attached computing units. This data is relevant to detect potential security breaches.
As can be seen, there is currently no device responsible for capturing "IT-Data" within the OT-part of a plant' s architecture. However, the "IT-Data" available in this part of the overall architecture might prove helpful to identify, investigate, or mitigate security breaches. These data might include:
- information about network packets (to identify Flooding, Replay, Spoofing or Man-in-the-Middle attacks)
- information about the state of the processing units (to identify unusual cycle times within the processing units)
- aggregated information about this data in the form of events generated by anomaly detection systems situated within zones on Security Level 2 or 3
In addition, ICS protocol-specific information might be available ("ICS-Data"). This ICS-Data can also be correlated with the IT-Data and events.A device responsible for capturing this kind of data for the zones on Security Level 1-3would require a mechanism to ensure integrity and authenticity of the collected data since an attacker might be interested in falsifying or destroying this data.
This paper will discuss the benefits ofincludingan OT-SOC (Operational Technology Security Operation Center) and the usage of anomaly detection systems situated on zones within Security Level 2 or 3 to act as probes for a modified SIEM (referred to as the Nuclear SIEM) on a Security Level 4 zone.This convergence of IT-OT data within a NPP architecture provides a holistic view of a plant's data communications and provides a more advanced defensive posture against potential cyber-capable adversaries.
[1] IAEA: COMPUTER SECURITY TECHNIQUES FOR NUCLEAR FACILITIES; https://www-ns.iaea.org/downloads/security/security-series-drafts/tech-guidance/nst047.pdf (accessed 28/05/19)

State

Germany

Gender

Not Specified

Primary authors: ALTSCHAFFEL, Robert (Otto-von-Guericke Universität Magdeburg); HOLCZER, Tamás (BME Crysys); NEAL, Christopher; HILDEBRANDT, Mario (Otto-von-Guericke-University of Magdeburg)

Presenters: ALTSCHAFFEL, Robert (Otto-von-Guericke Universität Magdeburg); HILDEBRANDT, Mario (Otto-von-Guericke-University of Magdeburg)

Track Classification: CC: Information and computer security considerations for nuclear security