Hardening The Substation’s Security Posture By Utilizing Trust

Kwasi Boakye-Boateng[+], , Ali A. Ghorbani[+], Arash Habibi Lashkari[*]

[+]Canadian Institute for Cybersecurity (CIC), University of New Brunswick (UNB)

[*]York University

ABSTRACT

We present a possible solution to the increasing threat of Advanced Persistent Threats (APTs) targeting Intelligent Electronic Devices (IEDs) within substations in the Smart Grid. The integration of cyberinfrastructure has increased the substation's attack surface, and traditional defensive strategies are no longer enough. To address this, we propose developing a trust model that utilizes risk and knowledge components. Physical functional dependency and communication between devices will generate risk and knowledge components, respectively. The trust model will enable IEDs to be the last line of defense by detecting, thwarting, and alerting operators of potential attacks triggered by APTs. The proposed solution is proactive and will ensure that the substation remains secure and reliable. The approach is scalable, transferable, and can be implemented across various substation types. By leveraging the concept of trust, we can enhance the cybersecurity posture of the Smart Grid's substation infrastructure.

Problem

- Substation’s attack surface has increased due to the integration of cyberinfrastructure.
- Advanced persistent threats (APTs), such as Industroyer2 and PipeDream malware (discovered in 2022), are undetected until they launch their final attacks towards Intelligent Electronic Devices (IEDs) to trigger blackouts .
- Defensive strategies using gateways to allow legitimate access to the IEDs are easily bypassed because these APTs compromise the substation’s Human Machine Interfaces (HMIs).
- Implementing an intrusion detection system (IDS) within the substation's network increases the substation's network utilization, adversely affecting its operations' efficiency.

Motivation

- An approach is made toward utilizing the concept of trust to enable IEDs as the last line of defence.
- This means they can detect attacks, thwart attacks, and alert operators on the final-phase attacks when triggered by the APTs.
- The model should also provide the overall risk posture of the substation and rank of each IED

Proposed Protocol

$$E_f = \begin{cases} 0,\ \kappa_{E_f} = 1,\ \texttt{if}\ l_{h_i} < 7 \\ 0,\ \kappa_{E_f} = 2,\ \texttt{if}\ \gamma_{fs_R} \neq \gamma_{fs_i} \\ 0,\ \kappa_{E_f} = 3,\ \texttt{if}\ \gamma_{fc_i} = 0 \\ \frac{\Gamma_R \cdot \Gamma_i}{\|\Gamma_R\|\|\Gamma_i\|},\ \kappa_{E_f} = 0\ \texttt{if}\ E_f \geq E_f^T \\ \frac{\Gamma_R \cdot \Gamma_i}{\|\Gamma_R\|\|\Gamma_i\|},\ \kappa_{E_f} = 4\ \texttt{if}\ E_f < E_f^T \end{cases}$$

$$C_i = \begin{cases} 0,\ \texttt{if}\ \tau|\omega|xi|\chi|phi = 0, \kappa_C = 0 \\ \xi,\ \texttt{if}\ \xi \neq 0, \kappa_C = \kappa_\xi \\ \tau,\ \texttt{if}\ \tau \neq 0, \kappa_C = \kappa_\tau \\ \omega,\ \texttt{if}\ \omega \neq 0, \kappa_C = \kappa_\omega \\ \chi,\ \texttt{if}\ \chi \neq 0, \kappa_C = \kappa_\chi \\ \phi,\ \texttt{if}\ \phi \neq 0, \kappa_C = \kappa_\phi \end{cases}$$

$$E_i = \begin{cases} 1,\ \kappa_{E_i} = 0\ \texttt{if}\ \vartheta = 1 \\ 0,\ \kappa_{E_i} = 1,\ \texttt{if}\ \zeta_{pt} > \zeta_{pt}^T \\ \frac{Z_R \cdot Z_i}{\|Z_R\|\|Z_i\|},\ \kappa_{E_i} = 0\ \texttt{if}\ E_i \geq E_i^T \\ \frac{Z_R \cdot Z_i}{\|Z_R\|\|Z_i\|},\ \kappa_{E_i} = 2\ \texttt{if}\ E_i < E_i^T \end{cases}$$

$$\boxed{\beta_i = \begin{cases} \beta^T,\ \texttt{if}\ \theta_I = 1 \\ F_i - C_i,\ \texttt{if}\ \theta_I = 0 \\ F_i - C_i + \mu,\ \texttt{if}\ \theta_I = 0, \theta_\mu = 1, \beta_i^o < \beta^T \end{cases}}$$

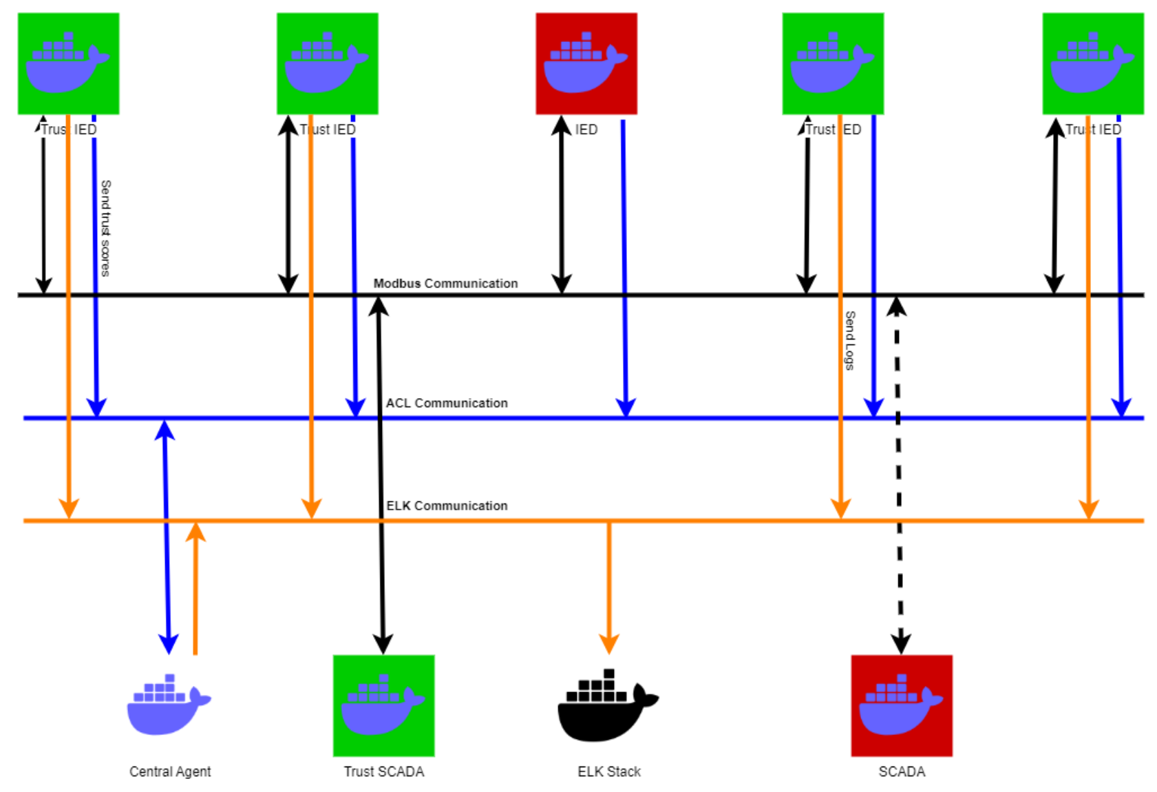
$$E_s = \begin{cases} 0,\ \kappa_{E_s} = 1\ \texttt{if}\ \psi_{\eta_i} \\ 0,\ \kappa_{E_s} = 2\ \texttt{if}\ \psi_{p_i} \neq 502 \\ \frac{\Psi_R \cdot \Psi_i}{\|\Psi_R\|\|\Psi_i\|},\ \kappa_{E_s} = 0,\ \texttt{if}\ E_s \geq E_s^T \\ \frac{\Psi_R \cdot \Psi_i}{\|\Psi_R\|\|\Psi_i\|},\ \kappa_{E_s} = 3,\ \texttt{if}\ E_s < E_s^T \end{cases}$$

$$\boxed{T_i = \{\beta_i, \kappa_{E_f}, \kappa_{E_s}, \kappa_{E_i}, \kappa_C\}}$$

$$F_i = \frac{2}{\sqrt{2}} \begin{vmatrix} \sqrt{\frac{1}{2}}E_f & \sqrt{\frac{1}{2}}E_f & 0 & 1 \\ 0 & \sqrt{\frac{1}{2}}E_s & \sqrt{\frac{1}{2}}E_s & 1 \\ \sqrt{\frac{1}{2}}E_i & 0 & \sqrt{\frac{1}{2}}E_i & 1 \\ 0 & 0 & 0 & 1 \end{vmatrix}$$

$$\boxed{\tau = 1 - \frac{2(1-\omega)}{m(m+1)} \left[\sum_{j=1}^{m} \left(\frac{j}{n} \sum_{i=1}^{n} \beta_i \right) \right]}$$

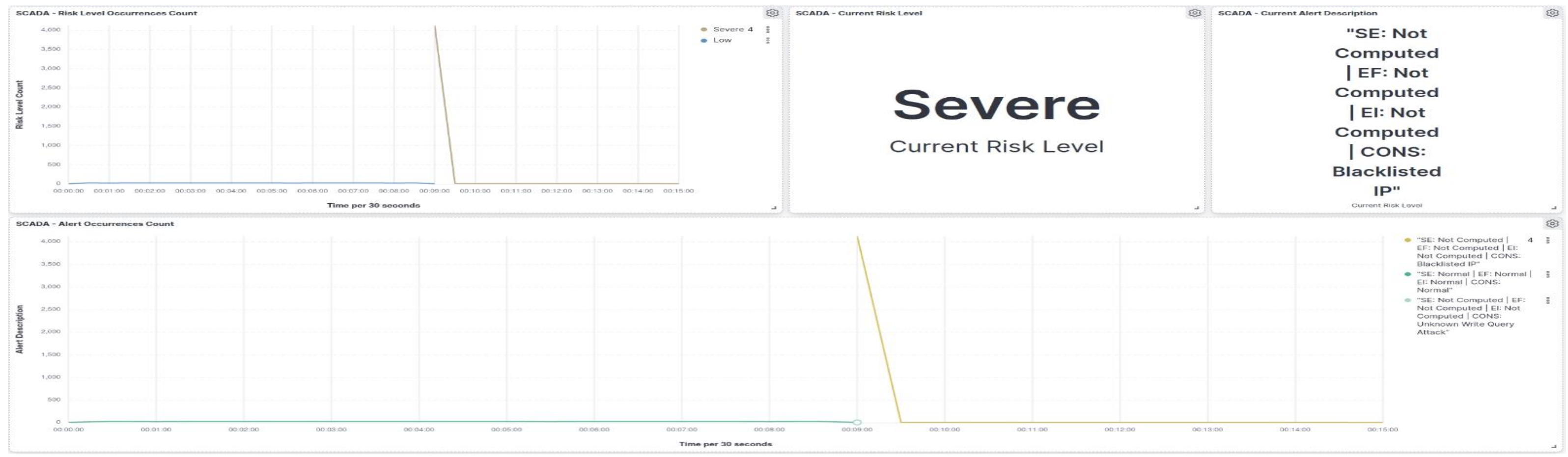
Testbed Setup



Tools Used

- Elasticsearch
- Python
- Java
- Docker
- JADE
- Modbus_tk

Results (Using SOC-style UI)


SCADA - Risk Level Occurrences Count

SCADA - Current Risk Level

Severe

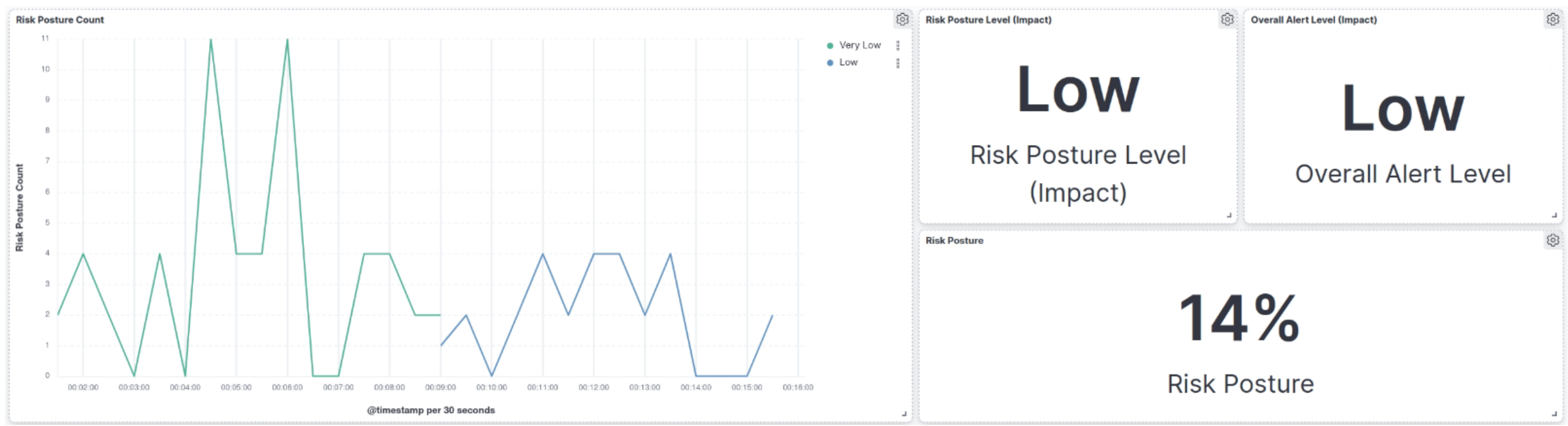
Current Risk Level

SCADA - Current Alert Description

"SE: Not Computed | EF: Not Computed | EI: Not Computed | CONS: Blacklisted IP"

SCADA - Alert Occurrences Count

Brute Force Write Attack Attack on Low-Ranked IED from Compromised HMI


Risk Posture Count

Risk Posture Level (Impact)

Low

Risk Posture Level (Impact)

Overall Alert Level (Impact)

Low

Overall Alert Level

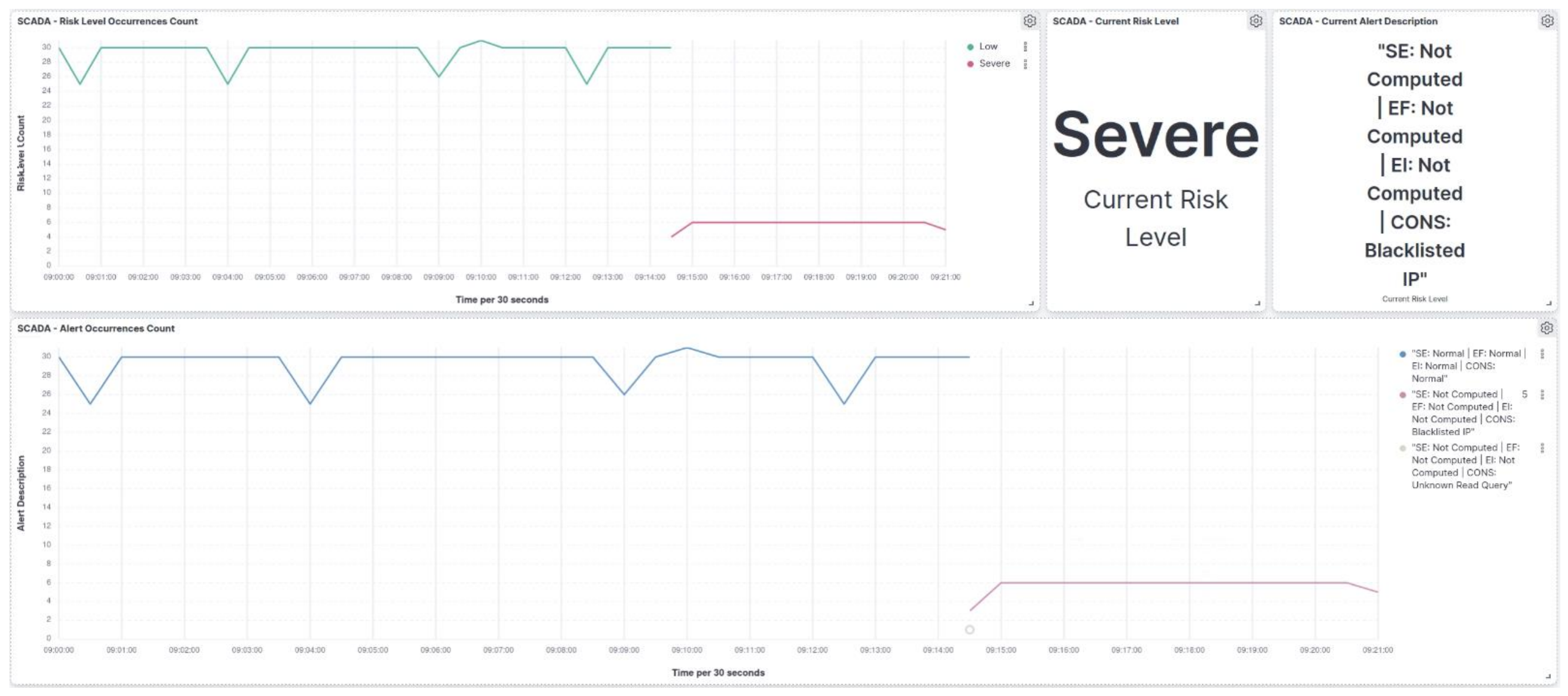
Risk Posture

14%

Risk Posture

Substation Risk Posture During Brute Force Attack on Low-Ranked IED From Compromised HMI

Results (contd.)


SCADA - Risk Level Occurrences Count

SCADA - Current Risk Level

Severe

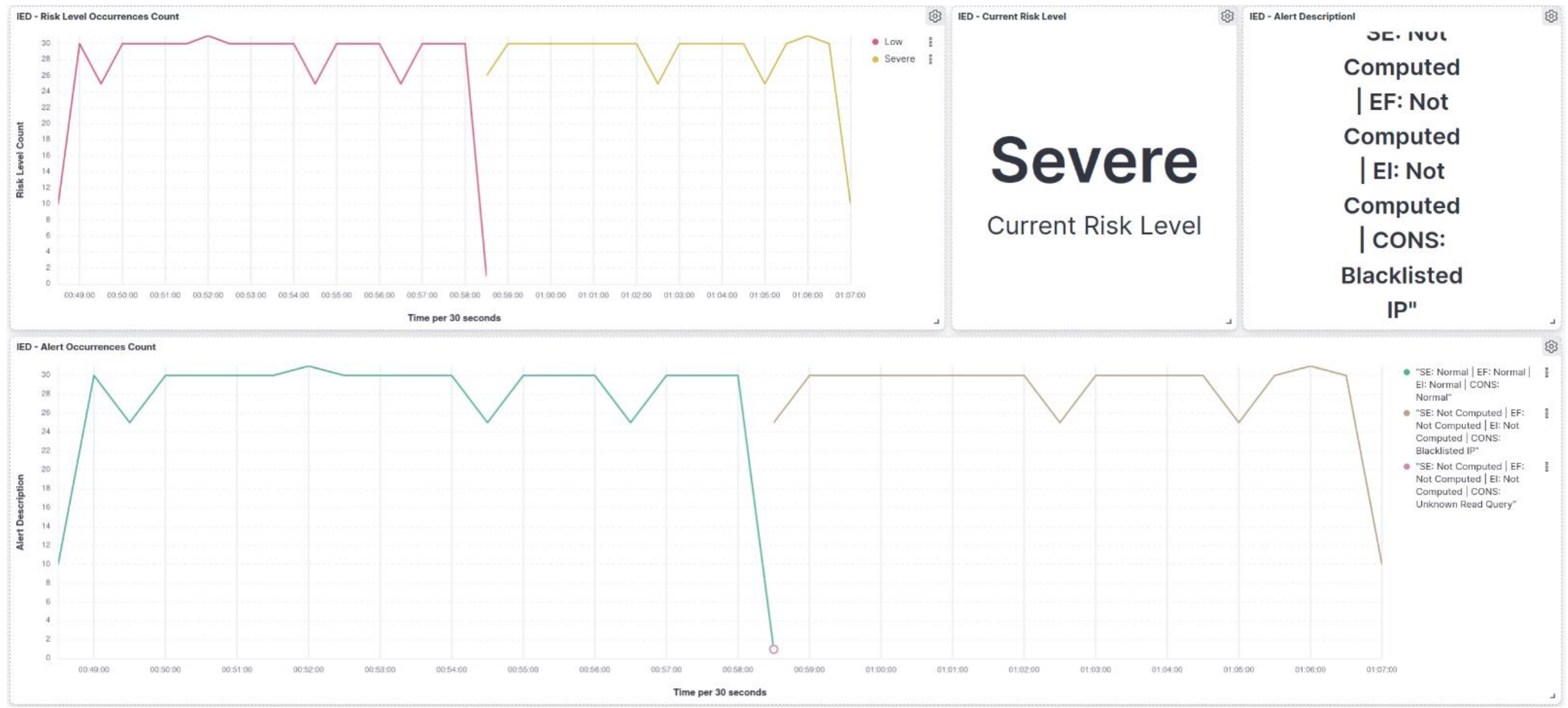
Current Risk Level

SCADA - Current Alert Description

"SE: Not Computed | EF: Not Computed | EI: Not Computed | CONS: Blacklisted IP"

SCADA - Alert Occurrences Count

Reconnaissance Attack on High-Ranked IED From Compromised HMI


IED - Risk Level Occurrences Count

IED - Current Risk Level

Severe

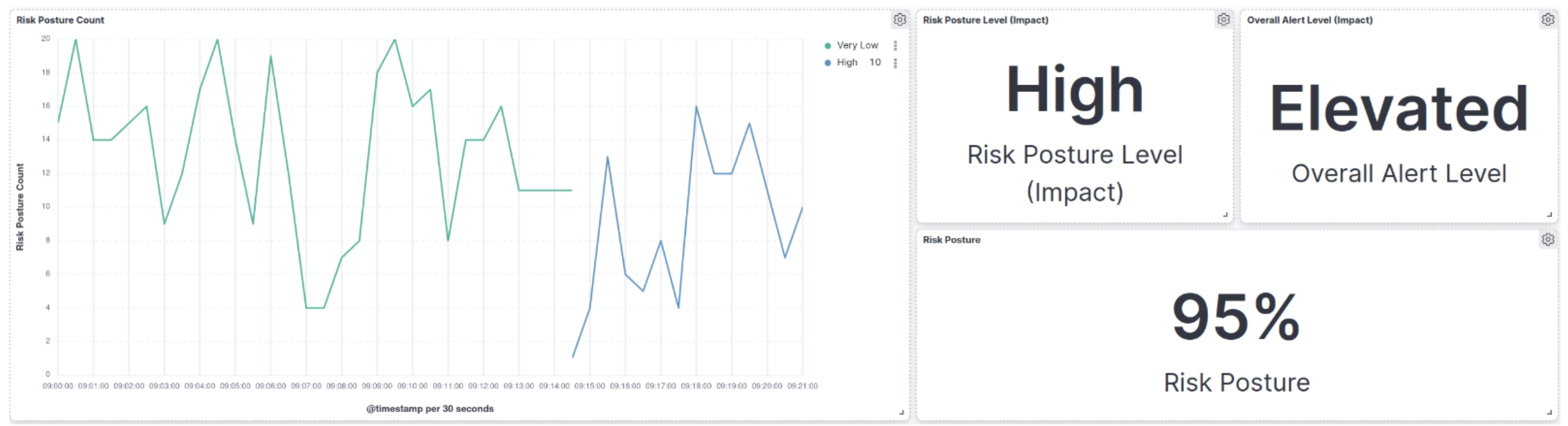
Current Risk Level

IED - Alert Description

"SE: Not Computed | EF: Not Computed | EI: Not Computed | CONS: Blacklisted IP"

IED - Alert Occurrences Count

False Data Injection Attack from Compromised High-Ranked IED Towards HMI


Risk Posture Count

Risk Posture Level (Impact)

High

Risk Posture Level (Impact)

Overall Alert Level (Impact)

Elevated

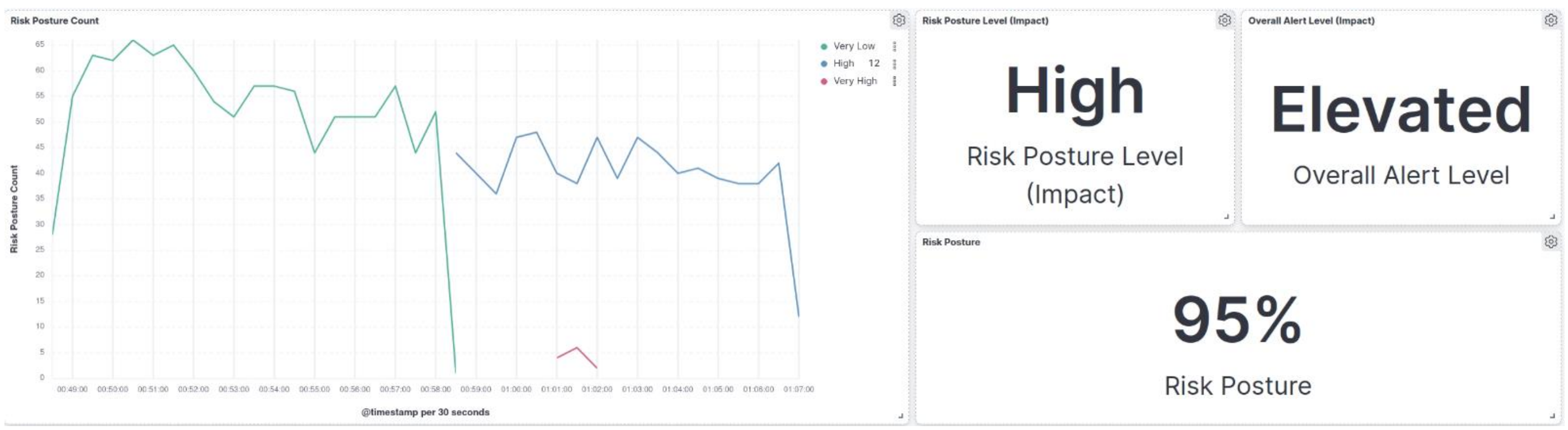
Overall Alert Level

Risk Posture

95%

Risk Posture

Substation Risk Posture During Reconnaissance Attack on High-Ranked IED From Compromised HMI


Risk Posture Count

Risk Posture Level (Impact)

High

Risk Posture Level (Impact)

Overall Alert Level (Impact)

Elevated

Overall Alert Level

Risk Posture

95%

Risk Posture

Substation Risk Posture False Data Injection Attack from Compromised High-Ranked IED Towards HMI

Conclusion and Future Work:

- Presented a trust model used for detecting attacks towards IEDs and SCADA HMI.
- Introduced a model that can compute the risk posture of the substation when the devices detect an attack towards them.
- Models were tested in a Docker environment and provided the results in SOC-influenced dashboard to show the status of the substation when attacks are made.
- Our model was robust against all attacks except of the baseline replay attack and the delay response attacks.
- These detecting these attacks will be considered as future work.
- Investigate the possibility of trust transferability as future works.