Angriffserkennung mit StationGuard

1 h | **Deutsch** | **# Wcyb04de**

In diesem Webinar erfahren Sie, wie Sie Cyberangriffe frühzeitig erkennen können. Sie erhalten einen Überblick über die Vor- und Nachteile der unterschiedlichen Ansätze zur Angriffserkennung (Blocklist, Allowlist, Selflearning, ...) und wir erklären Ihnen den Ansatz des StationGuard Systems im Detail. Sie erhalten Empfehlungen zum Schutz Ihrer Schaltanlagen auf Basis der umfangreichen Erfahrung unseres Teams. Wir zeigen Ihnen anhand von Beispielen, wie Geräterollen und Berechtigungen in StationGuard verwaltet werden.

Ziele

- Verstehen unterschiedlicher Ansätze zur Angriffserkennung und deren Stärken und Schwächen
- Den Ansatz kennen, der StationGuard so stark macht
- Hintergrund und Historie von OMICRON verstehen und wie dies hilft, ein maßgeschneidertes Produkt zur Angriffserkennung zu schaffen
- Empfehlungen auf Basis von jahrelanger Erfahrung mit und an Schaltanlagen

Inhalt

- Vielseitige Möglichkeiten der Angriffserkennung werden aufgezeigt und verglichen
- Der StationGuard Ansatz für ein gehärtetes IDS wird erläutert
- Die Entstehungsgeschichte von OMICRON wird aufgezeigt um zu verstehen, weshalb wir uns in Schaltanlagen wohlfühlen
- Die Geräterollen und die dazugehörigen Berechtigungen werden beispielhaft erläutert
- Der Wartungsmodus und dessen Einsatzmöglichkeiten werden vorgestellt

Lösungen

Angriffserkennung in Schaltanlagen mit StationGuard
Sichere Verwaltung von Konfigurationen und Prüfdokumenten mit ADMO
Cybersicheres IEC 61850-Prüfen mit StationScout ("Cyber-secure IEC 61850 testing with StationScout")

Teilnehmerkreis

Technisches Personal von Energieversorgern oder Unternehmen, die IEC 60870-5-104 oder IEC 61850-Kommunikation verwenden oder deren Verwendung planen.

Vorwissen

Keine Vorkenntnisse notwendig