SIEMENS
Ingenuity for life

Cyber Security Monitoring für Systemlösungen

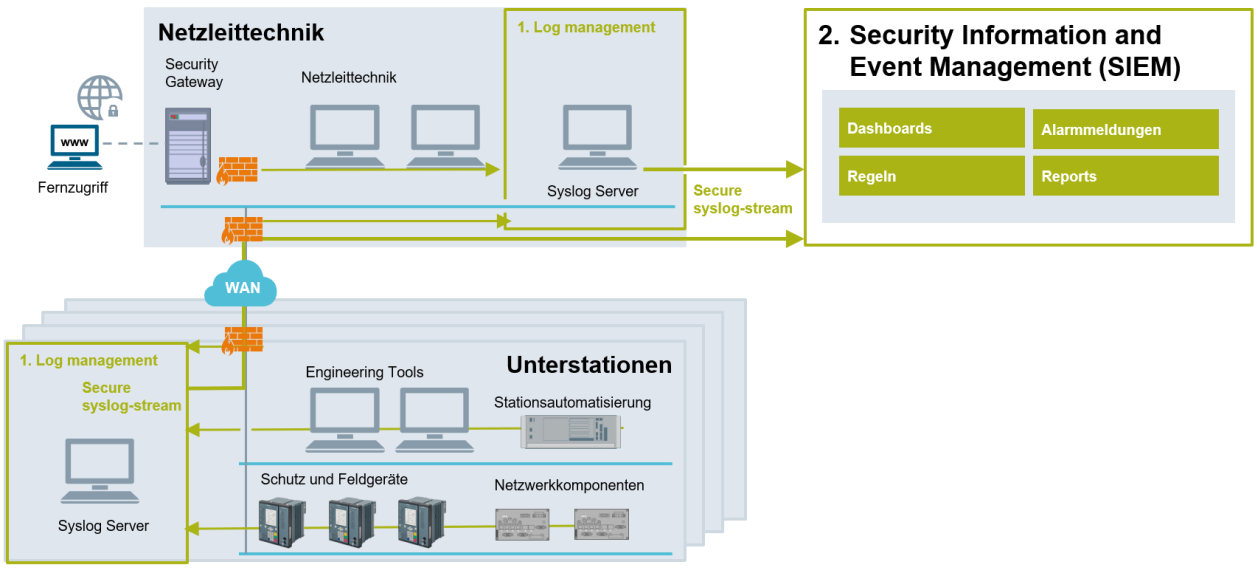
www.siemens.de/gridsecurity

Cyber Security für Energiesysteme

Der Schutz einer Energieautomatisierungsanlage allein reicht nicht aus. Es gilt Angriffsversuche auf die Systeme frühzeitig zu erkennen, um entsprechende Maßnahmen ergreifen zu können, bevor die Funktionen der Systeme durch den Angriff beeinträchtigt werden.
Die Lösung hierfür ist ein SIEM (Security Information and Event Management) System.

Was ist ein SIEM?

SIEM steht für Security Information and Event Management.
Ein SIEM sammelt alle Security relevanten Meldungen aus allen Komponenten des Systems. Die Informationen werden via „Syslog" Protokoll über einen Syslog Server, der als Zwischenspeicher agiert, oder direkt zum SIEM gesendet.
Die Security relevanten Informationen unterscheiden sich je nach Typ der Komponente. Generell werden Anmeldeversuche, Änderung der Konfiguration oder Ansprechen eines Schadsoftwareschutzes gemeldet. Eine Firewall meldet beispielsweise zusätzlich Zugriffsversuche auf geblockte Adressbereiche.
Diese Informationen werden dann im SIEM verknüpft, um anormales Verhalten des Systems zu erkennen.
Erkennt das SIEM einen Angriff oder eine Anomalie wird eine Alarmmeldung abgesetzt und der Operator beispielsweise via Mail informiert.
Die Syslog Informationen werden im SIEM gespeichert, um diese nach einem Cyber-Vorfall einer forensischen Analyse zuführen zu können.
In einem SIEM können Informationen aus verschiedenen Systemen intelligent verknüpft werden. Dies ermöglicht unter Umständen eine Erkennung eines Angriffs, der bei der Betrachtung eines einzelnen Systems unerkannt bliebe.
Das SIEM kann flexible Reports erzeugen, die eine bestimmte Störung oder einen Zeitraum abdecken.



Zuverlässig und sicherer

Internationale Standards und Regulierung
Auch internationale Standards wie IEC 27001, IEC 62443 und Branchenempfehlungen wie das BDEW Whitepaper (Bundesverband der Energie- und Wasserwirtschaft) adressieren die Themen „Logging“ und „Protokollierung und Überwachung“.
Eine manuelle Auswertung der Informationen ist in einer modernen Energieautomatisierungsanlage nicht möglich. Die Erfüllung dieser Anforderungen erfordert die Implementierung einer automatischen Auswertung der Informationen, also eines SIEM Systems.

Architektur
Die Architektur des Systems sieht das Sammeln der Security Informationen jeweils in den Unterstationen und in der Netzleitstelle vor. Von diesen lokalen Syslog Servern werden die Informationen zum zentralen SIEM System übertragen.

- Das stellt einen lückenlosen Zugriff auf die Informationen auch nach Verbindungsunterbrechungen zum SIEM sicher
- Das ermöglicht eine schlanke, sichere und verschlüsselte Schnittstelle von den Automatisierungssystemen zum SIEM
- Dies gibt ihnen die Möglichkeit ohne Eingriffe in die bestehende Infrastruktur, die Daten zukünftig an andere bzw. zusätzliche Systeme weiterzuleiten

Randbedingungen
Die wesentlichen Komponenten der Energieautomatisierungsanlage müssen die Security relevanten Meldungen sammeln und via Syslog Protokoll zur Verfügung stellen.

Die Siemens Komponenten für die Energieautomatisierung und Kommunikation wie SIPROTEC 5, SICAM A8000 und Ruggedcom erfüllen diese Anforderungen vollumfänglich.

Die Implementierung von Alarmregeln und Normalisierungen in einem SIEM erfordert des Weiteren tiefgreifende Kenntnisse der Funktionsweise und der Kommunikation eines Energieautomatisierungssystems, um Anomalien sicher von normalen Betriebsfällen unterscheiden zu können. Nur so können Fehlalarme minimiert werden.

Mit Siemens ProductCERT überprüft Siemens regelmäßig die Funktion der Siemens SIEM Lösung für unsere Energieautomatisierungslösungen. Das stellt sicher, dass potenzielle Angriffe von dem System sicher erkannt werden und Fehlalarme weitestgehend vermieden werden.

Moderne Siemens Unterstationen und Siemens Netzleitstellen erfüllen das Attribut „SIEM-ready“ und sind damit für zukünftige Anbindungen an SIEM Systeme vorbereitet.

Siemens SIEM Lösungen für Unterstationen und Netzleittechniksysteme erfüllen die Anforderungen internationaler Standards und unterstützen Betreiber kritischer Infrastrukturen bei der Einhaltung der regulatorischen Anforderungen wie Meldepflicht und Auskunftspflicht.

Unsere Leistungen:

- Lieferung des SIEM Systems inklusive SIEM-ready Hochrüstung ihrer Anlagen
- Implementierung von Alarmregeln im SIEM
- Regelmäßige Aktualisierung und Anpassung der Alarmregeln an aktuelle Bedrohungen
- Training für ihre Mitarbeiter

Siemens AG
Smart Infrastructure
Digital Grid
Humboldtstraße 59
90459 Nürnberg, Deutschland

Customer Support: http://www.siemens.com/csc

Cyber_Security_for_digital_Substations_Steckbrief_V3_2020_02.docx