SIEMENS
Engenhosidade para a vida

Soluções Siemens para Segurança Cibernética

www.siemens.com.br/ciberseguranca

A segurança cibernética é um dos pilares para a transformação digital, área altamente sensível na qual a Siemens foca sua atuação para garantir um elevado nível de segurança em seus produtos, sistemas, soluções e serviços.

O processo de integração e as soluções de segurança cibernética são aderentes as exigências de mercado, pois estão pautados em rigorosos padrões internacionais (por exemplo: IEC 62443, IEC 62351, NERC-CIP, IEC 27K etc.), garantindo assim alta disponibilidade com um alto patamar de segurança.

A Siemens foca esse tema com muita seriedade, contando com profissionais qualificados para garantir um elevado nível de segurança, desde a concepção das soluções até a implementação de seus projetos.

A Siemens considera uma abordagem holística para infraestruturas críticas, por meio de:

- Equipamentos concebidos com foco em segurança e soluções sistêmicas seguras;
- Processos adequados e políticas de segurança e
- Profissionais capacitados e conscientes sobre segurança cibernética, que entendem os riscos envolvidos e são treinados em operar sistemas críticos de maneira segura.

A solução Siemens é customizada para cada instalação e cliente, através das seguintes fases de projeto:

- Avaliação da infraestrutura;
- Plano de ação e implementação das medidas de segurança e
- Manutenção da segurança cibernética ao longo do tempo.

Nossos produtos são desenvolvidos de maneira segura e contam com uma série de funcionalidades de segurança cibernética embarcadas e de fácil integração, como por exemplo:

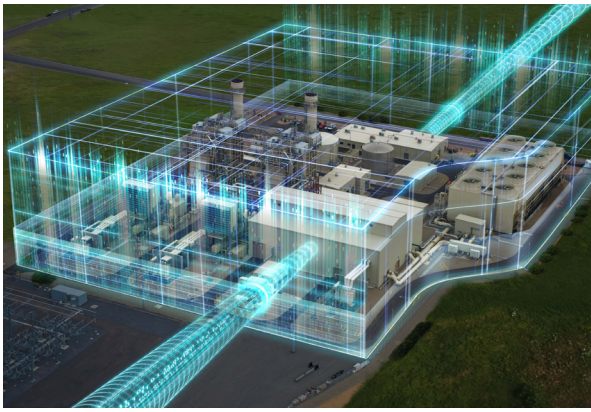
- Gerenciamento de contas de usuários com RBAC (Role-based Access Control);
- Logging e monitoramento de eventos de segurança com gestão central de alertas;
- Firmware digitalmente assinado, com uso de crypto-chip;
- Criptografia em protocolos e ferramentas de engenharia para tráfego de informação sensível;
- Armazenamento seguro de informações sensíveis dentro do equipamento e
- Equipamentos robustos e com mecanismos de defesa contra-ataques.

CLAROTY

Solução Claroty

A Plataforma Claroty para Detecção Contínua de Ameaças e Gestão de Vulnerabilidades foi projetada especificamente para garantir operações seguras e confiáveis em infraestruturas de redes industriais críticas e complexas, garantindo impacto zero nos processos operacionais e nos dispositivos OT subjacentes.

Ao extrair informações extremamente detalhadas sobre cada dispositivo conectado à rede industrial, construímos por meio de sistemas avançados de aprendizagem artificial um perfil de todas as comunicações e protocolos de ICS. Isso se torna a base de padrão comportamental que caracteriza o tráfego legítimo, permitindo assim que a plataforma Claroty alerte sobre quaisquer alterações, riscos e vulnerabilidades individuais ou sistêmicas, além de ameaças da rede.



Especificação Técnica da Solução

Continuos Threat Detection (CTD)

Principal pilar da Claroty, o Continuos Threat Detection fornece visibilidade extrema, monitoramento contínuo de ameaças e vulnerabilidades e insights profundos sobre as redes ICS. Suas principais funções são:

Monitoramento de Ameaças em Tempo Real

O CTD se baseia em avançados sistemas de aprendizagem artificial para detecção de anomalias e ameaças em todas as etapas dos incidentes propositalmente projetados para impactar os ICS. O sistema permite recursos de busca por ameaças e vulnerabilidades ao sistema, contextualizando os alertas gerados em histórias lineares para rápida interpretação. Isso permite investigação e resposta ágeis aos eventos, garantindo que as equipes do SOC tenham conhecimento situacional imediato e os detalhes compartilhados com as equipes de "chão de fábrica" para uma intervenção rápida.

Segmentação de rede OT virtual

Aproveitando do aprendizado de como seu sistema de automação industrial está configurado e se comunicando, usamos algoritmos inteligentes para agrupar ativos em segmentos lógicos e gerar um esquema ideal de "segmentação virtual". Munidos desse conhecimento sobre o comportamento, indicamos as políticas de segurança dos Firewalls (regras, portas, protocolo ou aplicativos) a serem implementadas ou como construir VLANs apropriadas para segmentar níveis mais baixos de redes OT, nas quais o bloqueio pode ser proibido.

Monitoramento Contínuo de Vulnerabilidades

O Claroty fornece insights profundos sobre o ambiente ICS, permitindo identificar e corrigir proativamente a configuração e outros problemas de higiene que podem deixar sua rede vulnerável a ataques. A Claroty monitora continuamente a infraestrutura de rede em busca por vulnerabilidades conhecidas, aproveitando a inteligência de segurança do Claroty Research, facilitando que as equipes de TI/OT tomem conhecimento dos riscos atuais do ICS. Um dos principais diferenciadores é a capacidade do sistema de fornecer uma correspondência precisa de CVE's dos ativos, atingindo até as versões precisas de firmware dos dispositivos industriais.

Usos e benefícios

Existem diversos casos de usos e benefícios associados à Plataforma Claroty para os mais diversos segmentos industriais. A ferramenta é aplicável a qualquer tipo de indústria colaborando inclusive com o atendimento a normas ou padrões demandados por cada setor. Dentre os diversos meios de utilização, destaque para:

- Detecção de anomalias de comunicação e ameaças em tempo real para atuação rápida para prevenção de incidentes;
- Gerenciamento de Ativos e Inventário automático do sistema, com criação de base de dados de riscos e vulnerabilidades além de score automático individual e sistêmico;
- Microsegmentação de redes de ICS, apoida no baseline comportamental de comnicação dos ativos e zonas periféricas;
- Controle e Detecção de Mudanças nos aplicativos de controle dos ativos aos sistemas ICS e
- Plataforma de Acesso Remoto Seguro integrada ao sistema de Detecção de Ameaças, garantindo acesso auditável e controlado de usuários externos (terceiros ou remotos) ao sistema de controle com recursos de autenticação, cofre de senhas, transferência de arquivos e gravação completa de sessões.

Secure Remote Access – Acesso Remoto Seguro

A Plataforma Claroty dispõe ainda do recurso de Secure Remote Access (ou SRA) como solução projetada para permitir o acesso aos Sistemas de Controle Industrial (ICS), seja através de redes internas ou remotas, garantindo a segurança do ambiente e da infraestrutura operacional durante todo o processo. Ele fornece visibilidade em tempo real dos ativos, tráfegos das redes e auditoria de todas as atividades dos usuários que os acessam remotamente com registros individuais por vídeo e controle total da sessão. Todos os registros e políticas de segurança implementados à solução SRA foram desenhados para atender aos requisitos de seguranças corporativos, operacionais e normativas das agências regulatórias.