WHITEPAPER

SIEM EM AMBIENTES OT: COLETA DE LOGS, CORRELAÇÃO E MONITORAMENTO DE SUBESTAÇÕES

Entenda SIEM em ambientes OT, fontes de logs, coletores, normalização, sincronismo, correlação, casos de uso, retenção e monitoramento de subestações.

A3A® Engenharia de Sistemas

SUMÁRIO

SIEM é uma plataforma que centraliza logs e eventos de segurança, normaliza informações, correlaciona sinais de diferentes fontes e gera alertas para investigação. Em ambientes OT, ele pode receber dados de firewalls, servidores SCADA, Active Directory, VPNs, jump servers, estações de engenharia, switches, EDR e outros componentes que sustentam a operação.

SIEM não é apenas um repositório de logs e não é sinônimo de SOC. O SIEM fornece tecnologia e dados; o SOC é a função organizacional que monitora, investiga e responde. Sem casos de uso, contexto de ativos, sincronismo e processo de resposta, a plataforma acumula eventos sem produzir detecção útil.

Em subestações, a coleta precisa respeitar disponibilidade e limitações dos ativos. IEDs e RTUs podem possuir poucos logs ou interfaces proprietárias. O projeto deve priorizar fontes capazes de registrar acesso, mudanças, comunicação, comandos e falhas sem introduzir carga ou risco ao processo.

1. O QUE É SIEM

SIEM significa *Security Information and Event Management*. A tecnologia combina gestão de informações de segurança com monitoramento de eventos.

A plataforma recebe registros, converte formatos, enriquece dados, executa regras, cria incidentes e mantém histórico para busca e auditoria.

Produtos modernos podem incluir analytics, machine learning, UEBA, SOAR e integração com inteligência de ameaças. Esses recursos não substituem fundamentos de coleta, qualidade e contexto.

2. SIEM, SOC E SOAR

SOC é a equipe e o processo de operação de segurança. SIEM é uma ferramenta central dessa operação.

SOAR automatiza orquestração e resposta. Ele pode abrir chamados, consultar fontes, bloquear indicadores ou executar playbooks.

Automação em OT precisa de cautela. Bloquear uma conta pode ser adequado; desligar uma porta ou isolar um servidor pode afetar operação. Ações automáticas devem ter avaliação de impacto e aprovação.

3. SIEM E SYSLOG

Syslog é um protocolo e formato de transporte de mensagens. SIEM recebe Syslog, mas também utiliza agentes, APIs, bancos, arquivos e coletores.

Um servidor Syslog pode armazenar mensagens sem normalização ou correlação. O SIEM adiciona pesquisa, regras, contexto e gestão de incidentes.

Syslog UDP pode perder mensagens e não fornece confirmação. TCP ou TLS podem melhorar transporte quando suportados.

4. PIPELINE DE COLETA

A coleta começa na fonte. O evento passa por agente, forwarder ou protocolo, chega a um coletor, é processado, normalizado, enriquecido e armazenado.

Cada etapa pode falhar. O SIEM precisa monitorar o próprio pipeline: última mensagem, volume esperado, erros de parsing, fila e atraso.

Uma fonte silenciosa pode representar ausência de eventos ou falha de coleta. O sistema precisa diferenciar.

5. AGENTES E FORWARDERS

Agentes instalados em Windows e Linux podem coletar logs locais, eventos, integridade e telemetria.

Forwarders encaminham dados para coletores centrais. Eles podem armazenar temporariamente durante perda de rede.

Em servidores SCADA, agentes precisam ser compatíveis e testados. Consumo de CPU, memória, disco e reinicialização devem ser avaliados.

6. COLETA SEM AGENTE

Syslog, Windows Event Forwarding, APIs, SNMP traps e consultas são alternativas.

Coleta sem agente reduz software no ativo, mas pode depender de credenciais e conectividade. Polling ativo em equipamentos sensíveis precisa de avaliação.

Firewalls e switches normalmente enviam Syslog. Aplicações podem exportar por API ou arquivo.

7. COLETORES EM ZONAS OT

Coletores locais reduzem conexões entre o SIEM corporativo e os ativos. Eles recebem logs dentro da zona e encaminham para cima.

A arquitetura deve seguir fluxos controlados, preferencialmente iniciados da zona OT para um coletor intermediário.

Uma DMZ entre TI e OT pode hospedar relay ou coletor. O SIEM não precisa consultar diretamente cada subestação.

8. NORMALIZAÇÃO E PARSING

Logs possuem formatos diferentes. Parsing extrai campos como usuário, origem, destino, ação, objeto e resultado.

Normalização converte campos para um esquema comum. Isso permite uma regra comparar VPN, Windows e PAM.

Parsers precisam ser versionados. Atualização de firmware pode mudar o formato e quebrar a extração sem interromper o recebimento bruto.

Eventos sem parsing devem ser monitorados. A ingestão não significa que o dado está utilizável.

9. ENRIQUECIMENTO

Enriquecimento adiciona contexto de inventário, criticidade, localização, proprietário, vulnerabilidade e identidade.

Um login em servidor crítico possui prioridade diferente de login em laboratório. Sem inventário, o SIEM trata ambos da mesma forma.

O contexto precisa ser atualizado. Ativos removidos e endereços reutilizados podem produzir atribuição incorreta.

10. SINCRONISMO DE TEMPO

Correlação depende de timestamps consistentes. O servidor NTP em redes e subestações é requisito básico.

O SIEM deve distinguir horário do evento, horário de recebimento e horário do coletor.

Fusos e horário de verão precisam ser normalizados. Uma diferença de minutos pode inverter a sequência entre acesso, comando e mudança.

11. FONTES DE LOG EM OT

Fontes incluem firewalls, switches, roteadores, VPN, PAM, jump servers, Active Directory, servidores, bancos, SCADA, historiadores, estações de engenharia e EDR.

RTUs e IEDs podem fornecer login, alteração, restart, falha e comunicação, mas o suporte varia. Logs não devem ser ativados em volume que comprometa o dispositivo.

Sensores de rede OT podem identificar protocolos, ativos e mudanças sem instalar agentes.

12. FIREWALLS E ROTEADORES

Logs de firewall mostram conexões permitidas, bloqueadas, tradução e sessões.

O volume pode ser elevado. O projeto precisa selecionar eventos e manter amostragem ou agregação quando apropriado.

Regras críticas, mudanças administrativas, novos destinos e acesso a portas industriais devem receber prioridade.

13. ACTIVE DIRECTORY E IDENTIDADE

Diretório fornece autenticação, grupos, criação de contas, bloqueios e mudanças de privilégio.

Casos de uso incluem login administrativo fora do padrão, adição a grupos críticos e criação de contas de serviço.

A identidade precisa ser correlacionada com VPN, PAM e endpoints.

14. PAM E JUMP SERVER

O PAM e jump server fornece solicitação, aprovação, sessão, destino e gravação.

O SIEM pode alertar acesso fora da janela, uso de break-glass e tentativa de caminho direto.

Logs do PAM devem ser enviados para fora da própria plataforma para preservar evidência diante de comprometimento.

15. MFA E VPN

VPN e MFA registram origem, usuário, método, dispositivo e resultado.

Múltiplas falhas, fator negado e acesso de localização inesperada são sinais relevantes.

O MFA em ambientes OT precisa ser integrado aos casos de uso de acesso remoto.

16. EDR E ENDPOINTS

EDR fornece processos, conexões, arquivos, usuários e detecções.

O SIEM correlaciona uma detecção no jump server com sessão PAM e conexão ao ativo.

O EDR e XDR em OT deve ser ajustado para compatibilidade e resposta segura.

17. SCADA E HISTORIADORES

Servidores SCADA podem registrar login, alteração de configuração, alarmes, comandos e falhas.

O formato varia. Casos de uso precisam distinguir operação legítima de mudança administrativa.

Comandos do processo exigem contexto de modo, usuário e janela. O SIEM não deve tentar interpretar cada evento de processo como ataque.

18. IEDS E RTUS

IEDs e RTUs possuem recursos limitados. A coleta pode utilizar Syslog, arquivos, protocolos de gestão ou integração com sistema de engenharia.

O IED e a RTU precisam ser monitorados sem aumentar carga.

Eventos prioritários incluem login, alteração, restart, falha de sincronismo, firmware e mudança de configuração.

19. SENSORES DE REDE OT

Sensores passivos analisam tráfego espelhado e identificam ativos, protocolos e anomalias.

Eles podem detectar novo mestre DNP3, cliente IEC 104, escrita Modbus ou mudança de comunicação.

A integração com SIEM combina visibilidade de rede e identidade. O sensor não deve ficar inline sem análise de disponibilidade.

SIEM útil começa pelos casos de uso, não pelo volume de logs.

Fontes, parsing, contexto, lógica, severidade e resposta precisam ser definidos para cada risco que a organização pretende detectar.

Conhecer a solução de SIEM

20. CASOS DE USO

Um caso de uso define ameaça, fontes, lógica, contexto, severidade e resposta.

Exemplos incluem acesso remoto fora de janela, novo cliente em porta industrial, alteração de regra de firewall, conta adicionada a grupo privilegiado e jump server sem EDR.

Regras genéricas importadas precisam ser adaptadas ao ambiente.

21. CORRELAÇÃO

Correlação combina eventos no tempo e por entidade. Uma falha de MFA seguida de sucesso, sessão PAM e alteração no SCADA forma uma narrativa mais útil que alertas separados.

A janela de correlação depende de latência e sincronismo. Eventos podem chegar atrasados de sites remotos.

O sistema precisa preservar o evento bruto para investigação.

22. DETECÇÃO BASEADA EM ASSINATURA

Assinaturas identificam padrões conhecidos, como hash, endereço ou sequência.

São úteis, mas possuem vida curta e podem gerar falsos positivos.

Inteligência de ameaças deve ser contextualizada. Bloquear automaticamente um endereço associado a serviço legítimo pode causar impacto.

23. DETECÇÃO COMPORTAMENTAL

Analytics identifica desvios de usuário, ativo ou tráfego.

Em OT, comportamento é frequentemente estável, o que ajuda a detectar novidade. Porém, manutenção e contingências legítimas também geram desvios.

Modelos precisam de período de aprendizagem, tags de manutenção e revisão humana.

24. UEBA

User and Entity Behavior Analytics relaciona usuários, dispositivos e ações.

Ele pode detectar administrador acessando ativos incomuns ou conta de serviço usada interativamente.

Dados de identidade e inventário precisam estar corretos. Conta compartilhada reduz eficácia.

25. SEVERIDADE E RISCO

Severidade técnica não é igual a risco operacional. Um malware bloqueado no notebook administrativo pode ser menos crítico que alteração silenciosa no servidor SCADA.

O cálculo deve considerar criticidade do ativo, privilégio, exposição e fase do incidente.

Alertas precisam ser priorizados para a equipe disponível.

26. FALSOS POSITIVOS

Falso positivo consome tempo e reduz confiança. A regra precisa de tuning com exclusões justificadas.

Excluir toda uma fonte ou usuário para reduzir ruído pode ocultar incidentes. As exceções devem ser específicas e revisadas.

Métricas incluem taxa de fechamento, tempo de investigação e recorrência.

27. PLAYBOOKS DE INVESTIGAÇÃO

Playbooks orientam coleta de evidências e decisão.

Um alerta de acesso remoto pode exigir verificar chamado, aprovação PAM, origem, MFA, comandos e mudanças.

O playbook deve indicar quando envolver operação, engenharia e resposta a incidentes.

Detecção sem resposta definida apenas transfere o problema.

Playbooks, responsáveis, escalonamento, preservação de evidências e limites para ações automáticas precisam considerar o impacto operacional.

Conhecer o serviço de Integração de Sistemas

28. RESPOSTA EM OT

A resposta precisa considerar segurança física e continuidade. Isolamento automático pode interromper processo.

Ações incluem bloquear conta, revogar sessão, limitar acesso, coletar evidência e ativar contingência.

O responsável operacional deve participar de decisões que alteram ativos críticos.

29. RETENÇÃO DE LOGS

Retenção depende de risco, investigação, contrato e capacidade.

Dados quentes ficam disponíveis para busca rápida; dados frios podem ser arquivados.

A política deve indicar fonte, período, integridade e descarte. Guardar tudo indefinidamente aumenta custo sem necessariamente aumentar valor.

30. DIMENSIONAMENTO POR EPS

EPS representa eventos por segundo. O dimensionamento considera média, pico, crescimento, parsing e retenção.

Um incidente ou atualização pode multiplicar o volume. Margem precisa existir.

Métricas de bytes por evento e compressão complementam EPS.

31. ARMAZENAMENTO

O cálculo considera ingestão diária, índices, réplicas, retenção e backup.

Logs de firewall e EDR podem dominar o volume. Filtragem deve ocorrer sem remover eventos essenciais.

A capacidade precisa ser monitorada. Disco cheio pode interromper ingestão ou busca.

32. ALTA DISPONIBILIDADE

Coletores, processamento, banco e interface podem exigir redundância.

A perda do SIEM não deve afetar o processo, mas não pode causar perda permanente de evidência. Forwarders armazenam filas locais.

Failover e restauração precisam ser testados.

33. SEGURANÇA DO SIEM

O SIEM concentra dados sensíveis e credenciais de integração. Ele é alvo de alto valor.

Acesso administrativo precisa de MFA, PAM, segmentação e logs. Contas de serviço seguem menor privilégio.

O hardening aplica-se a servidores, coletores e bancos.

34. ARQUITETURA DE REDE

Coletores OT enviam dados a uma DMZ ou plataforma central por fluxos definidos.

O SIEM não deve abrir conexões administrativas aos ativos apenas para coletar logs se existe alternativa segura.

Firewall, DNS, NTP e certificados fazem parte da matriz de comunicação.

35. DASHBOARDS

Dashboards devem responder perguntas operacionais: fontes sem dados, alertas críticos, acesso remoto, mudanças e cobertura.

Painéis com grande quantidade de gráficos não substituem casos de uso.

Cada indicador precisa de responsável e ação esperada.

36. COBERTURA E LACUNAS

Cobertura relaciona ativos críticos às fontes e casos de uso.

Uma tabela pode indicar se cada servidor possui logs de sistema, autenticação, aplicação e EDR.

Lacunas devem gerar plano de integração ou controle compensatório.

37. PROJETO E DOCUMENTAÇÃO

O projeto deve incluir arquitetura, fontes, protocolos, parsers, retenção, casos de uso, severidade, playbooks e responsabilidades.

Também precisa dimensionar EPS, armazenamento, alta disponibilidade e licenças.

A lista de fontes registra proprietário, formato, última mensagem e criticidade.

38. IMPLANTAÇÃO POR ETAPAS

A implantação começa por identidade, firewall, PAM, endpoints e servidores críticos.

Depois incorpora aplicações, sensores e fontes especializadas. Cada lote precisa de casos de uso e tuning.

Conectar todas as fontes antes de definir prioridades gera volume e atraso.

39. COMISSIONAMENTO E ACEITE

O aceite deve validar pipeline, parsing, correlação, retenção e resposta.

O roteiro mínimo inclui:

O Comissionamento e Aceite Técnico deve comprovar detecção e não apenas ingestão.

O aceite deve provar coleta, detecção e investigação.

Fontes, filas, parsing, regras, contexto, retenção, failover e acesso administrativo precisam ser testados com eventos positivos e negativos.

Conhecer o serviço de Comissionamento e Aceite Técnico

40. DIAGNÓSTICO DE FALHAS

Fonte sem eventos exige verificar geração, agente, rede, certificado e coletor. Eventos sem campos indicam parser.

Alerta que não dispara pode ter condição, janela, normalização ou contexto incorreto. Atraso pode decorrer de fila ou processamento.

Busca lenta aponta dimensionamento, índice ou armazenamento.

41. ERROS COMUNS

Erros frequentes incluem comprar SIEM antes de definir casos de uso, coletar tudo sem contexto e ignorar fontes silenciosas.

Também são comuns regras corporativas aplicadas a OT sem adaptação, relógios divergentes, retenção subdimensionada e resposta automática perigosa.

Outro erro é medir sucesso por volume ingerido. O objetivo é detectar, investigar e responder.

42. CONCLUSÃO

SIEM centraliza e correlaciona eventos para apoiar segurança. Em OT, ele integra identidade, acesso remoto, endpoints, rede e aplicações sem interferir no processo.

O valor depende de fontes confiáveis, parsing, contexto, casos de uso, playbooks e operação. Quando a arquitetura monitora seu próprio pipeline e respeita a criticidade dos ativos, o SIEM melhora visibilidade e resposta em subestações e centros de operação.

[1] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. NIST SP 800-92 — Guide to Computer Security Log Management.

[2] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. NIST SP 800-61 Rev. 2 — Computer Security Incident Handling Guide.

[3] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. NIST SP 800-82 Rev. 3 — Guide to Operational Technology Security. Gaithersburg, 2023.

[4] CISA. Cybersecurity Performance Goals — Logging and monitoring guidance.

[5] MITRE. ATT&CK for ICS — Knowledge base of adversary tactics and techniques.

[6] INTERNATIONAL ELECTROTECHNICAL COMMISSION. IEC 62443 series — Security for industrial automation and control systems.

O que é SIEM? SIEM é uma plataforma que centraliza logs, normaliza eventos, correlaciona sinais e gera alertas para investigação.**SIEM e SOC são a mesma coisa?** Não.

SIEM é tecnologia; SOC é a função organizacional de monitoramento e resposta.**Qual é a diferença entre SIEM e Syslog?** Syslog transporta mensagens. SIEM adiciona parsing, correlação, busca, contexto e gestão de incidentes.**Quais fontes devem entrar primeiro?** Identidade, firewall, VPN, PAM, endpoints, servidores críticos e aplicações de maior risco.**O que é EPS?** Eventos por segundo é uma métrica usada para dimensionar ingestão e licenciamento.**SIEM pode coletar logs de IEDs?** Depende do equipamento. A coleta deve respeitar recursos e pode utilizar Syslog, arquivos ou integrações específicas.**Como evitar falsos positivos?** Com tuning, contexto de ativos, exceções específicas, manutenção registrada e revisão contínua.**SIEM pode responder automaticamente em OT?** Algumas ações podem ser automatizadas, mas qualquer ação com impacto operacional precisa de análise de risco e aprovação.**Quanto tempo reter logs?** Depende de risco, investigação, contrato e capacidade. A política deve definir períodos por fonte.**Como testar um SIEM?** Devem ser testados coleta, fila, parsing, regras, contexto, investigação, retenção, failover e segurança da própria plataforma.

Soluções relacionadas

Serviços relacionados

Artigos e materiais técnicos relacionados

Sobre a A3A Engenharia de Sistemas

Com 30 anos de história, a A3A Engenharia de Sistemas se consolidou como referência em serviços de Engenharia, oferecendo soluções integradas de Telecomunicações, Segurança Eletrônica, Segurança Digital e Instalações Elétricas.

A empresa atua em todas as etapas do ciclo de Engenharia, desde a elaboração de projetos e consultoria técnica até a implantação, manutenção e retrofit de sistemas, sempre em conformidade com as normas técnicas e melhores práticas do setor.

A3A® Engenharia de Sistemas