WHITEPAPER

EDR E XDR EM AMBIENTES OT: PROTEÇÃO DE SERVIDORES SCADA E ESTAÇÕES DE ENGENHARIA

Entenda EDR e XDR, diferenças para antivírus, aplicação em SCADA e estações de engenharia, homologação, isolamento, SIEM e segurança OT.

A3A® Engenharia de Sistemas

SUMÁRIO

EDR é uma tecnologia de proteção, detecção, investigação e resposta instalada em endpoints e servidores. Ela coleta telemetria de processos, arquivos, usuários, conexões e comportamentos para identificar atividades maliciosas. **XDR** amplia a correlação para múltiplas camadas, como identidade, e-mail, rede, nuvem e endpoints.

Em ambientes OT, EDR pode proteger servidores SCADA, historiadores, jump servers, estações de engenharia e outros sistemas baseados em Windows ou Linux. Ele normalmente não é instalado em IEDs, RTUs e dispositivos embarcados proprietários.

A implantação precisa equilibrar detecção e disponibilidade. Agentes, atualizações, isolamento, quarentena e exclusões devem ser testados com aplicações industriais. Uma política corporativa aplicada sem validação pode interferir em serviços críticos.

1. O QUE É EDR

EDR significa *Endpoint Detection and Response*. A solução mantém visibilidade contínua sobre atividades do endpoint e permite investigar e responder.

Ela registra relações entre processos, arquivos, conexões, usuários e persistência. Esse contexto ajuda a compreender uma cadeia de ataque.

EDR pode bloquear comportamentos, matar processos, colocar arquivos em quarentena e isolar o host. Essas ações precisam de política adequada ao ambiente.

2. EDR E ANTIVÍRUS

Antivírus tradicional foca assinaturas e análise de arquivos. EDR adiciona telemetria, comportamento, busca e resposta.

Muitos produtos atuais combinam prevenção e EDR no mesmo agente. O nome comercial não garante o mesmo conjunto de recursos.

A avaliação deve considerar detecção, investigação, resposta, operação offline, suporte e impacto.

3. O QUE É XDR

XDR significa *Extended Detection and Response*. A tecnologia correlaciona sinais de várias fontes.

Uma detecção no endpoint pode ser relacionada a login, e-mail, identidade e tráfego de rede.

A abrangência depende do ecossistema e das integrações. XDR não substitui automaticamente SIEM; as duas tecnologias podem coexistir.

4. EDR, XDR E SIEM

EDR produz telemetria detalhada de endpoints. XDR correlaciona fontes integradas. SIEM centraliza logs e casos de uso mais amplos.

O SIEM pode receber alertas e eventos do EDR, combinando com PAM, firewall e SCADA.

Evitar duplicidade exige definir qual plataforma cria incidente, retém dados e executa resposta.

5. ARQUITETURA DO AGENTE

O agente roda no endpoint e observa eventos do sistema. Ele envia telemetria para um servidor ou serviço em nuvem.

Parte da prevenção pode funcionar localmente. Investigação e correlação podem depender de conectividade com a plataforma.

O projeto deve conhecer filas offline, consumo, portas, certificados e frequência de atualização.

6. CONSOLE E GERENCIAMENTO

O console define políticas, grupos, exclusões, alertas e ações.

Acesso administrativo precisa de MFA, PAM e menor privilégio. O console possui capacidade de resposta sobre muitos ativos e é alvo crítico.

Mudanças de política e ações remotas devem ser registradas e enviadas ao SIEM.

7. TELEMETRIA DE PROCESSOS

O EDR registra criação de processos, linha de comando, processo pai, usuário e assinatura.

Isso permite identificar scripts, ferramentas administrativas e execução incomum.

Aplicações SCADA podem gerar processos próprios e scripts legítimos. O tuning precisa diferenciá-los sem criar exclusões amplas.

8. ARQUIVOS E PERSISTÊNCIA

A solução monitora criação, alteração e execução de arquivos, além de mecanismos de inicialização.

Projetos de engenharia e bancos podem possuir arquivos grandes e frequência elevada. Análise intensiva pode impactar desempenho.

Exclusões devem ser específicas por caminho, processo e tipo, conforme suporte do produto.

9. CONEXÕES DE REDE

EDR relaciona processos a conexões, destinos e portas.

Uma estação de engenharia conectando a novos endereços ou uma aplicação iniciando conexão externa pode gerar alerta.

A telemetria complementa sensores de rede, mas não substitui visibilidade de protocolos industriais.

10. IDENTIDADE E USUÁRIOS

Logins, elevação e execução por usuário ajudam a correlacionar acesso privilegiado.

Integração com PAM e Active Directory melhora atribuição.

Contas compartilhadas reduzem capacidade de investigação.

EDR em OT precisa de homologação, não apenas instalação.

Compatibilidade, consumo, serviços, exclusões, atualização, operação offline e ações de resposta devem ser avaliados por classe de ativo.

Conhecer a solução de EDR/XDR

11. EDR EM SERVIDORES SCADA

Servidores SCADA possuem serviços, drivers, bancos e interfaces críticas.

O agente deve ser homologado ou testado com fabricante e versão. Reinicializações, atualizações e inspeção de arquivos podem afetar operação.

A política deve evitar bloqueio automático de componentes legítimos sem validação.

O SCADA no setor elétrico precisa permanecer disponível durante falhas do console ou da internet.

12. EDR EM HISTORIADORES

Historiadores realizam gravação intensiva e consultas. Diretórios de dados podem exigir exclusões específicas.

Excluir todo o servidor reduz proteção. O ideal é limitar caminhos de banco e manter monitoramento de processos, scripts e sistema.

Consumo de disco e latência precisam ser medidos antes e depois.

13. EDR EM ESTAÇÕES DE ENGENHARIA

Estações de engenharia executam ferramentas com alto privilégio e manipulam projetos, firmware e configurações.

Elas são alvos importantes e costumam permitir mídias e arquivos externos. EDR, controle de aplicação e PAM são relevantes.

A solução deve reconhecer compiladores, scripts e ferramentas legítimas sem liberar qualquer execução.

14. EDR EM JUMP SERVERS

Jump servers concentram acesso remoto e são prioridade de proteção.

O EDR pode identificar download, execução, persistência e conexão incomum durante sessões.

A integração com logs do PAM ajuda a atribuir atividade ao usuário remoto.

15. EDR EM CONTROLADORES DE DOMÍNIO

Controladores de domínio são críticos e exigem políticas específicas. O agente precisa ser suportado e o impacto testado.

Detecções de credenciais, grupos e replicação possuem grande valor.

Resposta automática que reinicia ou isola o controlador precisa de controle.

16. SISTEMAS LEGADOS

Sistemas operacionais sem suporte podem não aceitar agentes atuais.

Instalar uma versão antiga de agente pode não oferecer proteção suficiente e criar dependências.

Controles compensatórios incluem segmentação, allowlisting, virtual patching, jump server e monitoramento de rede.

A decisão deve ser documentada e acompanhada por plano de atualização.

17. IEDS E RTUS

IEDs e RTUs normalmente utilizam firmware proprietário e não suportam EDR.

A proteção ocorre por hardening, segmentação, firmware, controle de acesso e monitoramento passivo.

Não se deve instalar agente não suportado em dispositivo embarcado.

18. MODOS DE PREVENÇÃO

Produtos podem oferecer modo auditoria, detect only e bloqueio.

A implantação em OT deve começar com observação para identificar compatibilidade. Depois, controles são ativados por grupo.

Manter indefinidamente em modo somente detecção reduz benefício. A evolução precisa de critérios e responsáveis.

19. DETECÇÃO COMPORTAMENTAL

Detecções analisam relações e sequências, como script iniciando ferramenta de rede e criando persistência.

Comportamento legítimo de engenharia pode parecer suspeito. O contexto de janela, usuário e ferramenta ajuda no tuning.

As regras devem ser testadas com atividades reais e simulações controladas.

20. ASSINATURAS E INTELIGÊNCIA

Assinaturas identificam arquivos e indicadores conhecidos.

Atualizações precisam chegar aos endpoints isolados. A arquitetura pode utilizar relay interno.

Indicadores possuem validade. Bloqueios devem ser revisados para evitar impacto em serviços legítimos.

21. MACHINE LEARNING

Modelos classificam arquivos e comportamento. Eles podem detectar ameaças desconhecidas, mas também gerar falsos positivos.

A organização precisa entender telemetria enviada, dependência de nuvem e opções offline.

Decisões automáticas em servidores críticos exigem avaliação.

22. THREAT HUNTING

Threat hunting busca sinais sem aguardar alerta.

Consultas podem procurar ferramentas, conexões, persistência e comportamento de contas.

O hunting em OT deve usar conhecimento da arquitetura e das janelas de manutenção.

23. ISOLAMENTO DE HOST

Isolamento bloqueia a maioria das conexões do endpoint, mantendo comunicação com a plataforma.

Em estação de usuário, pode ser apropriado. Em servidor SCADA, pode interromper operação e comunicação com dispositivos.

A política precisa indicar quais grupos permitem isolamento automático e quais exigem aprovação operacional.

24. QUARENTENA E REMOÇÃO

Quarentena impede uso de arquivo. Se o arquivo pertencer à aplicação, pode causar falha.

A solução deve permitir restauração controlada e preservação para análise.

Exclusões posteriores precisam ser específicas, não uma liberação ampla do diretório.

25. ENCERRAMENTO DE PROCESSO

Matar um processo malicioso é resposta comum. Em OT, encerrar serviço de automação pode ter impacto.

Playbooks devem diferenciar processos do sistema, aplicação e usuário.

A resposta pode priorizar bloquear conta ou acesso antes de atuar no servidor.

26. ROLLBACK E REMEDIAÇÃO

Alguns produtos oferecem rollback de alterações. O recurso depende do sistema de arquivos e tipo de ataque.

Não substitui backup. Em bancos e historiadores, rollback genérico pode ser inadequado.

O procedimento de recuperação deve seguir o plano da aplicação.

27. APPLICATION CONTROL

Allowlisting permite executar apenas software aprovado. Pode complementar EDR em sistemas estáveis.

A implantação exige inventário e processo para atualizações. Regras rígidas sem planejamento bloqueiam ferramentas legítimas.

Scripts, bibliotecas e instaladores precisam de tratamento.

28. EXCLUSÕES

Exclusões são necessárias em alguns casos, mas reduzem visibilidade.

Devem possuir justificativa, proprietário, escopo e revisão. Preferir exclusão de arquivo ou processo específico a pastas inteiras.

Uma exclusão recomendada por fabricante precisa ser validada para a versão real.

29. DESEMPENHO

O teste mede CPU, memória, disco, latência e tempo de inicialização.

Cargas normais e picos devem ser considerados. Varredura completa não deve ocorrer durante período crítico sem planejamento.

Métricas antes e depois ajudam a demonstrar compatibilidade.

30. ATUALIZAÇÕES DE AGENTE

Atualizações podem introduzir drivers e comportamento novo.

Anéis de implantação permitem testar em laboratório, piloto e produção.

Servidores críticos não devem receber atualização automática sem janela e retorno.

O console precisa mostrar versões divergentes e falhas.

31. ATUALIZAÇÕES DE CONTEÚDO

Assinaturas e modelos são atualizados com frequência. A política pode permitir conteúdo automático mantendo agente controlado.

Ambientes isolados precisam de relay ou pacote offline.

A falha de atualização deve gerar alerta.

32. OPERAÇÃO OFFLINE

O agente deve manter prevenção e buffer sem conexão com o console.

A capacidade e duração precisam ser conhecidas. Após retorno, eventos devem ser enviados sem sobrecarregar enlace.

A perda da nuvem não pode desabilitar proteção local.

33. DEPENDÊNCIA DE NUVEM

Soluções SaaS exigem conexão a endpoints do fornecedor. A DMZ entre TI e OT pode intermediar tráfego.

Permitir domínios amplos precisa ser evitado quando existem listas documentadas.

Privacidade, soberania e retenção devem ser avaliadas.

34. ARQUITETURA ON-PREMISES

Soluções locais reduzem dependência externa, mas exigem servidores, banco, backup e atualização.

A alta disponibilidade e capacidade de ingestão precisam ser dimensionadas.

O console local também é um ativo crítico.

35. INTEGRAÇÃO COM SIEM

Alertas, incidentes e telemetria selecionada podem ser enviados ao SIEM.

O SIEM correlaciona com VPN, PAM, identidade e firewall.

Enviar toda a telemetria bruta pode aumentar custo. O projeto define nível de detalhe e retenção em cada plataforma.

36. INTEGRAÇÃO COM XDR

XDR correlaciona endpoint com outras camadas do mesmo ecossistema ou integrações.

A investigação pode mostrar e-mail, login, processo e conexão em uma linha temporal.

O modelo precisa respeitar limites de dados e dependências do fornecedor.

Responder no endpoint exige conhecer o impacto no processo.

Isolamento, quarentena, encerramento de processos e automações devem seguir playbooks específicos para estações, jump servers e servidores críticos.

Conhecer o serviço de Integração de Sistemas

37. RESPOSTA COORDENADA

Um incidente no endpoint pode exigir revogar sessão PAM, bloquear usuário e limitar rede.

A automação deve considerar impacto. Em OT, resposta aprovada por operação é frequentemente necessária.

Playbooks precisam definir evidências antes de reiniciar ou isolar sistemas.

38. RANSOMWARE EM OT

Ransomware pode atingir servidores e estações, afetando supervisão e engenharia.

EDR ajuda a detectar comportamento, mas backup, segmentação e recuperação são indispensáveis.

O hardening em ambientes OT reduz superfície.

Backups precisam ser offline ou protegidos e testados.

39. ADMINISTRAÇÃO DO EDR

Administradores possuem capacidade de executar ações nos endpoints. O acesso deve usar MFA e PAM.

Funções de analista, operador e administrador precisam ser separadas.

Ações e mudanças de política são registradas e enviadas ao SIEM.

40. INVENTÁRIO E COBERTURA

A plataforma deve indicar endpoints protegidos, sem agente, offline, desatualizados e não suportados.

Cobertura é comparada ao inventário oficial. Ativos descobertos sem proteção geram tratamento.

Servidores críticos precisam de responsável e política definida.

41. PROJETO E DOCUMENTAÇÃO

O projeto deve incluir escopo, arquitetura, sistemas suportados, políticas, exclusões, atualização, rede, retenção e resposta.

Matriz por ativo registra modo, versão, ações permitidas e dependências.

Exceções possuem prazo e controle compensatório.

42. PILOTO E HOMOLOGAÇÃO

O piloto utiliza sistemas representativos e tarefas reais.

Testes incluem operação normal, backup, atualização, failover, manutenção e carga.

Fabricante da aplicação deve ser consultado quando necessário, mas a compatibilidade precisa ser comprovada no ambiente.

43. IMPLANTAÇÃO POR ONDAS

A expansão pode começar por jump servers, notebooks e estações, depois servidores menos críticos e finalmente sistemas de maior impacto.

Cada onda monitora falsos positivos e desempenho.

Planos de rollback e suporte precisam estar disponíveis.

44. COMISSIONAMENTO E ACEITE

O aceite deve validar prevenção, detecção, operação offline, atualização e resposta.

O roteiro mínimo inclui:

O Comissionamento e Aceite Técnico deve comprovar compatibilidade e resposta segura.

O aceite precisa provar prevenção, detecção e operação offline.

Políticas, desempenho, evento de teste, isolamento controlado, atualização, perda do console, integração com SIEM e retorno precisam ser verificados.

Conhecer o serviço de Comissionamento e Aceite Técnico

45. DIAGNÓSTICO DE FALHAS

Agente offline pode indicar serviço, certificado, firewall ou proxy. Alto consumo exige analisar varredura, exclusões e conflito.

Falso positivo recorrente precisa de evidência e ajuste específico. Alerta sem telemetria pode indicar retenção ou licença.

Isolamento que não funciona exige verificar suporte, rede e política.

46. ERROS COMUNS

Erros frequentes incluem aplicar política corporativa a servidores SCADA sem piloto, criar exclusões amplas e permitir isolamento automático em todos os ativos.

Também são comuns atualizações sem anel, console sem MFA, dependência de nuvem não documentada e sistemas legados ignorados.

Outro erro é considerar agente instalado como proteção concluída. Cobertura, alertas, resposta e operação precisam ser testados.

47. CONCLUSÃO

EDR fornece visibilidade e resposta nos endpoints; XDR amplia correlação entre camadas. Em OT, essas tecnologias protegem principalmente servidores e estações com sistemas operacionais convencionais.

O valor depende de homologação, políticas por criticidade, operação offline, tuning, integração e playbooks. Quando ações de resposta respeitam o impacto operacional, EDR e XDR fortalecem a segurança sem transformar o agente em risco de indisponibilidade.

[1] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. NIST SP 800-83 Rev. 1 — Guide to Malware Incident Prevention and Handling for Desktops and Laptops.

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

[3] CISA. Cybersecurity Performance Goals — Endpoint security and application control guidance.

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

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

O que é EDR? EDR é uma tecnologia de detecção, investigação e resposta baseada em telemetria de endpoints e servidores.**Qual é a diferença entre EDR e antivírus?** Antivírus foca prevenção e assinaturas. EDR adiciona comportamento, investigação, busca e resposta.**O que é XDR?** XDR correlaciona sinais de endpoints, identidade, rede, e-mail e outras camadas.**EDR pode ser instalado em SCADA?** Pode ser instalado em servidores e estações compatíveis, após homologação e testes de desempenho.**EDR pode ser instalado em IEDs?** Normalmente não. IEDs e RTUs embarcados usam controles de rede, hardening e firmware.**O que é isolamento de host?** É uma ação que bloqueia conexões do endpoint. Em servidores OT, precisa de aprovação devido ao impacto.**Como tratar exclusões?** Devem ser específicas, justificadas, documentadas e revisadas, evitando liberar pastas amplas.**EDR funciona offline?** Depende da solução. A prevenção local e o buffer offline precisam ser confirmados e testados.**EDR substitui backup?** Não. Backup e

recuperação continuam essenciais, especialmente contra ransomware.**Como testar EDR em OT?** Devem ser testados desempenho, detecção, política, offline, atualização, isolamento controlado, SIEM e rollback.

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