WHITEPAPER

CISCO CYBER VISION: VISIBILIDADE DE ATIVOS, RISCOS E SEGURANÇA EM REDES OT

Entenda Cisco Cyber Vision: sensores, inventário de ativos, protocolos, vulnerabilidades, anomalias, integração com ISE, SIEM e switches industriais.

A3A® Engenharia de Sistemas

SUMÁRIO

Cisco Cyber Vision é uma plataforma de visibilidade e segurança para redes industriais e ambientes OT. Ela identifica ativos, protocolos e comunicações, organiza inventário, contextualiza vulnerabilidades e ajuda a detectar mudanças ou comportamentos anômalos sem depender de agentes instalados em cada equipamento.

A plataforma utiliza sensores que observam o tráfego industrial e enviam metadados para um componente central. Esses sensores podem ser integrados a determinados switches industriais Cisco ou implantados em appliances dedicados, conforme a arquitetura. O objetivo é aproximar a coleta do processo sem exigir que todo o tráfego seja enviado continuamente a um ponto remoto.

Cyber Vision não substitui firewall, SIEM, EDR, ISE ou gestão de vulnerabilidades. Ele fornece contexto específico de OT — ativos, firmware, protocolos, células, fluxos e riscos — que pode ser utilizado por essas plataformas e pelas equipes de engenharia, operação e segurança.

1. O QUE É CISCO CYBER VISION

Cisco Cyber Vision é uma solução de visibilidade de ativos e detecção para sistemas industriais. Ela analisa protocolos e padrões de comunicação para construir um inventário dinâmico da rede.

Em ambientes OT, inventários tradicionais são frequentemente incompletos. Equipamentos permanecem em operação por muitos anos, utilizam protocolos proprietários e não aceitam agentes. A observação passiva permite descobrir dispositivos sem instalar software neles.

A solução pode ser aplicada em manufatura, energia, saneamento, mineração, logística, óleo e gás e outras infraestruturas críticas.

2. COMO FUNCIONA

Sensores recebem cópias ou observam tráfego de rede. Eles processam pacotes, identificam protocolos e extraem metadados relevantes. O componente central consolida informações, apresenta topologias, grupos, riscos e eventos.

O processamento distribuído reduz a necessidade de transportar todos os pacotes até um data center. Dependendo da implantação, apenas metadados e eventos são enviados ao centro.

A arquitetura precisa definir onde os sensores observam o tráfego. Um sensor instalado em um ponto sem visibilidade das comunicações não pode inventariar os ativos ocultos atrás de outro segmento.

3. SENSORES INTEGRADOS E DEDICADOS

Determinados switches industriais Cisco podem executar funções de sensor ou apoiar a coleta. Essa integração aproxima visibilidade do acesso e reduz a necessidade de hardware adicional.

Appliances ou sensores dedicados continuam necessários em redes com equipamentos de outros fabricantes, áreas não atendidas por switches compatíveis ou requisitos específicos de desempenho.

A escolha deve considerar cobertura, capacidade, licenças, versões, topologia e manutenção. Uma arquitetura híbrida pode combinar sensores integrados e dedicados.

O artigo sobre switch industrial Cisco apresenta os critérios de seleção e integração.

4. COLETA PASSIVA E ATIVA

A coleta passiva observa o tráfego existente e possui menor risco de impacto. Ela identifica dispositivos que se comunicam, mas pode não descobrir ativos silenciosos.

Métodos ativos enviam consultas ou utilizam integrações para obter informações adicionais. Em OT, qualquer coleta ativa precisa ser avaliada, porque equipamentos legados podem reagir de forma inesperada.

O projeto deve definir quais técnicas são permitidas por classe de ativo. A visibilidade não pode comprometer disponibilidade.

5. DESCOBERTA E INVENTÁRIO DE ATIVOS

A plataforma tenta identificar fabricante, família, modelo, endereço, função, protocolo, firmware e relações. A precisão depende do tráfego disponível e do suporte ao protocolo.

O inventário deve ser revisado por engenharia. Uma classificação automática não substitui a validação do responsável pelo processo.

Tags, grupos e zonas ajudam a organizar ativos por site, célula, linha, bay, criticidade e responsável. Essa taxonomia precisa ser padronizada.

6. PROTOCOLOS INDUSTRIAIS

Cyber Vision interpreta protocolos industriais para compreender contexto. Isso permite diferenciar uma simples conexão TCP de uma operação de leitura ou escrita em um protocolo específico.

A cobertura pode incluir protocolos como Modbus, EtherNet/IP, PROFINET, S7, OPC UA, BACnet, DNP3 e IEC 60870-5-104, conforme versão e licença.

O suporte deve ser confirmado para os protocolos reais do ambiente. Protocolos proprietários podem aparecer apenas como comunicação genérica.

7. MAPA DE COMUNICAÇÕES

O mapa mostra quem se comunica com quem, por quais protocolos e com que frequência. Essa visualização ajuda a identificar dependências e fluxos inesperados.

Uma linha de produção pode possuir comunicação legítima entre CLP, IHM, estação de engenharia e servidor. Um acesso direto da rede corporativa ao CLP pode indicar arquitetura inadequada.

O mapa deve ser comparado com o projeto de redes industriais e com a matriz de fluxos aprovada.

8. GRUPOS, CÉLULAS E ZONAS

Ativos podem ser agrupados por célula, área ou função. Esses grupos ajudam a representar a arquitetura Purdue ou outras zonas definidas pelo projeto.

A visualização lógica facilita identificar comunicações que cruzam limites. Entretanto, criar grupos na ferramenta não cria segmentação física ou regras de firewall.

A taxonomia deve refletir o processo e ser mantida quando ativos mudam.

Visibilidade OT precisa ser construída a partir da cobertura real da rede.

Sensores, pontos de espelhamento, protocolos, células, ativos silenciosos e limites de coleta devem ser definidos antes de avaliar risco e anomalias.

Conhecer a solução de Redes Cisco

9. CONTEXTO DE VULNERABILIDADES

A plataforma pode associar informações de produto e versão a vulnerabilidades conhecidas. Isso ajuda a priorizar riscos.

A presença de uma CVE não significa automaticamente que o ativo está explorável. É necessário avaliar versão, configuração, exposição, compensações e criticidade.

Em OT, correções podem exigir parada e homologação. O contexto de comunicação e posição na rede ajuda a escolher mitigação, segmentação ou janela de atualização.

10. PONTUAÇÃO E PRIORIZAÇÃO DE RISCO

Risco combina vulnerabilidade, exposição, criticidade e comportamento. Uma pontuação deve apoiar decisão, não substituí-la.

Ativos críticos com vulnerabilidade moderada e acesso amplo podem exigir prioridade maior que equipamentos isolados com CVE de alta severidade.

A organização precisa definir critérios de aceitação, responsável e prazo. Sem processo, o painel acumula alertas sem tratamento.

11. DETECÇÃO DE MUDANÇAS

Cyber Vision pode identificar novos ativos, novos fluxos, mudanças de protocolo e comportamentos fora da linha de base.

Nem toda mudança é incidente. Manutenção, atualização ou expansão podem gerar eventos legítimos. A integração com gestão de mudanças reduz falso positivo.

Eventos precisam de contexto: ativo, horário, origem, ação e impacto potencial.

12. ANOMALIAS E DETECÇÃO

A detecção observa desvios ou padrões conhecidos. Exemplos incluem varredura, comunicação nova, alteração de firmware, mudança de programação e acesso remoto incomum.

A qualidade depende da linha de base e da visibilidade. Períodos de comissionamento e produção têm comportamentos diferentes.

A plataforma não deve ser configurada para alertar sobre qualquer variação. Regras e thresholds precisam ser ajustados ao processo.

13. INTEGRAÇÃO COM CISCO ISE

Cyber Vision pode fornecer contexto de ativos ao Cisco ISE e apoiar políticas de acesso e segmentação.

O Cisco ISE toma decisões de autenticação e autorização. Cyber Vision ajuda a identificar o tipo e o risco do dispositivo.

A política pode restringir um endpoint desconhecido ou aplicar acesso específico a uma classe. Em OT, bloqueios automáticos devem ser avaliados com cuidado.

14. INTEGRAÇÃO COM FIREWALLS E SEGMENTAÇÃO

O inventário e os fluxos observados ajudam a desenhar regras de firewall e microsegmentação. A ferramenta mostra comunicações reais que podem ser comparadas com o fluxo esperado.

Antes de bloquear, é necessário observar ciclos de produção, manutenção, backup e contingência. Uma comunicação rara pode ser legítima.

A segmentação deve ser implementada nos controles adequados — firewalls, switches, ACLs, VLANs ou SGTs — e não apenas representada na plataforma.

15. INTEGRAÇÃO COM SIEM

Eventos podem ser enviados ao SIEM para correlação com autenticação, firewall, EDR e logs de servidores.

O SIEM em ambientes OT precisa preservar contexto do ativo e da zona. Um IP isolado não é suficiente para o analista entender impacto operacional.

A integração deve controlar volume, severidade e campos. Enviar todos os eventos sem filtro aumenta ruído.

16. INTEGRAÇÃO COM GESTÃO DE VULNERABILIDADES

Ferramentas corporativas de vulnerabilidade podem não escanear ativos OT por risco. Cyber Vision fornece uma fonte alternativa de inventário e contexto.

Os resultados podem alimentar processos de patching, compensação e risco. A organização precisa evitar duplicidade e divergência entre bases.

Um identificador comum de ativo facilita integração com CMDB e inventário de engenharia.

17. CYBER VISION E IEC 62443

A série IEC 62443 recomenda inventário, zonas, conduítes, gestão de riscos e controles ao longo do ciclo de vida.

Cyber Vision pode apoiar essas atividades ao mostrar ativos e fluxos. Ele não torna o ambiente conforme por si só.

O artigo sobre IEC 62443 em subestações e sistemas de potência contextualiza governança e arquitetura.

18. APLICAÇÃO EM SUBESTAÇÕES

Em subestações, a plataforma pode observar IEDs, gateways, RTUs, servidores, estações de engenharia e ativos de telecomunicações.

Protocolos como IEC 61850, DNP3 e IEC 104 exigem suporte e posicionamento adequados. Redes PRP ou HSR podem exigir atenção para evitar duplicidade e garantir visibilidade.

O projeto precisa preservar tráfego de proteção e controle. Coleta e espelhamento não devem introduzir gargalos.

19. APLICAÇÃO EM MANUFATURA

Em manufatura, Cyber Vision pode mapear CLPs, IHMs, drives, robôs, estações e servidores.

A organização por célula e linha facilita análise de dependências. A ferramenta pode ajudar a identificar acessos de fornecedores e notebooks temporários.

Períodos de troca de produto ou manutenção devem ser considerados na linha de base.

20. ARQUITETURA DE IMPLANTAÇÃO

O projeto começa com levantamento da rede e dos pontos de observação. Diagramas, VLANs, trunks, switches e enlaces precisam ser conhecidos.

Sensores devem cobrir comunicações relevantes sem duplicação excessiva. A capacidade considera quantidade de ativos, tráfego, protocolos e eventos.

O centro precisa de recursos, armazenamento, backup, DNS, NTP, certificados e conectividade segura.

21. POSICIONAMENTO DE SENSORES

Pontos próximos à distribuição enxergam tráfego agregado, mas podem perder comunicações locais dentro de uma célula. Sensores no acesso oferecem granularidade, porém aumentam quantidade.

SPAN e TAPs podem fornecer cópia de tráfego. SPAN precisa ser dimensionado para evitar oversubscription e perda de pacotes.

Sensores integrados em switches podem simplificar implantação, desde que modelo e licença sejam compatíveis.

22. DIMENSIONAMENTO

O dimensionamento deve considerar ativos, fluxos, throughput, protocolos, retenção, eventos e crescimento.

Não se deve dimensionar apenas pela quantidade de endereços IP. Um ativo pode gerar muitos fluxos, enquanto outro permanece silencioso.

A rede entre sensores e centro também precisa suportar metadados, atualizações e administração.

Inventário e contexto de risco só geram valor quando entram no processo operacional.

ISE, SIEM, firewalls, gestão de vulnerabilidades, engenharia e operação precisam compartilhar responsabilidades, critérios e fluxos de resposta.

Conhecer o serviço de Integração de Sistemas

23. SEGURANÇA DA PRÓPRIA PLATAFORMA

Cyber Vision contém inventário e topologia sensíveis. Acesso deve ser restrito por função e registrado.

Interfaces administrativas precisam de segmentação, TLS, certificados, backup e atualização. Contas compartilhadas devem ser evitadas.

A integração com MFA e PAM fortalece acessos privilegiados.

24. HARDENING DOS SWITCHES E SENSORES

A coleta integrada não elimina hardening. Switches precisam de AAA, SNMPv3, SSH, ACLs, logs e proteção de portas.

O checklist de hardening para switches Cisco deve ser aplicado com cuidado para não bloquear telemetria da solução.

Sensores e centros também precisam seguir baseline e gestão de vulnerabilidades.

25. OPERAÇÃO E GOVERNANÇA

A plataforma precisa de responsáveis claros. Engenharia valida ativos e processo; segurança analisa riscos e eventos; operação coordena mudanças.

Novos ativos e fluxos devem ser revisados. Alertas precisam de classificação, SLA e registro de decisão.

Sem governança, o inventário envelhece e eventos acumulam sem tratamento.

26. PROJETO E DOCUMENTAÇÃO

O Projeto de Telecomunicações deve incluir arquitetura, sensores, fluxos, requisitos de infraestrutura, segurança e integração.

Documentos mínimos incluem diagrama, lista de pontos de coleta, capacidade, endereçamento, certificados, regras de firewall e matriz de responsabilidades.

A integração com ISE, SIEM e firewalls precisa registrar atributos e comportamento de falha.

27. IMPLANTAÇÃO GRADUAL

A implantação deve começar por visibilidade. Sensores são posicionados, ativos são identificados e grupos são revisados.

Depois, vulnerabilidades e fluxos são analisados. Integrações e alertas são habilitados progressivamente.

Ações automáticas de bloqueio devem vir somente após maturidade, testes e aprovação operacional.

28. COMISSIONAMENTO E CRITÉRIOS DE ACEITE

O comissionamento deve verificar cobertura, identificação, protocolos, eventos, integrações e recuperação.

O roteiro mínimo inclui:

O Comissionamento e Aceite Técnico deve registrar evidências e limites conhecidos.

O aceite precisa comprovar cobertura, contexto e recuperação.

Descoberta de ativos, identificação de protocolos, novos fluxos, integrações, perda de sensor, backup e controle de acesso devem ser ensaiados com evidências.

Conhecer o serviço de Comissionamento e Aceite Técnico

29. DIAGNÓSTICO DE FALHAS

Ativos ausentes podem indicar ponto de coleta inadequado, tráfego inexistente, protocolo não suportado ou filtro.

Topologia incorreta pode resultar de NAT, redundância, SPAN incompleto ou classificação automática. A engenharia precisa validar.

Eventos em excesso podem indicar baseline inadequada ou período de mudança. Ausência de eventos pode indicar perda de sensor ou política de filtro.

30. ERROS COMUNS

O erro mais frequente é instalar a plataforma sem planejar cobertura. Outro é considerar inventário automático como verdade absoluta.

Também é inadequado enviar todos os eventos ao SIEM sem priorização ou bloquear automaticamente ativos críticos.

Por fim, a ferramenta não substitui segmentação, hardening, gestão de patches ou resposta a incidentes.

31. CONCLUSÃO

Cisco Cyber Vision fornece visibilidade de ativos, protocolos, fluxos, vulnerabilidades e mudanças em redes OT.

Seu valor depende de posicionamento de sensores, taxonomia, validação de engenharia e integração com processos de risco e resposta. Quando combinada com switches industriais Cisco, ISE, SIEM, segmentação e hardening, a plataforma cria contexto operacional para decisões de segurança sem depender de agentes nos ativos de campo.

[1] CISCO. Cisco Cyber Vision. Disponível em: https://www.cisco.com/c/en/us/products/security/cyber-vision/index.html. Acesso em: 13 jul. 2026.

[2] CISCO. Cisco Cyber Vision Data Sheet. Disponível em: https://www.cisco.com/c/en/us/products/collateral/security/cyber-vision/nb-06-cyber-vision-data-sheet-cte-en.html. Acesso em: 13 jul. 2026.

[3] CISCO. Cisco Cyber Vision Installation and Configuration Guides. Disponível em: https://www.cisco.com/c/en/us/support/security/cyber-vision/products-installation-and-configuration-guides-list.html. Acesso em: 13 jul. 2026.

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

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

[6] MITRE. ATT&CK for Industrial Control Systems.

[7] CISA. Recommended Cybersecurity Practices for Industrial Control Systems.

O que é Cisco Cyber Vision? É uma plataforma de visibilidade e segurança OT que identifica ativos, protocolos, fluxos, riscos e mudanças na rede industrial.**Precisa instalar agente nos CLPs?** Normalmente não. A solução observa o tráfego por sensores e integrações.**Os sensores podem rodar em switches Cisco?** Determinados switches industriais e versões suportam sensores integrados. A compatibilidade precisa ser confirmada.**Cyber Vision substitui SIEM?** Não. Ele fornece contexto OT e eventos que podem ser enviados ao SIEM para correlação.**Substitui firewall industrial?** Não. A plataforma oferece visibilidade; firewalls e switches aplicam segmentação e bloqueio.**Como identifica vulnerabilidades?** Associa informações observadas de produto e versão a bases de vulnerabilidades, que precisam ser validadas pela engenharia.**Pode integrar com Cisco ISE?** Sim. O contexto de ativos pode apoiar políticas de acesso e segmentação no ISE.**Coleta ativa é segura?** Depende do ativo e do método. Em OT, qualquer consulta ativa deve ser avaliada e testada.**Como dimensionar?** Considerando ativos, throughput, fluxos, protocolos, sensores, retenção, eventos e crescimento.**Como**

aceitar a implantação? Testando cobertura, identificação, fluxos, riscos, eventos, integrações, falha de sensores, backup e controle de acesso.

Soluções relacionadas

Serviços relacionados

Cisco, identidade e segmentação

Segurança, monitoramento e operação OT

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