Tripwire Industrial Visibility

Mapeamento automatizado de redes ICSs para máximo tempo de atividade

Se você é responsável por manter um sistema de controle industrial (industrial control system, ICS) seguro, você sabe como é difícil ter uma ideia precisa do que está acontecendo em todos os seus dispositivos, especialmente quando você usa tecnologia antiga e moderna. A solução Tripwire® Industrial Visibility resolve desafios operacionais com monitoramento contínuo de ameaças e inteligência avançada de registro em log, que proporciona uma visibilidade profunda e granular do ICS.

Como uma empresa Belden, a Tripwire está posicionada de forma única para preencher a lacuna de segurança cibernética entre seus ambientes de TI e TO. As soluções da Tripwire integram-se perfeitamente aos produtos que você já tem em funcionamento, como firewalls e switches industriais.

O Tripwire Industrial Visibility reúne dados de ameaças que podem ameaçar a segurança e a disponibilidade do seu ambiente de TO, analisando o tráfego da rede e realizando inspeção profunda de pacotes. Reconhece mais de 40 dos protocolos industriais nativos comumente encontrados no ICS, entendendo os dados produzidos por toda a sua gama de dispositivos industriais conectados à IIoT.

Obter um mapa preciso da sua rede

Então, o que o Tripwire Industrial Visibility faz com os dados que ele coleta? Durante um período de algumas semanas, ele usa o aprendizado de máquina para construir uma linha de base de operações normais, que é então usada para detectar anomalias. Ao ler o tráfego de rede, ele isola todos os ativos em sua rede e mapeia o fluxo de tráfego entre eles. Esses dados são usados para criar mapas de rede gráficos que facilitam a visualização da atividade e a observação de alterações não planejadas antes que qualquer dano ocorra.

Ele também simula ataques a ativos essenciais para ajudá-lo a entender sua exposição. Juntos, esses recursos permitem que o Tripwire Industrial Visibility mantenha suas redes ICS seguras de uma maneira perfeitamente otimizada para aplicações de automação.

Corrigir vulnerabilidades de forma proativa

Depois que você souber o que realmente está acontecendo em seu ambiente TO em termos de dispositivos conectados e tráfego de rede, é possível usar o Tripwire Industrial Visibility para fazer uma busca detalhada e observar as vulnerabilidades e exposições comuns (common vulnerabilities and exposures, CVEs). Essas CVEs estão publicamente disponíveis e continuamente atualizadas em uma central centralizada onde vulnerabilidades emergentes são postadas e verificadas. Se estiver usando uma versão específica de firmware ou modelo de dispositivo, você obterá informações acionáveis sobre qualquer risco conhecido de segurança cibernética a ele associado.

Detectar ameaças mais cedo

Ao contrário das redes de TI, as redes TO têm uma preponderância de repetição e comportamento previsível e consistente. A área produtiva precisa entregar milhares da mesma barra de doces todos os dias. As empresas de eletricidade

devem fornecer eletricidade dentro de uma janela estreita de desempenho. Essa repetição facilita a distinção entre comportamento normal e anormal. Quando o Tripwire Industrial Visibility usa o aprendizado de máquina para entender o que é "normal" em sua rede, ele cria uma linha de base segura e gera alertas acionáveis sempre que um comportamento inesperado ocorre. Alterações inadequadas na configuração e comandos incomuns são comparados com o comportamento base para identificar intrusos.

Por exemplo, se os arquivos começarem a desaparecer ou se os dados apresentarem erro, o comportamento suspeito acionará um alerta, fornecendo uma percepção situacional imediata. Essa abordagem de base significa que você saberá quando um adversário estiver em sua rede. A engenharia social e outros métodos de invasão de senhas dificultam a captura de usuários inválidos. O Tripwire Industrial Visibility pode sinalizar invasores mesmo que eles tenham conseguido roubar credenciais legítimas - suas informações de login podem parecer banais, mas o comportamento delas se desviará do estado base normal.

Bloquear vetores de ataque

Os invasores do ICS têm vários motivos. Você precisa estar pronto para uma ampla gama de cenários de violação, como funcionários insatisfeitos que desejam comprometer a produtividade, concorrentes que tentam o roubo de propriedade intelectual e até ataques criminosos organizados ou patrocinados pelo estado em infraestruturas essenciais. O Tripwire Industrial Visibility ajuda você a identificar seus ativos mais sensíveis e entender como eles podem ser alcançados através de vários vetores de ataque em sua rede.

Por exemplo, alguém supervisionando um andar em uma refinaria de petróleo pode saber que seu ativo mais sensível é o sistema que mantém a temperatura do óleo. Um hacker entra em um servidor de e-mail por meio de um dispositivo conectado à internet. Como eles chegam do servidor de e-mail ao destino final? O hacker precisa seguir um caminho para o seu destino final da TI para TO usando dispositivos frágeis como trampolins. É por isso que as operadoras de ICS precisam ter um mapa de rede preciso que detalhe as vulnerabilidades conhecidas

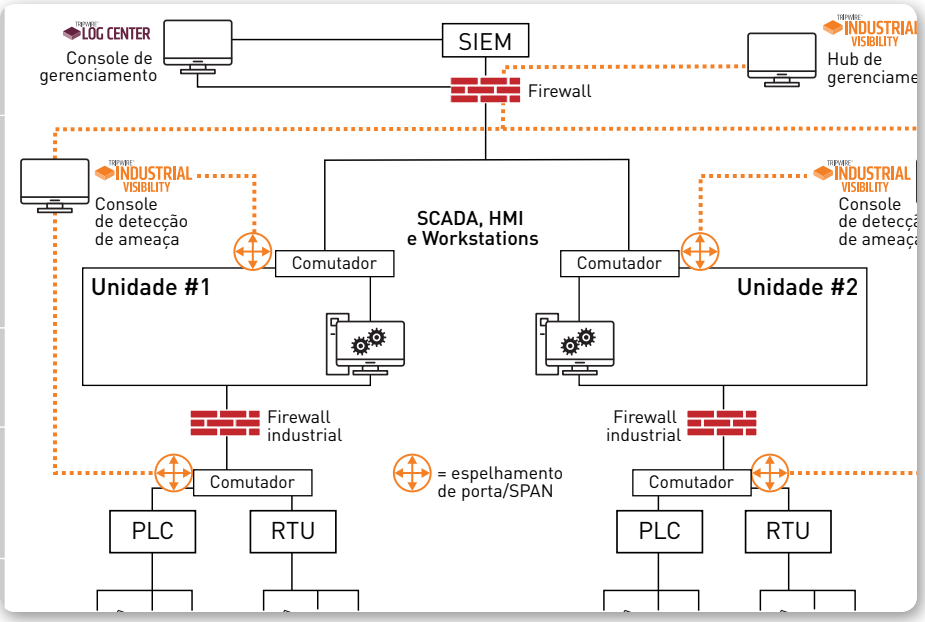

Figura 1 O Tripwire Industrial Visibility emprega sensores em toda a sua rede TO para fornecer visibilidade completa e oferecer integridade e resistência.

de cada dispositivo. Você pode usar essas informações para bloquear o caminho do hacker para seu ativo mais sensível.

Essencialmente, você pode usar o recurso de modelagem de ameaças do Tripwire Industrial Visibility para saber quais dispositivos estão conectados a seus ativos sensíveis e quebrar os links que seus adversários poderiam usar para alcançá-los. Quando você destaca um ativo sensível, o Tripwire Industrial Visibility considerará vetores de ataque que poderiam ser executados contra ele.

O recurso de gerenciamento de log do Tripwire Industrial Visibility ajuda a alinhar seu ICS aos padrões de melhores práticas de segurança cibernética industrial, como IEC 62443 e NIST.

Automatizar controles de segurança

O Tripwire Industrial Visibility potencializa o gerenciamento de alterações, o registro de eventos e a verificação passiva.

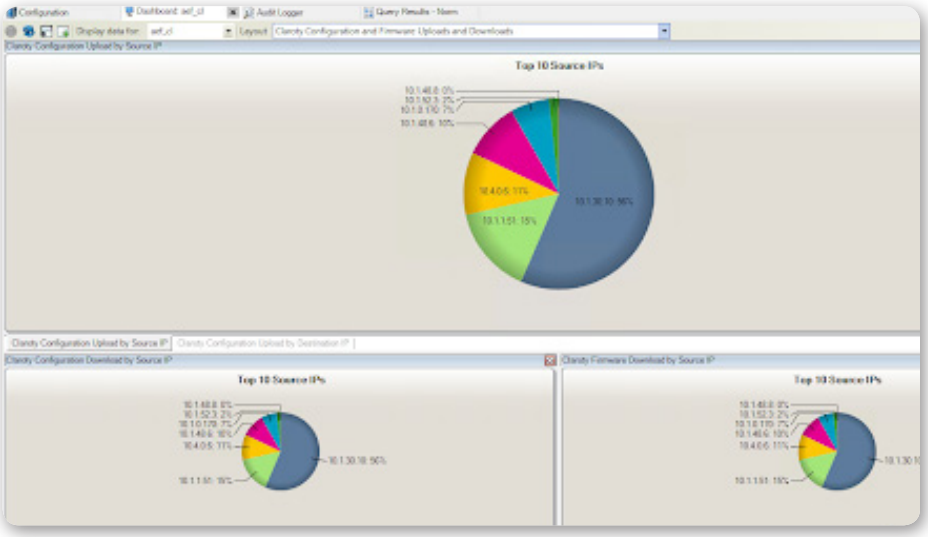

Figura 2 Principais IPs de destino e origem.

Gerenciamento de alterações

O Tripwire Industrial Visibility lê as alterações de configuração assim que elas são feitas para registrar e relatar modificações. Você poderá detectar uma alteração suspeita, como escalonamento de credenciais, antes que isso resulte em dano real ao processo e ao produto de seu ambiente de TO.

Log de eventos

O log de eventos de alteração possibilita redefinir um sistema penetrado até o último estado válido conhecido, reduzindo o tempo médio de reparo. A solução Tripwire Industrial Visibility inclui automaticamente o Tripwire Log Center™, que reúne e agrega logs de eventos em vários dispositivos. O Tripwire Log Center normaliza os dados transportados por vários dispositivos e fluxos de syslog. Em seguida, correlaciona os eventos a partir desses dados, exibindo percepções acionáveis em uma visualização clara em painel.

A inspeção profunda de pacotes (Deep Packet Inspection, DPI) é usada para extrair e analisar o tráfego TO. Ela utiliza a comunicação de rede TO ouvindo através da porta SPAN de roteadores e switches conectados ao segmento de rede, abrindo pacotes de dados e interpretando protocolos sem interromper as operações normais. Como você sabe, as redes TO herdadas podem ser sensíveis à latência e à alteração de largura de banda - e é por isso que o Tripwire Industrial Visibility usa monitoramento sem agente e descoberta passiva de ativos para deixar sua rede intacta.

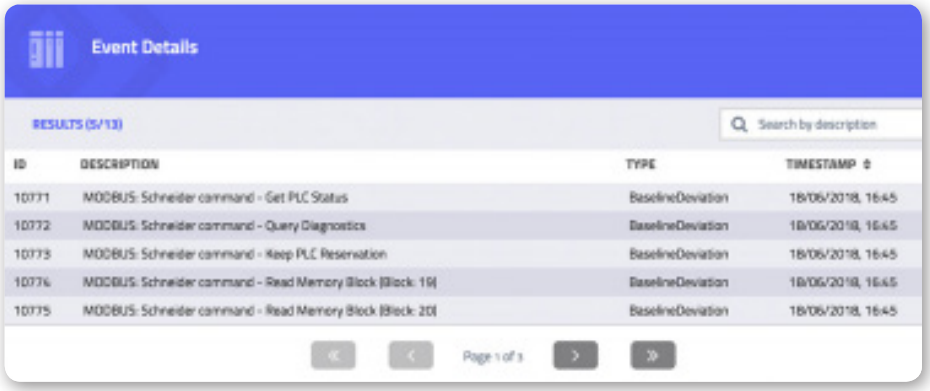

Figura 3 Os dados de eventos obtidos das comunicações do dispositivo são normalizados e apresentados como um log de evento.

Varredura passiva

A solução usa varredura passiva para evitar a interrupção de sistemas legados sensíveis. Uma combinação estratégica de varredura passiva sem agente e com base em agente mantém os sistemas herdados em funcionamento. Ao contrário dos produtos tradicionais de gerenciamento de vulnerabilidades (vulnerability management, VM) e de gerenciamento de configuração de segurança (security configuration management, SCM), ela emprega detecção sem toque que pode ser usada no momento em que sistemas herdados apresentarem falha quando pesquisados.

Conclusão

O Tripwire Industrial Visibility fornece aos operadores do ICS total clareza sobre os dispositivos e atividades em sua rede. Ele usa o gerenciamento de alterações, o log de eventos e a modelagem de ameaças para ajudar você a manter seus ativos mais sensíveis fora do alcance de intrusos. A solução protege a integridade do núcleo e a resistência cibernética de seu ambiente TO, usando varredura e detecção passivas para mantê-lo operando com disponibilidade e tempo de atividade máximos.

Pronto para uma demonstração?

Vamos levá-lo por uma demonstração da Tripwire Industrial Visibility e responder a qualquer pergunta que você tenha. Entenda como o conjunto de produtos e serviços de gerenciamento de segurança e vulnerabilidade da Tripwire pode ser personalizado para suas necessidades específicas de segurança e conformidade de TO. Visite **tripwire.com/contact/request-demo/**

A Tripwire é a líder mais confiável para estabelecer uma forte base de cibersegurança. Em parceria com empresas da Fortune 500, organizações industriais e agências governamentais, a Tripwire protege a integridade de sistemas críticos em ambientes físicos, virtuais, em nuvem e de DevOps. O premiado portfólio da Tripwire proporciona os mais importantes controles de segurança, inclusive descoberta de ativos, gerenciamento seguro de configurações, gestão de vulnerabilidades e de registros. Como pioneira no monitoramento da integridade de arquivos (file integrity monitoring, FIM), a experiência da Tripwire se fundamenta em uma trajetória de mais de 20 anos de inovação, ajudando organizações a descobrirem, minimizarem e monitorarem suas superfícies de ataque. **Mais informações em tripwire.com**

Saiba mais em tripwire.com e receba notícias, tendências e valiosas informações sobre segurança em tripwire.com/blog, ou conecte-se conosco no LinkedIn, no Twitter e no Facebook.