DARKTRACE INDUSTRIAL

DESTAQUE DO SETOR

Defesa cibernética para petróleo e gás

Nos últimos anos, o setor de petróleo e gás testemunhou a digitalização acelerada de suas operações. O setor obteve enormes benefícios, como maior eficiência e mais agilidade, mas essa transformação também mudou fundamentalmente o paradigma de segurança. As empresas de petróleo e gás agora devem proteger dispositivos de campo, sensores e sistemas de controle conectados, bem como sistemas legados, geralmente em ambientes remotos, desafiadores e com baixa largura de banda.

> À medida que a Tecnologia Operacional (OT) e a Tecnologia da Informação (TI) convergem, o setor enfrenta ameaças cibernéticas tradicionais e novos ataques contra ambientes industriais.

Esses ambientes ciber-físicos híbridos apresentam um conjunto único de desafios para as equipes de segurança já sobrecarregadas. As soluções antigas de proteção de redes de TI não são adequadas para a finalidade: elas não conseguem defender esses ambientes híbridos complexos contra um adversário em constante mudança.

> A Darktrace proporcionará aos clientes conhecimentos e inteligência acionáveis para possibilitar a identificação e neutralização dessas ameaças com mais rapidez, protegendo ativos essenciais contra ataques prejudiciais e dispendiosos.
>
> **Aymeric Sarrazin, Vice-presidente sênior da Siemens**

Big West Oil LLC

DOLPHIN ENERGY دولفين للطاقة

Ameaças em números

68% das empresas de petróleo e gás sofreram um comprometimento em 2016-17

De acordo com o Ponemon Institute, 68% das empresas desse setor sofreram pelo menos um comprometimento de segurança cibernética. Os sistemas de controle desatualizados e antigos representam uma das maiores vulnerabilidades, pois neles são baseadas todas as etapas, desde a exploração e produção até o refino e a distribuição. Muitos deles criados bem antes da segurança cibernética ser considerada uma prioridade nos negócios, esses sistemas são muito mais difíceis de corrigir, deixando deficiências na segurança da infraestrutura e nas empresas expostas a invasores mal-intencionados.

46% dos ataques cibernéticos em ambientes OT não são detectados

O Ponemon Institute também informou que uma média de 46% de todos os ataques cibernéticos no ambiente de OT não são detectados. Com tantos elementos diferentes no processo de petróleo e gás e todo um conjunto de sistemas de controle funcionando em conjunto, torna-se extremamente difícil obter visibilidade da infraestrutura distribuída e dos sites remotos. No entanto, essa falta de visibilidade significa que os invasores podem passar longos períodos despercebidos em ambientes de OT, construindo um entendimento completo da rede antes de atacar.

29% das empresas de petróleo e gás não têm uma visão em tempo real das ameaças cibernéticas

Para proteger adequadamente as redes das quais as empresas de petróleo e gás dependem, a detecção de ameaças em tempo real é fundamental. A detecção antecipada é essencial para interromper ameaças, defendendo ambientes de OT antes que a eficiência operacional seja comprometida. Considerando a segurança tradicional existente das redes de OT, as empresas de petróleo e gás precisam implantar tecnologias inovadoras de autoaprendizagem para se defender em um cenário dinâmico de ameaças.

Darktrace Industrial

Com o apoio de algumas das maiores empresas de petróleo e gás do mundo, a Darktrace Industrial protege ambientes industriais complexos contra ameaças cibernéticas. Seja na produção, no refino ou no processamento e distribuição, a Darktrace Industrial pode ser implantada em ambientes industriais em todas as etapas de operações para proteger a produção e o transporte de petróleo e gás.

A Darktrace Industrial é a primeira tecnologia de IA do mundo a implementar um "sistema imunológico" em tempo real para ambientes de OT e TI para proteger dispositivos de rede contra todo o espectro de ameaças cibernéticas, desde ransomware velozes até campanhas cibernéticas silenciosas e furtivas que passam despercebidas nas redes.

Acionada por inteligência artificial, a Darktrace Industrial aprende o "padrão de vida" de todos os controladores e estações de trabalho na rede de controle e de todos os usuários e dispositivos da rede corporativa, desenvolvendo uma compreensão ampla do "self" de todo o ambiente. Esse entendimento progressivo de "normal" possibilita à Darktrace Industrial detectar os primeiros indicadores de uma ameaça emergente, sem depender de regras, assinaturas ou suposições prévias.

> A tecnologia exclusiva de autoaprendizagem da Darktrace Industrial representa uma mudança radical na defesa de ambientes industriais, permitindo a proteção de ambientes únicos sem distinguir entre dispositivos OT, IT ou IoT.

Reconhecendo os ambientes diversos e difíceis em que as empresas de petróleo e gás operam, a Darktrace Industrial também pode oferecer suporte a ambientes remotos e com baixa largura de banda com o uso de sondas industriais robustas. As implantações remotas em plataformas podem incluir modelagem e análise local, bem como correlação central para o monitoramento da segurança de todo o patrimônio.

A Darktrace Industrial em ação

Downloads suspeitos e infecção pelo ransomware Serpent

Em uma refinaria e fornecedor de petróleo integrados, a Darktrace Industrial identificou os primeiros sinais de uma infecção por ransomware na rede da empresa. Foi constatado que um dispositivo, além de escrever seus próprios arquivos de notas de resgate, estava realizando uma série de comunicações para destinos externos raros por meio de um servidor proxy interno e, em seguida, baixando arquivos mal-intencionados.

O dispositivo passou a fazer várias consultas ao diretório SMB, ampliando a série anormal de ações. Tendo identificado ransomware anteriormente, a Darktrace Industrial reconheceu que essa atividade correspondia ao padrão de comportamento da infecção por Serpent.

A Darktrace Industrial alertou a equipe de segurança sobre o padrão de comportamento incriminador antes que a infecção se espalhasse para o ambiente de OT.

Reconhecimento detectado a partir de dispositivo externo em lista negra

O reconhecimento interno foi detectado no centro de uma empresa de produção de petróleo e gás dos EUA. Foi descoberto um dispositivo externo em lista negra com endereço IP na China conectando-se a vários elementos importantes da infraestrutura de rede usando uma VPN. Depois de conectar-se brevemente ao controlador de domínio, ele se conectou ao computador de um funcionário e ao servidor de e-mail, tentando obter acesso por meio de três pontos de entrada diferentes. O dispositivo chegou ao ponto de testar a presença de um honeypot, o que pode ter chamado a atenção para sua presença.

A Darktrace Industrial detectou essa tentativa mal-intencionada de exploração em seus estágios iniciais, permitindo que a equipe de segurança reforçasse suas defesas e garantisse que não houvesse comprometimento.

Contato

São Paulo: +55 (11) 4949 7696
Londres: +44 (0) 1223 394 100
EUA: +1 415 229 9100
APAC: +65 6804 5010

info@darktrace.com
darktrace.com