Continuous Compromise Assessment™

Um falso senso de segurança generalizado

Apesar dos bilhões de dólares investidos, continuamos a observar um aumento no número de violações de dados. O fato é: as violações ainda acontecem porque o adversário frequentemente já está dentro da organização causando estragos sem nenhuma supervisão e tornando as práticas atuais de teste ineficientes. Todos os investimentos em segurança cibernética têm o propósito de evitar algum tipo de comprometimento, então por que não estamos medindo os comprometimentos para avaliar a performance dos sistemas? Por que não estamos usando métricas para melhorar continuamente os sistemas de segurança cibernética?

O poder da Lumu:

- Detecção e resposta ampliadas
- Busca automatizada de ameaças
- Proteção da força de trabalho remota
- Combate à fadiga gerada por excesso de alertas

Fatores principais:

- Em 2020, o tempo médio de detecção e contenção de uma violação era de 280 dias.
- Entre 2015 e 2019, as empresas investiram US $670 bilhões em segurança cibernética.
- O número de violações cresceu de 781 em 2015 para 1108 em 2020.

A resposta está nos metadados da sua própria rede

Todos os ataques têm um denominador comum: **o agente de ameaças precisa usar a rede para comprometer a organização**. Por isso deixa rastros com provas que a Lumu consegue seguir por meio da análise de um vasto conjunto de fontes de metadados.

Consultas DNS

Quando um dispositivo é comprometido, ele resolve um domínio que pertence à infraestrutura do adversário, oferecendo provas concretas do comprometimento.

Logs de proxies e firewalls

Se o ataque não usar a infraestrutura DNS, sua única alternativa será conectar-se diretamente com um endereço IP.

Email

A inteligência contra ameaças, aplicada em sua plataforma de email, permite analisar quem está atacando sua organização, como estão fazendo isso e quão bem sucedidos são.

Fluxos de rede

Os fluxos de rede oferecem informações valiosas sobre os objetivos do adversário e suas tentativas de movimentar-se lateralmente.

Como funciona

O processo de Iluminação da Lumu é o principal facilitador do modelo Continuous Compromise Assessment™, que correlaciona os metadados da rede com IA e IoCs conhecidos e resulta em provas confirmadas e acionáveis do comprometimento.

Principais recursos

Informações sobre o Comprometimento Confirmado

Informações detalhadas e em tempo real sobre como os ativos da empresa estão se comunicando com as infraestruturas adversárias.

Agrupamento de incidentes

Gestão simplificada de comprometimento por meio do agrupamento dos contatos relacionados a cada incidente, reduzindo o volume de alertas e os ruídos.

Entrega em nuvem

Modelo baseado em nuvem permite implantação acelerada e retorno sobre investimento imediato e positivo.

Resposta automatizada

Responda rapidamente e com precisão. Utilize a API para integrar informações em tempo real sobre as instâncias confirmadas de comprometimento com as suas ferramentas e orquestrar a sua defesa.

Contexto do comprometimento

Contexto robusto sobre os incidentes confirmados de comprometimento, permitindo que as equipes respondam com agilidade e precisão.

Ingestão diversa de metadados

Colete metadados de rede à sua maneira. Escolha entre uma ampla gama de coletores de metadados, incluindo máquinas virtuais, agentes ou coletores personalizados por API.

Playback™

Capacidade com pedido de patente pendente que revisa até dois anos de tráfego de metadados de rede e compara os dados com os novos IoCs conhecidos.

Integrações personalizadas e prontas para uso

Aproveite os benefícios de integrações que não dependem do fornecedor, permitindo que você use a inteligência de ameaças da Lumu onde você mais precisa.

> *"As médias e grandes empresas que buscam uma solução NAV, fácil de usar com com alta capacidade, deveriam considerar seriamente a Lumu."*
> **- Forrester NAV Wave Q2 2023**

> *"Independente da disponibilidade de uma ferramenta de SIEM, a Lumu adiciona uma camada crítica na estratégia de segurança, fornecendo inteligência de comprometimento conclusiva sem interromper os processos existentes"*
> **- Gigaom Radar Network Detection and Response, Agosto 2023**

Só faltam alguns cliques
para o seu teste **GRATUITO** do **Continuous Compromise Assessment™**

Crie uma conta em
https://portal.lumu.io/account/sign-up

Lumu Technologies Inc. | 8600 NW 36th St., Suite 150 Doral, FL 33166 | sales@lumu.io | +1 (877) 909-5868