# Analisis y Monitoreo Continuo de Compromisos

## La constante duda y falsa sensación de seguridad

Independientemente de los millones de dólares que se invierten en ciberseguridad, seguimos viendo un aumento sin precedentes en el número de brechas de datos. Las brechas siguen ocurriendo debido a que casi siempre el adversario ya está dentro, y las prácticas de pruebas actuales son insuficientes para identificarlos. Si todas las inversiones en ciberseguridad tienen como objetivo evitar compromisos, entonces, ¿por qué no medimos los compromisos para averiguar cómo está funcionando el sistema? ¿Por qué no mejoramos continuamente los sistemas de ciberseguridad con métricas?

### El Poder de Lumu:

- Mejora estrategia de detección y respuesta (XDR)
- Automatiza la caza de amenazas automatizada
- Asegura la fuerza de trabajo remota
- Combate la fatiga de alertas

### Datos Clave:

- En 2020, el tiempo promedio para detectar y contener una brecha fue de 280 días.
- Entre 2015 y 2019, las empresas desplegaron $670 billones de dólares en ciberseguridad.
- El número de brechas creció de 781 en 2015 a 1108 en 2020.

## La respuesta está en sus propios metadatos de red

Todos los ataques tienen un denominador común: el actor de la amenaza debe utilizar la red para comprometer una organización. Por lo tanto, dejan un rastro de evidencia que Lumu sigue al examinar una amplia gama de fuentes de metadatos.

### Consultas DNS

Cuando un dispositivo está comprometido, este resolverá un dominio que pertenece a la infraestructura adversaria, ofreciendo así evidencia concreta del compromiso.

### Logs de Proxy y Firewall

Si el ataque no utiliza infraestructura DNS, su única opción es conectarse directamente a una dirección IP.

### Email

La inteligencia de amenazas sobre su plataforma de email permite analizar quiénes atacan a su organización, cómo lo hacen y qué tanto éxito tienen.

### Flujos de red

Los flujos de red proporcionan información detallada del objetivo de un adversario y sus intentos de moverse lateralmente.

## Cómo funciona

El proceso de Iluminación de Lumu es el habilitador de Continuous Compromise Assessment™, el cual correlaciona los metadatos de red con IoC conocidos e inteligencia artificial, resultando en evidencia accionable y confirmada del compromiso.

# Características Clave

### Inteligencia de Compromisos Confirmados

Inteligencia detallada y en tiempo real de compromisos que indica cómo los activos de la empresa se comunican con la infraestructura adversaria.

### Agrupación de Incidentes

Gestión de compromisos simplificada al agrupar los contactos relacionados en un solo incidente, para obtener menos alertas y eliminar el ruido.

### Entrega Basada en la Nube

Modelo basado en la nube que permite un despliegue acelerado y un ROI positivo inmediato.

### Respuesta Automatizada

Responda con rapidez y precisión. Integre información en tiempo real sobre instancias de compromiso confirmadas con sus herramientas existentes a través de API para orquestar su defensa.

### Contexto del Compromiso

Contexto robusto alrededor de incidentes de compromiso confirmados que les permite a los equipos ejecutar una respuesta precisa de manera oportuna.

### Ingestión de metadata diversa

Recopile metadatos de la red a su manera. Elija entre una amplia gama de colectores de metadatos, incluidas máquinas virtuales, agentes o colectores vía API.

### Playback™

Funcionalidad con patente pendiente que revisa hasta 2 años de tráfico de metadatos de red y lo compara con nuevos IoC conocidos.

### Integraciones personalizadas y listas para usar

Aproveche las integraciones "out of the box" para poder utilizar las instancias de compromiso confirmadas detectadas por Lumu donde más se necesita.

> *"Medianas y grandes empresas que busquen una solución NAV, fácil de usar y con altas capacidades, deberían considerar seriamente a Lumu."*
> **- Forrester NAV Wave Q2 2023**

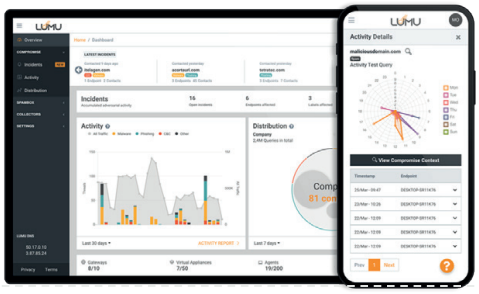
> *"Sin importar que se disponga de un SIEM o no, Lumu agrega una capa fundamental a la estrategia de seguridad al proporcionar inteligencia de compromiso concluyente sin interrumpir los procesos existentes."*
> **- Gigaom Radar Network Detection and Response, Agosto 2023**

Su POC de Continuous Compromise Assessment™ esta a su alcance, contacte a nuestro partner autorizado para agendar su prueba.

Soporte y Servicio
servicio@cybert.com.mx
www.cybert.com.mx Tel: 55-2583 - 7474

Cyber-T

Ventas
froldan@cybert.com.mx
Tel: 55-5419 - 8368



**Lumu Technologies Inc.** | 8600 NW 36th St., Suite 150 Doral, FL 33166 | jbonilla@lumu.io | 55 - 1295 - 9307