AVALORA

Boosting
human
capabilities

LUMU

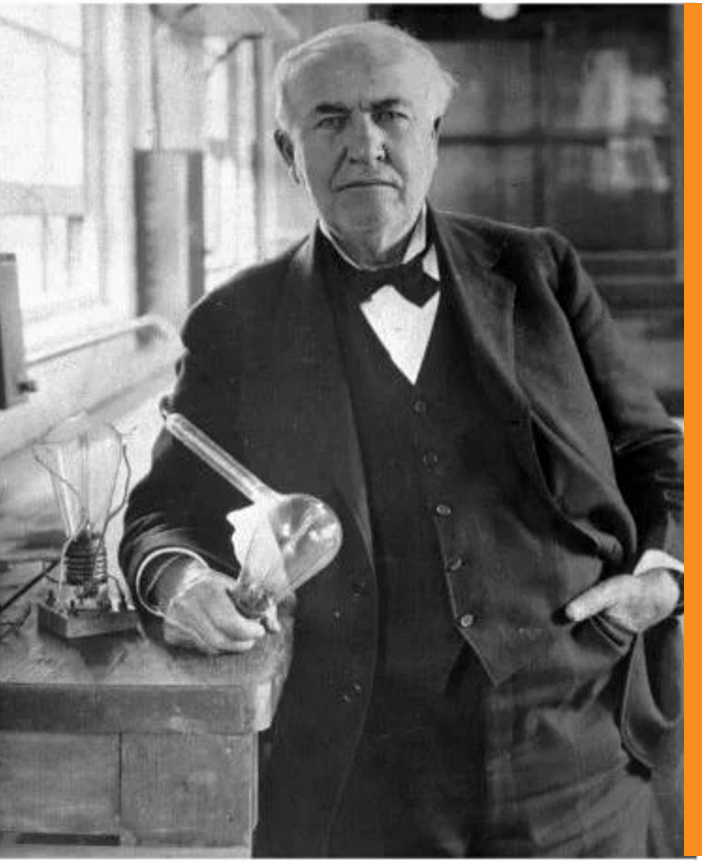
LIMITACIONES EN PRUEBAS DE SEGURIDAD Y CÓMO SUPERARLAS

avalora.com

Luis Gonzalo Acosta C.
BDM Andean Region
lacosta@lumu.io

LIMITACIONES EN PRUEBAS DE SEGURIDAD Y CÓMO SUPERARLAS

Luis Gonzalo Acosta C.
BDM Andean Region
lacosta@lumu.io



Lecciones históricas
de las pruebas

ELECTRICIDAD

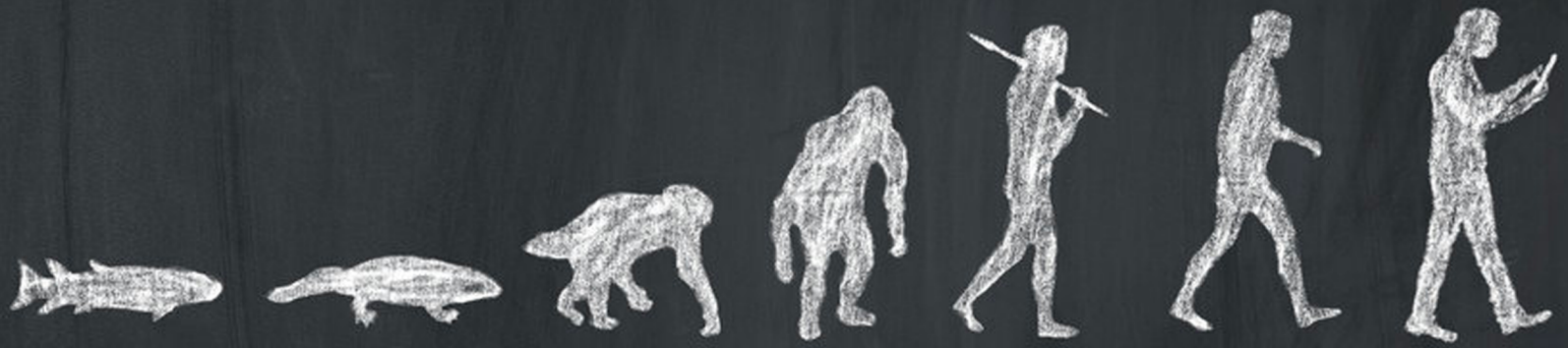
TRANSPORTE

MANUFACTURA

INTERNET ETC.

- OBSERVACIÓN
- PREGUNTA
- HIPÓTESIS
- EXPERIMENTACIÓN
- ANÁLISIS
- ITERACIÓN

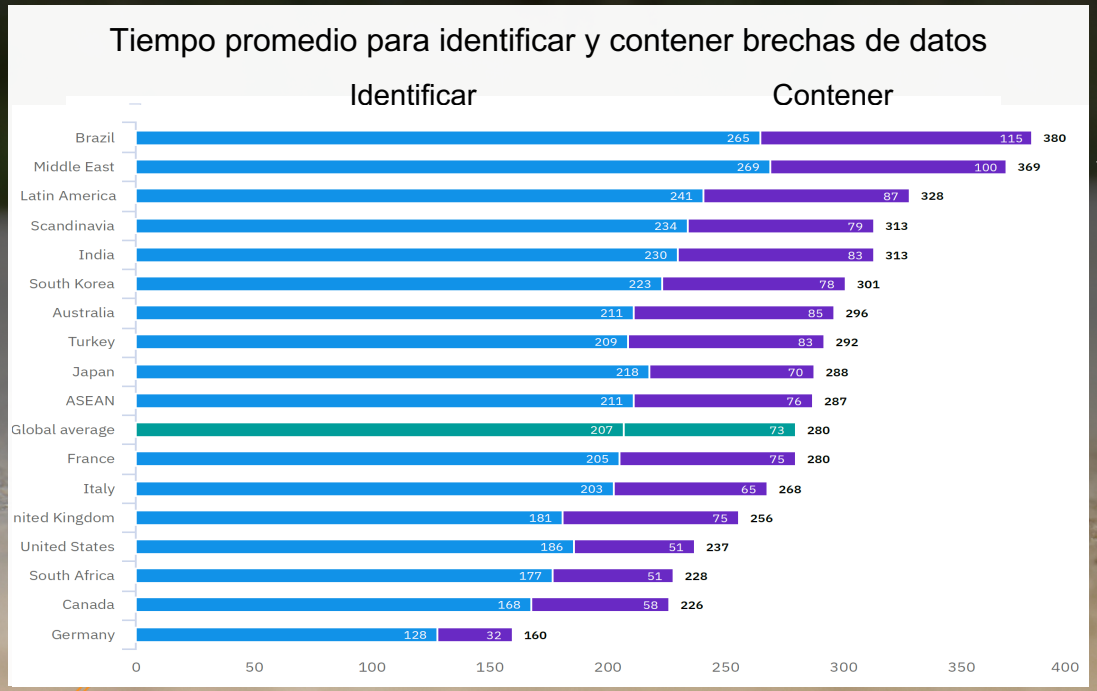
ORIGEN DE LAS PRUEBAS DE CIBERSEGURIDAD




elastic
THE HOME DEPOT
Marriott INTERNATIONAL
yahoo!
JPMorganChase
ebay
EQUIFAX
Uber
PlayStation.Network
Anthem
Nintendo
CapitalOne
No se puede mostrar la imagen.
LUMU

SOMOS LENTOS EN DETECTAR COMPROMISOS

IBM **Security** Cost of a Data Breach Report 2020



CITRIX®
10 AÑOS

yahoo!
MÚLTIPLES BRECHAS
MESES

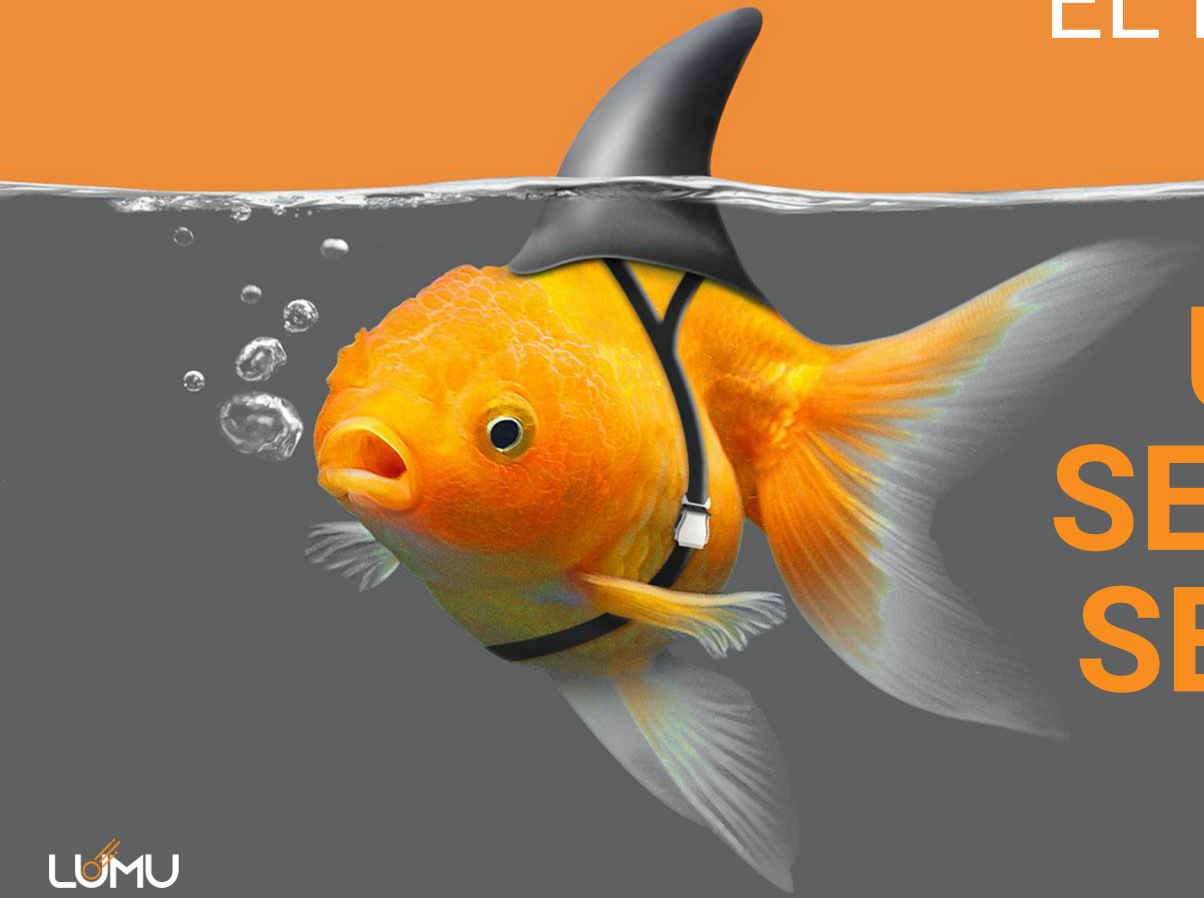
EQUIFAX
6 MESES

Marriott
INTERNATIONAL
4 AÑOS

Promedio Global :
207 dias para Identificar
73 dias para contener

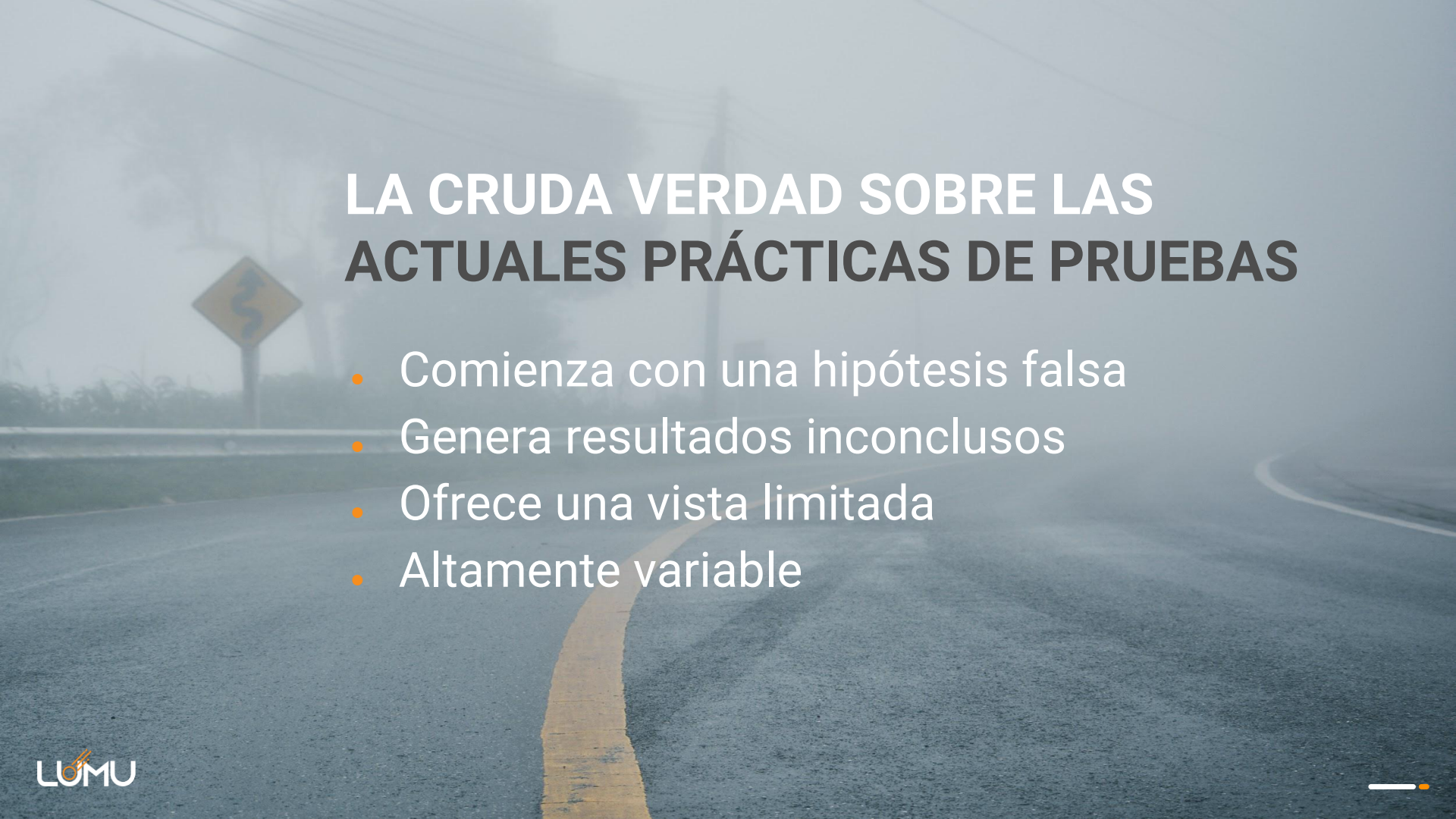
LUMU

EL RESULTADO ES



UN FALSO SENTIDO DE SEGURIDAD

LUMU



LA CRUDA VERDAD SOBRE LAS ACTUALES PRÁCTICAS DE PRUEBAS

- Comienza con una hipótesis falsa
- Genera resultados inconclusos
- Ofrece una vista limitada
- Altamente variable

LUMU

LAS ACTUALES PRUEBAS DE SEGURIDAD SON BUENAS PERO APENAS SUFICIENTES.

ES NECESARIA UNA NUEVA OLA DE PRUEBAS EN CIBERSEGURIDAD.

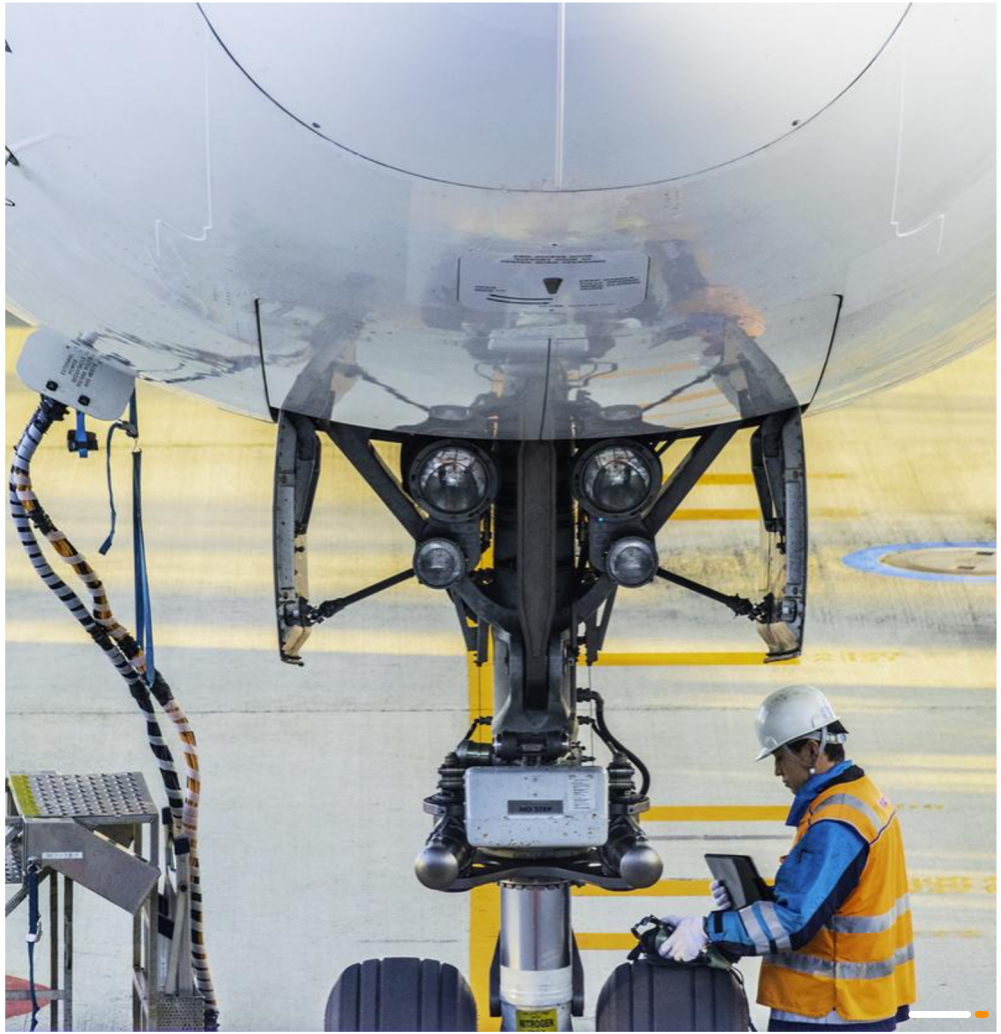
LA CIBERSEGURIDAD PUEDE APRENDER DE OTRAS INDUSTRIAS QUE HAN PERFECCIONADO EL ARTE DE HACER PRUEBAS

LUMU


1 EN 29'000.000
PROBABILIDAD DE MORIR
TRANSPORTE
AÉREO Y ESPACIAL
NO STEP
NITROGEN

Mejores prácticas en pruebas de aviación

- Sentido de urgencia
- Investigación detallada
- Remediación inmediata
- Tecnología creada con proposito
- Procesos estandarizados
- Información compartida y colaboración con la industria



Mejores prácticas en pruebas diagnósticas

HEPATITIS C

- Descubierta en 1989
- Casi siempre es asintomática
- Tratamientos altamente seguros y efectivos en 2014
- Se planea su erradicación global para 2030

CÁNCER DE SENO

- Métodos mejorados de detección
- Las muertes han disminuido en 40% en los últimos 25 años
- La tasa de supervivencia ha aumentado a 90%


ESTAMOS PROBANDO
LA HIPÓTESIS
EQUIVOCADA.
DEBEMOS ASUMIR QUE
EL ADVERSARIO YA
ESTÁ ADENTRO.

¿Cómo podemos adaptar el método científico para que se ajuste a las necesidades de la ciberseguridad?

HACER UNA OBSERVACIÓN: La industria de la ciberseguridad tiene un mal desempeño. Las brechas de datos siguen creciendo en escala y sofisticación, a pesar de las inversiones.

PREGUNTAR: ¿Por qué las brechas siguen ocurriendo?

FORMULAR UNA HIPÓTESIS: Si evolucionamos los métodos de pruebas de seguridad, las brechas se reducirán.

REALIZAR UN EXPERIMENTO: Analicemos datos de red para encontrar compromisos. Revisemos si esta información brinda valor adicional al compararla con pruebas tradicionales de seguridad.

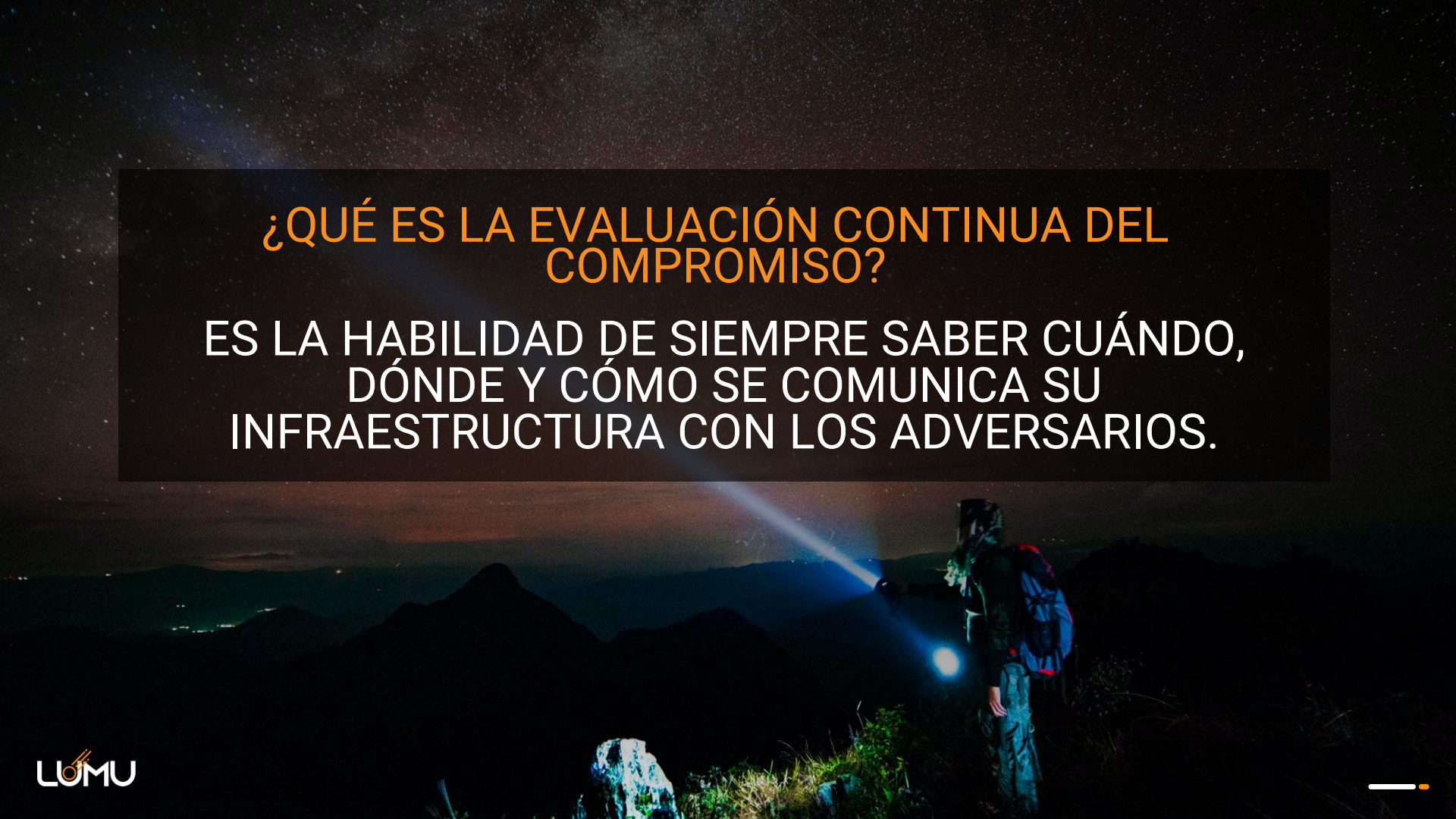
ANALIZAR DATOS: Analicemos cómo esos descubrimientos mejoran o no la postura de una organización contra los riesgos y si está mejorando su ciber-resistencia.

ITERAR: Desarrollemos una cultura de "prueba y repetición". Repitamos el proceso con información **adicional**.

LUMU

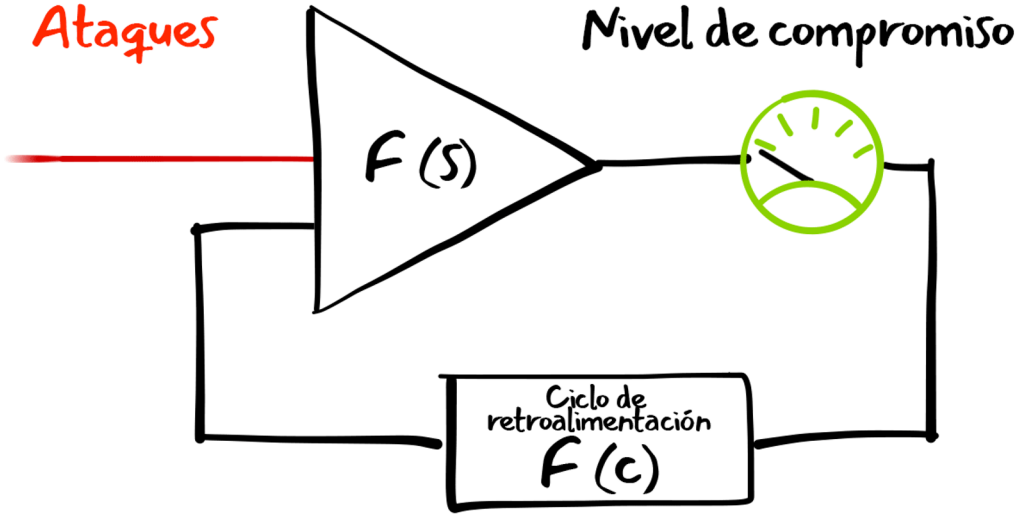
Ahora es tiempo de comenzar

- Cambie su mentalidad
- Desbloquee los metadatos de la red de su compañía
- Adopte el modelo de evaluación continua del compromiso


¿QUÉ ES LA EVALUACIÓN CONTINUA DEL COMPROMISO?
ES LA HABILIDAD DE SIEMPRE SABER CUÁNDO, DÓNDE Y CÓMO SE COMUNICA SU INFRAESTRUCTURA CON LOS ADVERSARIOS.

Sus datos cuentan la historia

Medición intencional del compromiso



F (S): Arquitectura de seguridad

F (c): Nivel de compromiso

“NUNCA SE PUEDE COMETER EL MISMO ERROR DOS VECES, PORQUE LA SEGUNDA VEZ NO ES UN ERROR, ES UNA DECISIÓN”.

Steve Denn

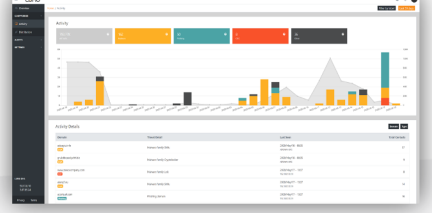
AVALORA

PARTICIPA POR 2 GIFT CARDS AMAZON (USD 50)

LOS 2 PRIMEROS QUE IMPLEMENTEN EL PORTAL LUMU FREE CON TRÁFICO

LUMU

Mida Compromiso
EN 3 PASOS



Paso 1

Crear la cuenta gratuita
e ingresar

Login with your account information

Email

someone@example.com

Password

.....

Login

INGRESAR

https://portal.lumu.io

Paso 2

Adicionar Gateway

Create Gateway

Name

My Gateway

CIDR/IP

Enter a valid IPv4 or IPv6v

Custom

Create

MUESTRAME COMO

https://docs.lumu.io/add-a-public-gateway

Paso 3

Apuntar su DNS a Lumu

Nuestros DNS son

50.17.0.10
3.87.85.24

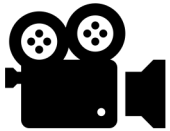
ESTOY LISTO

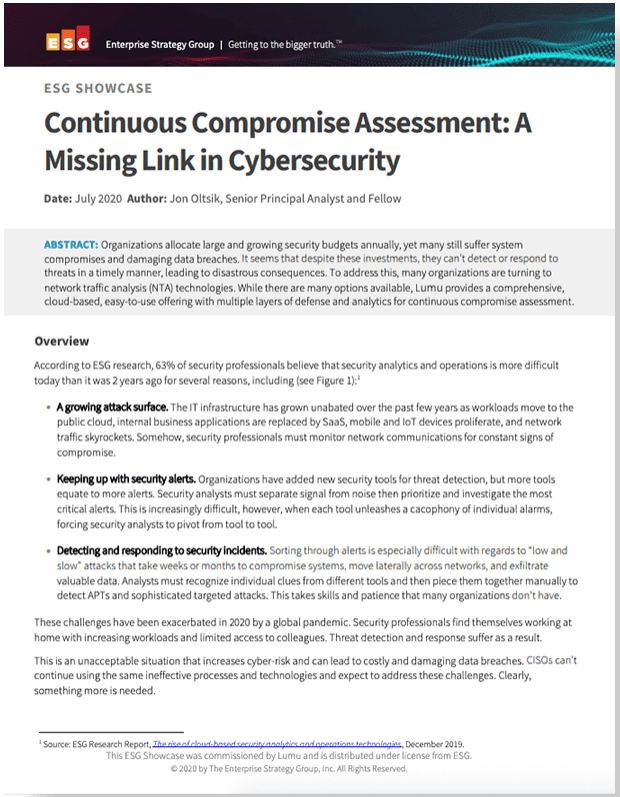
https://docs.lumu.io/point-your-dns-to-lumu

ESG Showcase:

The Missing Link in Cybersecurity

http://qrco.de/esgshow





ESG Enterprise Strategy Group | Getting to the bigger truth.™

ESG SHOWCASE

Continuous Compromise Assessment: A Missing Link in Cybersecurity

Date: July 2020 **Author:** Jon Oltsik, Senior Principal Analyst and Fellow

ABSTRACT: Organizations allocate large and growing security budgets annually, yet many still suffer system compromises and damaging data breaches. It seems that despite these investments, they can't detect or respond to threats in a timely manner, leading to disastrous consequences. To address this, many organizations are turning to network traffic analysis (NTA) technologies. While there are many options available, Lumu provides a comprehensive, cloud-based, easy-to-use offering with multiple layers of defense and analytics for continuous compromise assessment.

Overview

According to ESG research, 63% of security professionals believe that security analytics and operations is more difficult today than it was 2 years ago for several reasons, including (see Figure 1):[1]

- **A growing attack surface.** The IT infrastructure has grown unabated over the past few years as workloads move to the public cloud, internal business applications are replaced by SaaS, mobile and IoT devices proliferate, and network traffic skyrockets. Somehow, security professionals must monitor network communications for constant signs of compromise.
- **Keeping up with security alerts.** Organizations have added new security tools for threat detection, but more tools equate to more alerts. Security analysts must separate signal from noise then prioritize and investigate the most critical alerts. This is increasingly difficult, however, when each tool unleashes a cacophony of individual alarms, forcing security analysts to pivot from tool to tool.
- **Detecting and responding to security incidents.** Sorting through alerts is especially difficult with regards to "low and slow" attacks that take weeks or months to compromise systems, move laterally across networks, and exfiltrate valuable data. Analysts must recognize individual clues from different tools and then piece them together manually to detect APTs and sophisticated targeted attacks. This takes skills and patience that many organizations don't have.

These challenges have been exacerbated in 2020 by a global pandemic. Security professionals find themselves working at home with increasing workloads and limited access to colleagues. Threat detection and response suffer as a result.

This is an unacceptable situation that increases cyber-risk and can lead to costly and damaging data breaches. CISOs can't continue using the same ineffective processes and technologies and expect to address these challenges. Clearly, something more is needed.

[1] Source: ESG Research Report, *The rise of cloud-based security analytics and operations technologies*, December 2019.

¿Preguntas?

Luis Gonzalo Acosta C.

lacosta@lumu.io

+57 312-8338-678

www.lumu.io

/lumutech /lumutech /lumutech /lumutech

/lumutechnologies