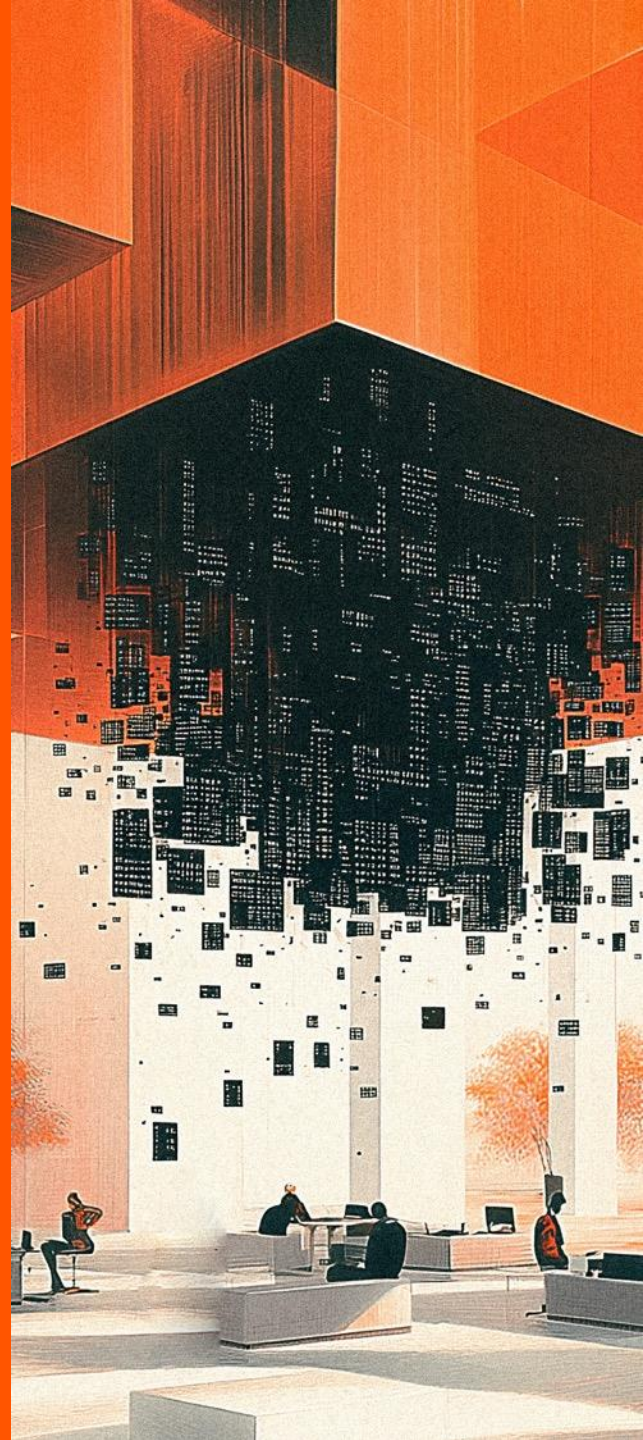
illumio

inception
Un evento de TrustDimension
EXECUTIVE SUMMIT
2026

The Mythos Moment – Bienvenidos al *vulnapocalipsis*

¿Por qué la observabilidad, contención y microsegmentación son ahora más relevantes que nunca?

Mayo 2026



illumio

inception
Un evento de TrustDimension
EXECUTIVE SUMMIT
2026

“La IA acaba de lograr en velocidad máquina lo que ningún investigador logró en décadas”

Qué es Anthropic Mythos?

U nuevo modelo de IA que ha cambiado el panorama de vulnerabilidades

Zero-Days Encontrados

1000s

Fallas críticas encontradas de manera autónoma en sistemas operativos dominantes y browsers

Tasa de Conversión de Exploit

72%+

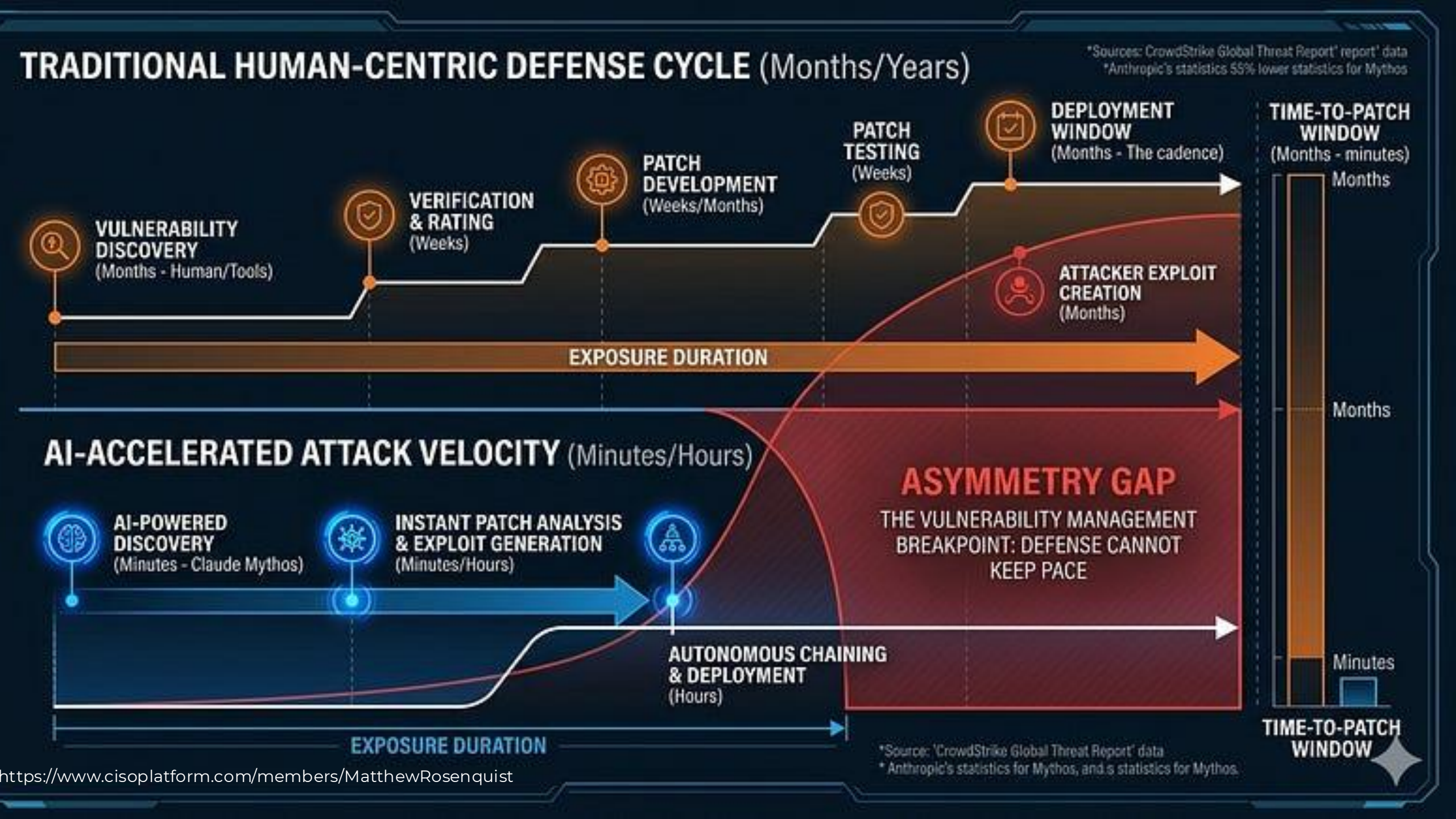
De las fallas encontradas en Firefox se convirtieron en exploits en producción

De divulgación al ataque

~Zero

La Ventana entre el descubrimiento de la vulnerabilidad y su explotación

https://red.anthropic.com/2026/mythos-preview/


TRADITIONAL HUMAN-CENTRIC DEFENSE CYCLE (Months/Years)
*Sources: CrowdStrike Global Threat Report' report' data
*Anthropic's statistics 55% lower statistics for Mythos
VULNERABILITY DISCOVERY
(Months - Human/Tools)
VERIFICATION & RATING
(Weeks)
PATCH DEVELOPMENT
(Weeks/Months)
PATCH TESTING
(Weeks)
DEPLOYMENT WINDOW
(Months - The cadence)
ATTACKER EXPLOIT CREATION
(Months)
EXPOSURE DURATION
TIME-TO-PATCH WINDOW
(Months - minutes)
Months
Months
Minutes
TIME-TO-PATCH WINDOW
AI-ACCELERATED ATTACK VELOCITY (Minutes/Hours)
AI-POWERED DISCOVERY
(Minutes - Claude Mythos)
INSTANT PATCH ANALYSIS & EXPLOIT GENERATION
(Minutes/Hours)
AUTONOMOUS CHAINING & DEPLOYMENT
(Hours)
ASYMMETRY GAP
THE VULNERABILITY MANAGEMENT BREAKPOINT: DEFENSE CANNOT KEEP PACE
EXPOSURE DURATION
*Source: 'CrowdStrike Global Threat Report' data
* Anthropic's statistics for Mythos, and.s statistics for Mythos.
https://www.cisoplatform.com/members/MatthewRosenquist

Algo no Cuadra...

La prevención y parches no pueden mantenerse al ritmo

1

El backlog Eterno de parches

Dependencias, ventanas, controles de cambios, no importa el tamaño de la compañía, siempre lo habrá

2

Ciclos de patching de 30 a 90 días incrementan el riesgo

La explotación ocurre antes que los fabricantes publiquen un CVE. Ahora la velocidad del ataque supera cualquier remediación.

3

La prevención no ayuda...

Las fallas se encuentran, los exploits son construidos, incluso de hace más de 20 años ahora con Mythos

¿Qué cambia?

Antes:

“¿Podemos encontrar, arreglar y bloquear cualquier exploit antes que los atacantes?”

Ahora:

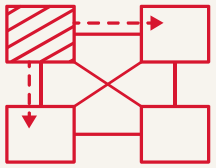
“¿Qué tanto daño es posible si un ataque es exitoso?”

- Radio de explosión

¿Por qué los ataques son exitosos?

La prevención y la detección fallarán

- Intrusión no detectada
- Atacantes dentro de la red
- Tiempo de permanencia *(dwell time)*



Propagación del Ataque

- El movimiento lateral permite a los atacantes control total de la red.
- Redes planas sin segmentación lo facilitan

En las redes modernas, híbridas y multi-nube el movimiento lateral es el MAYOR factor de Riesgo.

Activos Críticos Comprometidos

- El malware bloquea los sistemas y demandan rescate.
- Riesgo de exfiltración de datos, doble extorsión
- Penalizaciones por incumplimiento

illumio

inception
Un evento de TrustDimension
EXECUTIVE SUMMIT
2026

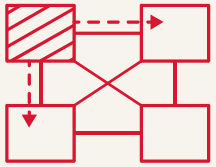
“Mythos transforma lo que los atacantes pueden descubrir y la velocidad con la que pueden explotarlo. Sin embargo, no altera la física del ataque: el atacante sigue teniendo que moverse lateralmente para alcanzar los activos que realmente importan.

La física no cambia

Las brechas se convierten en desastres a causa del movimiento lateral

La prevención y la detección fallarán

- Un zero-day explotable de forma remota le abre la puerta al atacante. Cualquier vulnerabilidad sirve. *Mythos* lo ha demostrado



Propagación del Ataque

- El atacante tiene que recorrer la red para llegar a los activos críticos. Ahí es donde las brecha es un desastre

En las redes modernas, híbridas y multi-nube el movimiento lateral es el MAYOR factor de Riesgo.

Activos Críticos Comprometidos

- Datos críticos, sistemas de producción son alcanzables si el movimiento lateral es libre

Contención – La nueva estrategia

Para asegurar ataques faclilitados por la IA

Contención NO es...

- Apagar todo
- Rediseñar la red
- Escoger entre Prevención y Respuesta

Contención SI es...

- Definir lo que más importa, datos, aplicacines, activos, servicios
- Remover la confianza implícita eliminando el movimiento lateral libre
- Asegurar el acceso de mínimo privilegio a los activos más importantes

illumio

inception
Un evento de TrustDimension
EXECUTIVE SUMMIT
2026

Atacando la física del ataque

1 Observabilidad continua

No se puede detener lo que no se ve, Illumio provee visibilidad en los caminos de comunicación y sus relaciones

2 Asume la brecha, Contén el incidente

La segmentación previene que un activo comprometido se convierta en un desastre

3 Control que ataca la física del ataque

Cuando la prevención es falible y *Mythos lo ha probado*, la segmentación determina el impacto y radio de acción de la brecha

4 Protección agnóstica a la vulnerabilidad

Illumio limita el movimiento lateral, independiente del exploit utilizado, no requiere conocimiento del CVE

Zero Trust en la era “Mythos”

Zero Trust es la Arquitectura viable

Asume la brecha

Diseña asumiendo un atacante está en la organización

Definir el “core”

Qué activos, identidades y planos d econtrol son críticos a proteger

Permite solo caminos legítimos

Mínimo privilegio, política a nivel del recurso gobierna lo que puede hablar con quién

Verificación continua

Elimina la confianza implícita en la red, acceso heredado o contexto desactualizado

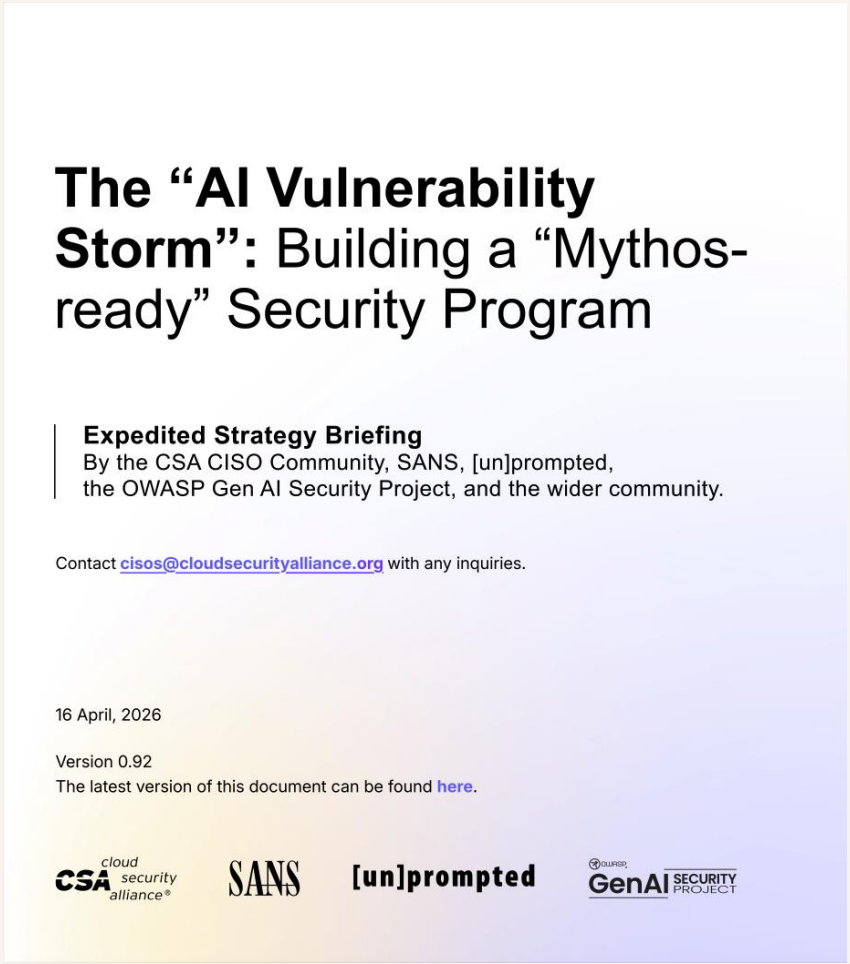
Aislamiento Rápido

Cuando se sospeche del compromiso, el control limita la propagación y acelera la contención

Resultado: una brecha aún puede ocurrir, pero no se convierte en un desastre corporativo

La necesidad de segmentación es real:

Guidance from the CSA: https://labs.cloudsecurityalliance.org/wp-content/uploads/2026/04/mythosreadyv92.pdf



The "AI Vulnerability Storm": Building a "Mythos-ready" Security Program

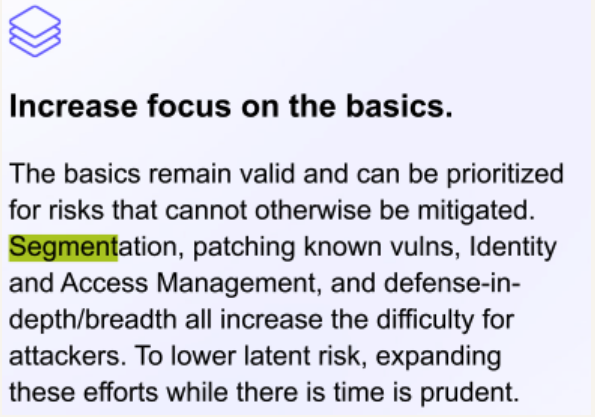
Expedited Strategy Briefing
By the CSA CISO Community, SANS, [un]prompted, the OWASP Gen AI Security Project, and the wider community.

Contact cisos@cloudsecurityalliance.org with any inquiries.

16 April, 2026

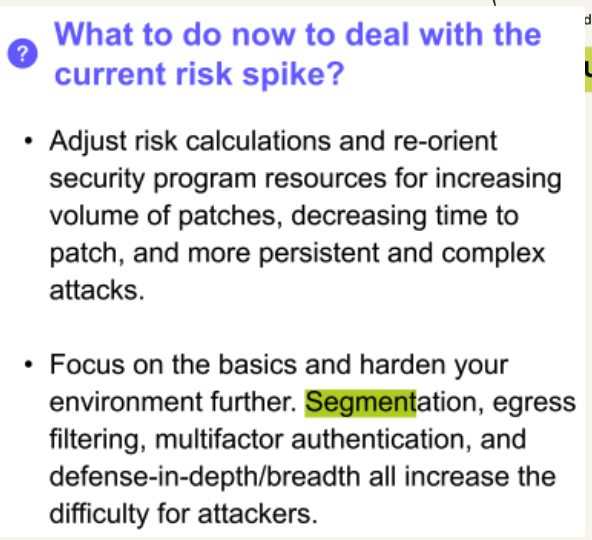
Version 0.92
The latest version of this document can be found here.

CSA cloud security alliance® SANS [un]prompted GenAI SECURITY PROJECT



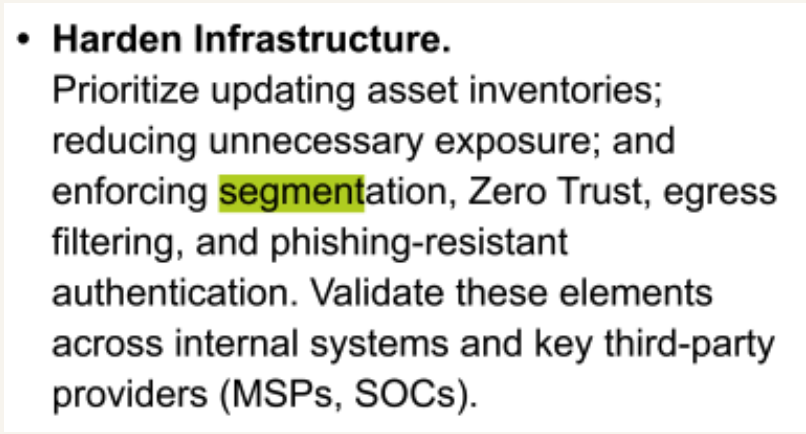
Increase focus on the basics.

The basics remain valid and can be prioritized for risks that cannot otherwise be mitigated. Segmentation, patching known vulns, Identity and Access Management, and defense-in-depth/breadth all increase the difficulty for attackers. To lower latent risk, expanding these efforts while there is time is prudent.

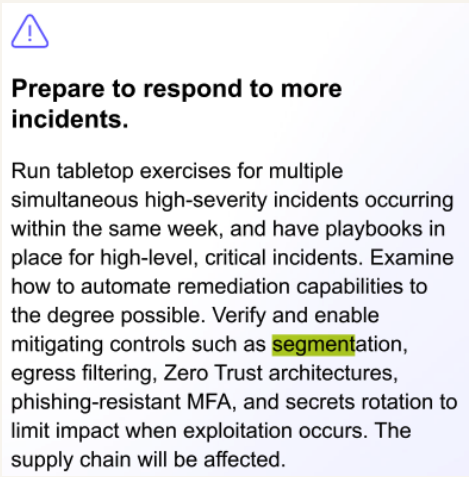


What to do now to deal with the current risk spike?

- Adjust risk calculations and re-orient security program resources for increasing volume of patches, decreasing time to patch, and more persistent and complex attacks.
- Focus on the basics and harden your environment further. Segmentation, egress filtering, multifactor authentication, and defense-in-depth/breadth all increase the difficulty for attackers.



- **Harden Infrastructure.**
  Prioritize updating asset inventories; reducing unnecessary exposure; and enforcing segmentation, Zero Trust, egress filtering, and phishing-resistant authentication. Validate these elements across internal systems and key third-party providers (MSPs, SOCs).



Prepare to respond to more incidents.

Run tabletop exercises for multiple simultaneous high-severity incidents occurring within the same week, and have playbooks in place for high-level, critical incidents. Examine how to automate remediation capabilities to the degree possible. Verify and enable mitigating controls such as segmentation, egress filtering, Zero Trust architectures, phishing-resistant MFA, and secrets rotation to limit impact when exploitation occurs. The supply chain will be affected.

illumio

inception
Un evento de TrustDimension
EXECUTIVE SUMMIT
2026

> **La contención de brechas no es negociable en la era del AI.**
> El uso de AI hace el uso, consumo, creación más rápido, más económico y más escalable.
> **La contención de brechas lo hace sobrevivible**

https://matthew-rosenquist.medium.com

Anthropic Claude Mythos will break vulnerability management