La Era Mythos

La fábrica de zero days

Javier Vallejos Martínez

- **CEO & Co-founder en Securetia** | Lic. en Informática y Especialista en Seguridad Informática.
- **Co-creador de Vulseek y Logseek** | Plataformas de gestión continua de vulnerabilidades y trazabilidad de seguridad.
- **Académico** | Creador de la Diplomatura en Ciberseguridad (UP) y Docente en la Maestría de Seguridad Informática (UBA).
- **Conferencista e Investigador** | Divulgador activo en congresos del sector sobre ciberseguridad defensiva, ofensiva e informática forense.

El impuesto de la ilusión

- Seguridad como un Add-On.
- Ciclos de escaneo periódicos e inconexos.
- Pentests anuales
- Dependencia del CVSS estático.

Claude Mythos:
Zero-Days Autónomos de la IA

- Propiedad Emergente de Razonamiento
- El Tsunami de Vulnerabilidades
- Democratización de la Explotación
- Quiebre del Modelo Defensivo Tradicional

Tiempo récord de movimiento lateral del atacante

27 SEGUNDOS

La Amenaza Silenciosa
Identidad

- 82% de las intrusiones no utilizan malware.
- Intrusiones de tipo Living off the Land.
- Validaciones ultra-veloces mediante IA.

La Brecha Insostenible

- **Atacante (IA):** Segundos para explotar.
- **Empresa Promedio:** 74 Días para remediar un CVE crítico.

Cuando el Código Cruza al Mundo Real

30% de efectividad en compromiso de extremo a extremo en sistemas industriales (Simulación Cooling Tower).

Ciberhigiene según la NSA

Niveles

0

Actividades inmediatas para reducir el riesgo

1

Actividades de transición y remediación

2

Desarrollo y validación de SOAR

3

Emulación de atacantes y resiliencia continua

Nivel 0

Actividades inmediatas para reducir el riesgo

1. Identificación de brechas de seguridad
2. Validación de parcheo automatizado y automatización de configuraciones
3. Implementar MFA
4. Validar la ingesta de logs en el SIEM
5. Revisar y eliminar rutas o conexiones de red innecesarias
6. Líneas base de comportamiento y alertas
7. Refinar las reglas de EDR
8. Control estricto de aplicaciones (Allowlisting)
9. Establecer y validar los procesos de IR y las capacidades de respuesta del CSSP

Nivel 0
1. Identificación de brechas de seguridad

- Establecer un inventario completo de la red
  - Dispositivos de Hardware
  - Inventario de Software
  - Usuario/Acceso
  - Config. de Seguridad
  - Topología
  - Propietario/Ubicación
  - Backup/Recuperación

Nivel 0
1. Identificación de brechas de seguridad

- Establecer un inventario completo de la red

“Para contrarrestar los intentos de intrusión impulsados por IA, comience realizando inventarios exhaustivos. Ingrese los datos en la IA para el reconocimiento de patrones y sugerencias de vulnerabilidades (se requiere validación humana).”

Nivel 0
1. Identificación de brechas de seguridad (cont.)

- Proteger privilegios y cuentas
  - Implementar gestión de identidades y accesos (IdAM)
  - Restringir el uso de cuentas con privilegios
  - Aplicar accesos basados en tiempo / temporales
  - Limitar los roles dentro de la plataforma de IdAM
  - Auditar las cuentas de usuario

Nivel 0
1. Identificación de brechas de seguridad (cont.)

- Segmentar las redes
  - Usar NGFW para aislar los sistemas críticos
  - Considerar instancias de VPC para limitar el movimiento lateral entre servicios críticos

Nivel 0
1. Identificación de brechas de seguridad (cont.)

- Desplegar defensas orientadas a aplicaciones
  - Monitorear y restringir el comportamiento de las aplicaciones

Nivel 0

2. Validación de parcheo automatizado y automatización de configuraciones

- Actualizar el software de inmediato
- Actualizar (upgrade) el software de manera regular
- Gestionar activamente los sistemas y sus configuraciones

Nivel 0
3. Implementar MFA

- Exigir MFA resistente al phishing de forma universal
- Transicionar de un MFA básico a uno avanzado

Nivel 0

4. Validar la ingesta de logs en el SIEM

- Desplegar un SIEM que facilite una integración sencilla
- Garantizar el reenvío de registros (log forwarding)

Nivel 0

5. Revisar y eliminar rutas o conexiones de red innecesarias

- Monitorear las conexiones entre segmentos de red
- Eliminar las conexiones que no sean necesarias

Nivel 0

6. Líneas base de comportamiento y alertas

- Establecer la línea base del tráfico normal y detectar anomalías
- Usar herramientas de auditoría para la detección del abuso de privilegios
- Realizar una búsqueda continua de intrusiones (threat hunting)

Nivel 0
7. Refinar las reglas de EDR

- Optimizar el EDR para la detección de anomalías
- Integrar el EDR con las operaciones de cacería de amenazas (hunt operations)

Nivel 0

8. Control estricto de aplicaciones (Allowlisting)

- Exigir políticas de ejecución de software firmado
- Monitorear aplicaciones anómalas, scripts y herramientas de uso legítimo (living off the land tools)

Nivel 0

9. Establecer y validar los procesos de IR y las capacidades de respuesta del CSSP

- Crear, ejercitar y revisar los planes de recuperación



Nivel 1
Actividades de transición y remediación

1. Planificación e Inicio de SOAR
    - Identificar situaciones para automatizar respuestas
    - Testear Integraciones
    - Documentar procesos
2. Refinamiento de Capacidades EDR y SIEM
    - Asegurar la comprensión del logueo y alertas
3. Validación Estricta de Segmentación de Red
    - Testeo de aislamiento
    - Eliminar las rutas o accesos de Shadow IT

Nivel 2
Desarrollo y validación de SOAR

1. Iniciar la implementación de SOAR
    - Priorizar acciones automatizadas
2. Desarrollar y validar respuestas
    - Probar en entornos controlados
3. Integrar con otros sistemas
    - Vincular con SIEM, EDR y flujos de trabajo (workflows)
4. Finalizar la documentación
    - Asegurar la supervisión humana (human-in-the-loop) donde corresponda en procesos impulsados por IA

Nivel 3
Emulación de atacantes y resiliencia continua

1. Planificar la emulación de adversarios
    - Prepararse para ejercicios de Red Team
2. Realizar evaluaciones
    - Analizar los hallazgos
    - Corregir brechas mediante Blue Teaming
3. Validación final
    - Ejercitar la recuperación
    - Realizar cacerías continuas de amenazas (threat hunts)

Acelerador de nuestra Defensa



Buscar activo

Español | Solicitar Pentest | Cerrar sesión

Tablero de control

Actualizar cada Desactivado minutos. Última actualización: 08:04:13

Vulnerabilidades por prioridad

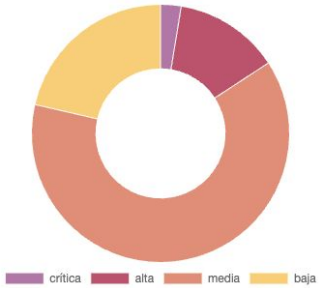
Crítica	Alta	Media	Baja
20	38	73	28

4	25	4	316
Dominios	Hostnames	Direcciones IP públicas	Direcciones IP privadas

Hallazgos por antigüedad

	90+ días	61-90 días	31-60 días	8-30 días	0-7 días
Crítica	18	0	1	3	0
Alta	72	5	11	9	16
Media	260	179	7	26	65
Baja	55	108	1	16	3

Hallazgos por prioridad



Vulseek: Acelerador de la Defensa

- ✓ Enfoque reactivo y tardío (La seguridad como addon)
- ✓ Ciclos de escaneo periódicos e inconexos
- ✓ Dependencia absoluta del CVSS estático
- ✓ Parálisis por priorización y tsunami de CVEs
- ✓ Múltiples silos de herramientas
- ✓ Intento de transición al "Shift Left Security"
- ✓ El quiebre de la "Última Milla"

En la era de los Zero-Days autónomos,
la ventaja estratégica no es de quien acumula más alertas en una consola,
sino de quien tiene la agilidad operacional para cerrar brechas a tiempo.

El futuro le pertenece a los ágiles

¿Preguntas?

Javier Vallejos Martínez

in /jjvmar

✉ jvallejos@securetia.com

¡Muchas gracias!



Securetia

Expertos en ciberseguridad

info@securetia.com