encamina

PIENSA EN COLORES

# Una consultora tecnológica que piensa en colores

*Para organizaciones vivas*

Microsoft Solutions Partner
Data & AI
Azure

Microsoft Solutions Partner
Digital & App Innovation
Azure

Microsoft Solutions Partner
Infrastructure
Azure

Microsoft Solutions Partner
Modern Work

Microsoft Solutions Partner
Security

# Workshop Threat Protection con Microsoft Sentinel

Una inmersión profunda en la estrategia de seguridad, adaptada a la organización del cliente.

# Taller de Threat Protection y Sentinel

El compromiso incluye una evaluación de verificación de amenazas y eso le permitirá obtener visibilidad de las amenazas en el entorno de nube de Microsoft 365 a través del correo electrónico, identidad y datos. Microsoft Sentinel también supervisará su entorno en busca de amenazas en todos los usuarios, dispositivos, aplicaciones e infraestructura, tanto en el entorno local como en la nube.

encamina

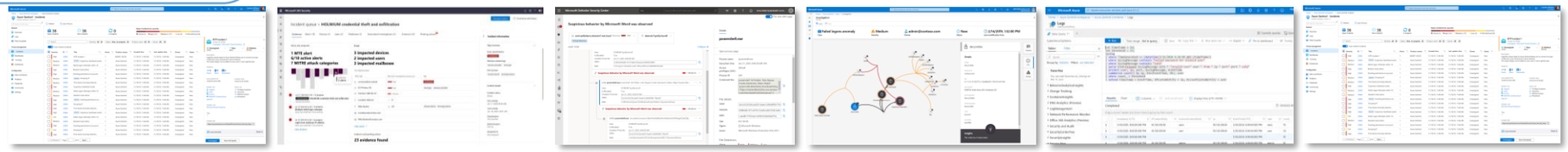
# El flujo de investigación conjunta

**Evaluación de prioridades** en Microsoft Sentinel

Iniciar **investigación** en M365 Defender

**Investigación** completa en Sentinel

**Resolver** incidente en Sentinel



- Las actualizaciones sobre el ciclo de vida (estado, propietario, clasificación) se comparten entre los productos.
- Las pruebas recogidas durante la investigación se muestran en el incidente de Sentinel.

# Metodología del taller

# Metodología del workshop

## 01. Escenarios de amenazas

El compromiso cubre dos escenarios de amenazas comúnmente vistos:

- Ransomware operado por humanos
- Riesgos de seguridad de datos provenientes de información privilegiada de la empresa

## 02. Descubrir

- Utilizando las herramientas de participación, descubra vulnerabilidades dentro del entorno de producción del cliente en la nube, servidores y puntos finales.

## 03. Analizar

- Las vulnerabilidades y los riesgos se analizan y priorizan para mostrar qué tan preparadas están las defensas contra los escenarios de amenazas.

## 04. Recomendar

- Recomendaciones detalladas de la evaluación para ayudar a priorizar mejorar su postura de ciberseguridad..


encamina

# Metodología del workshop

## Analizar

- Requisitos empresariales y de TI
- Herramientas SIEM/SOC existentes
- Orígenes de datos que se van a conectar
- Requisitos de automatización de las operaciones de seguridad.

## Definir el alcance e implementar

- Definir el ámbito de la implementación de Microsoft Sentinel
- Implementación y configuración de Microsoft Sentinel
- Conexión con Microsoft Sentinel para ingerir datos de:
  - Office 365 y Azure
  - Entra ID Protection
  - Microsoft 365 Defender
  - Microsoft Defender for Office 365
  - Microsoft Defender for Cloud Apps
  - Microsoft Defender for Endpoint
  - Integración acordada de Syslog de terceros (firewalls, servidores proxy)

## Descubrir

- Use Microsoft Sentinel para analizar y detectar amenazas para su organización
- Use Microsoft Sentinel para buscar amenazas de seguridad de forma proactiva.

## Recomendar

- Asignar amenazas encontradas a los productos de seguridad de Microsoft 365
- Proporcionar una hoja de ruta de implementación de Microsoft Sentinel

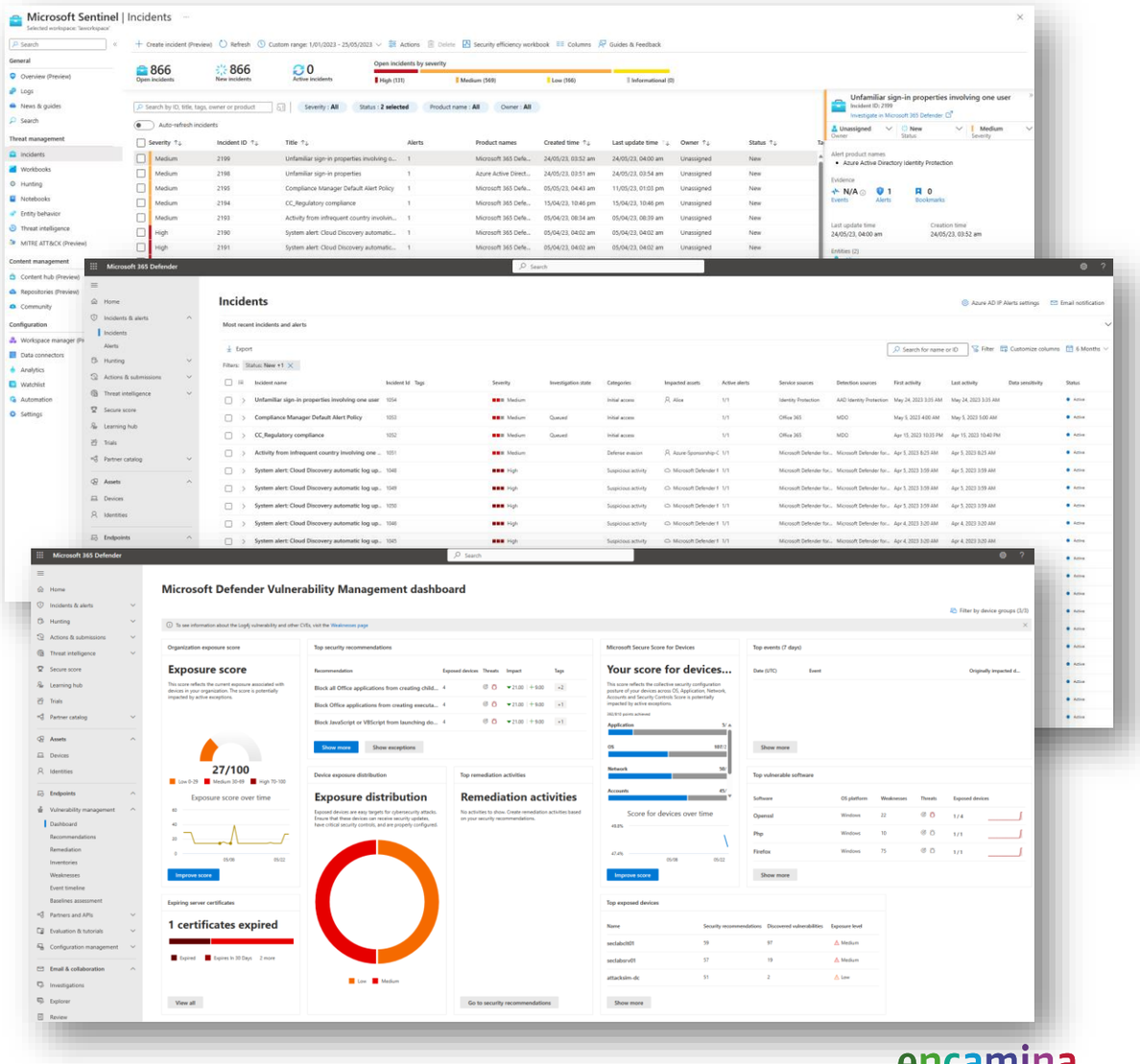
# Recogida de datos

- Amenazas a la identidad, los endpoints, el correo electrónico y los datos detectados por las herramientas de participación.
- Vulnerabilidades y configuraciones incorrectas detectadas por las herramientas de participación.
- Carga de registros de Cloud Discovery (hacia el final)*.

* A menos que use Microsoft Defender para punto de conexión como origen de los datos de detección en la nube.

# Exploración de amenazas y vulnerabilidades

- Obtenga visibilidad de las amenazas y vulnerabilidades de sus entornos locales y en la nube obtenidos a través de Microsoft Sentinel y Microsoft 365 Defender.
- Obtenga información sobre los escenarios y características clave del producto de Microsoft Sentinel y Microsoft 365 Defender.
- Obtenga recomendaciones sobre:
  - Cómo mitigar los ciberataques.
  - Cómo descubrir y priorizar vulnerabilidades y configuraciones incorrectas.




encamina

# Siguientes pasos (Servicios Continuos) Referencial

## Seguridad

- Reuniones semanales de mejoras en la seguridad de M365.
- Participación como consultoría de seguridad ante auditorias.
- Apoyo especializado en seguridad en M365 para resolver situaciones o eventos de seguridad.
- Participación en incidentes de seguridad como especialista.
- Participación en ejercicio de phishing (temas a solicitud de empresa serán adicionales).
- Atención de Incidentes que se generarán desde la plataforma MCAS  los casos de uso que están definidos en el monitoreo.
- Eventos de malware en base a criterios que serán definidos durante los primeros días del servicio.
- Risk sing-in
- Remediación de alertas críticas 8x5.
- Remediación de actividad anómalas en cuentas de correo bajo criterios que se definan.
- Seguimiento de campañas masivas de phishing y remediación de materialización de riesgos en tanto se tome el servicio de gestión de identidad y protección avanzada.
- Informes mensuales.
- Creación de nuevos indicadores a demanda de equipo de seguridad TI .

## Gestión de identidad

- Administración y soporte de la solución de Microsoft Entra P1 en horario 8x5, de manera remota de los siguientes servicios:
  - Habilitación y deshabilitación de MFA
  - Generación de políticas de Acceso condicional
  - Configuración de alertas y notificaciones.

## Protección avanzada de amenazas (Phishing-Malware)

- Administración y soporte de la solución de Microsoft Defender para Office 365 en horario 8x5, de manera remota.
- Administración y operación de Microsoft Defender para Office 365 bajo las best practices, capacity Planning, soporte y troubleshooting.

# ¡Gracias! Para localizar o contactar con ENCAMINA puedes:

Enviar un mail a:

info@encamina.com
administracion@encamina.com

O llamar al:

Madrid +34 917 893 823
Valencia +34 962 698 064
Dublín +353 85 815 0750

O enviar un fax al 962 698 063

O hablar personalmente con tu Account Manager

O visitarnos en:

C/O'Donnell, 34
28009, **Madrid**

---

C/Jerónimo Roure, 49
46520 Puerto de Sagunto, **Valencia**

---

2 Dublin Landings
North Dock, **Dublín**

---

InnovaParq Universidad de La Laguna
Av. Trinidad, 61. Campus Central
38200, S. Cristóbal de La Laguna, **Tenerife**

Puedes encontrarnos en: