Security Operations Integration_

Malware Information Sharing Platform (MISP) Integration

Cytomic Orion se integra con la plataforma MISP_

La Integración de las plataformas permite enriquecer la plataforma MISP con la Cyber Threat Intelligence propia de Cytomic, así como la búsqueda de Indicadores de Compromiso relativos a incidentes de seguridad recibidos en MISP en los activos protegidos con la plataforma Cytomic.

La integración de Cytomic en la plataforma MISP permite extender la información disponible en MISP con la Cyber Threat Intelligence de la plataforma Cytomic.

Cuando, desde la plataforma MISP, se interroga a la de Cytomic por un indicador de compromiso, esta devuelve su estado y prevalencia en los assets de la organización.

Así mismo, la integración en la taxonomía de MISP, permite al equipo de seguridad de la organización, o su proveedor de servicio, buscar atributos de eventos, provenientes de otras fuentes de ciber inteligencia, como IOCs en la actividad de los activos protegidos con las soluciones Cytomic.

La búsqueda de estos atributos (hashes, IPs, Dominios, URLs) puede ser configurada para realizarse en tiempo real y/o en retrospectivo, hasta 365 días. Siendo esta la retención de telemetría estándar en la plataforma Cytomic.

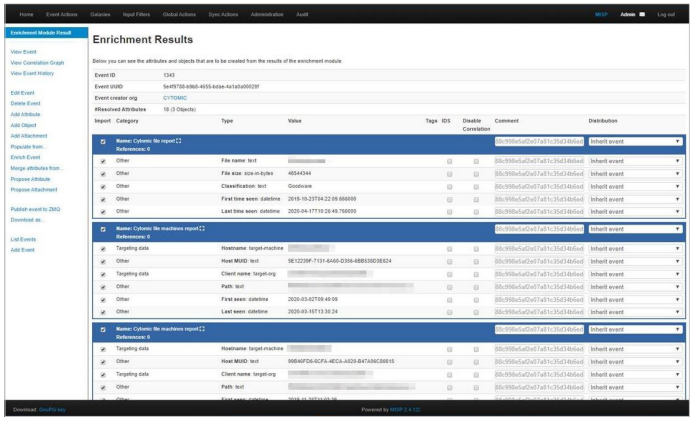


Figura 1. *Enriquecimiento en la plataforma MISP con la Cyber Threat Intelligence de Cytomic. Además de la clasificación y prevalencia de la entidad, se obtiene los activos de la organización donde la entidad se ha visto y su prevalencia.*

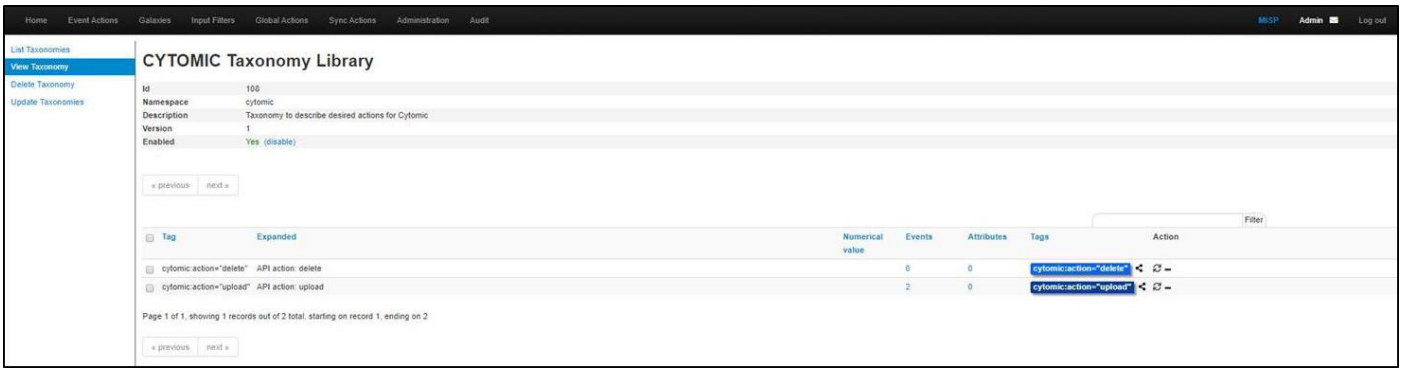
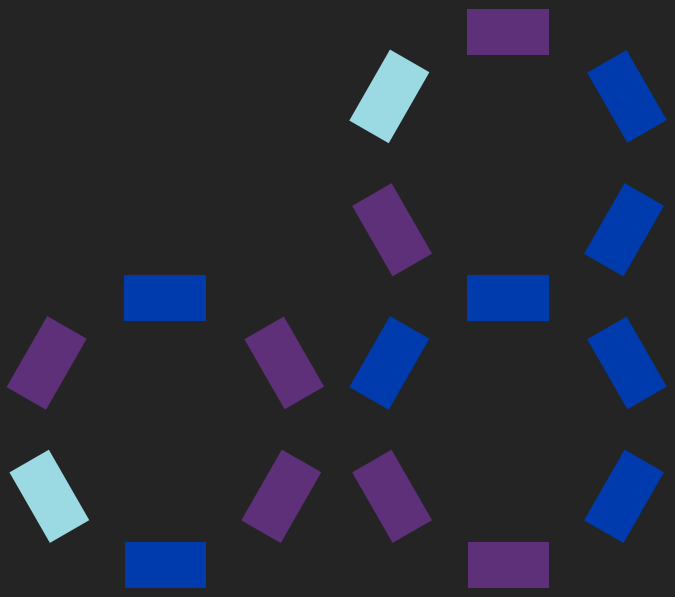


Figura 2. *Desde MISP se habilita la búsqueda de IOCs en los activos de la organización, tanto en tiempo real como en retrospectivo, hasta 365 días.*

La Taxonomia de Cytomic permite configurar la búsqueda continúa de atributos proveniendes de ciertos feeds de confianza o la búsqueda manual de eventos y atributos relativos a incidentes concretos.

Beneficios para los cliente de Cytomic y MISP_

- Automatizar el enriquecimiento de información en MISP con Cyber Threat Intelligence de Cytomic.
- Información inmediata de los activos donde se ha visto determinados atributos, por ejemplo, aplicaciones maliciosas provenientes de información de otras fuentes. De esta forma, se acelera el proceso de respuesta a Incidentes antes de que resulte en una violación de seguridad.
- Automatización de la búsqueda dinámica de Indicadores de compromiso provenientes de eventos/ incidentes de otras fuente de MISP. Estos indicadores se buscan en tiempo real y/o de forma retrospectiva en la actividad recogida, de hasta 365 días, de los activos de la organización.



La Plataforma Cytomic_

La plataforma Cytomic proporciona una solución de seguridad avanzada endpoint, EDR, Patch management, full Encryption, una solución nativa cloud para la detección, caza, contención y respuestas a ciberamenazas de forma centralizada desde la nube y desplegando un único agente ligero.

Cytomic protege a los clientes contra ciberataques avanzados, utilizando inteligencia artificial/aprendizaje automático y prevención de amenazas basada en Indicadores de Ataque (IOA) para detener amenazas conocidas y desconocidas en tiempo real.

Permite, además, la respuesta eficiente, desde la nube, ante incidentes antes de que estos se conviertan en una violación de seguridad.

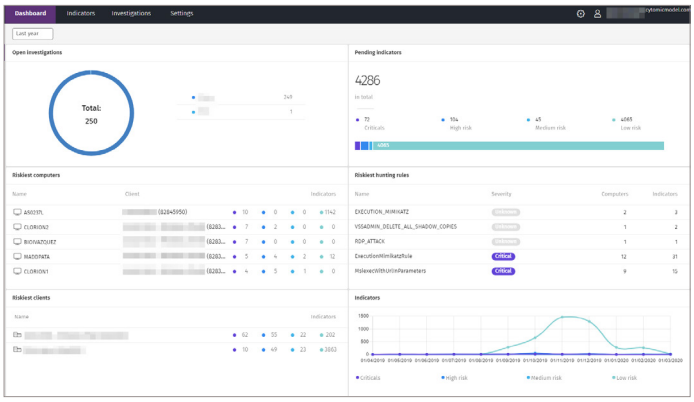


Figura 3. *Dashboard de Operación de Cytomic Orion. Indicios de actividad sospechosas, alertas e investigaciones de incidentes de seguridad.*

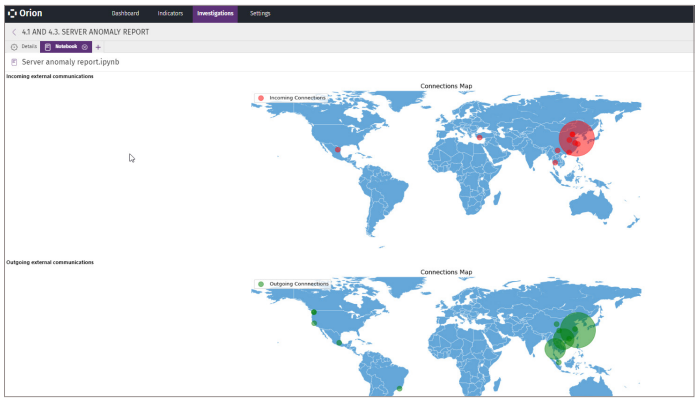


Figura 4. *Ejemplos de una investigación de un incidente mediantes un Jupyter Notebook que ejecuta algoritmos de correlacción de eventos y determinar así el origen del incidentes de seguridad.*

Premios y Reconocimientos_

Common Criteria "EAL2+"
Information Technology Security Evaluation

High "ENS" Classification
Esquema Nacional de Seguridad Español

Qualified IT Security Product
Centro Criptológico Nacional

Panda Security participa regularmente y obtiene premios en protección y rendimiento de Virus Bulletin, AV-Comparatives, AV-Test, NSSLabs. El portfolio de Cytomic comparte tecnologías, plataformas y servicios con las soluciones de Panda Security, extendiendo sus capacidades con los servicios gestionado de Hunting y con Cytomic Orion

[AV-Comparatives test Adaptive Defense 360 "Esta solución clasifica todos los procesos ejecutados, registra cualquier tipo de malware"]

CYTOMIC

More info at_
cytomic.ai

Let's talk_
+34 900 90 70 80

cytomic.ai