Security Operations Integration_

Malware Information Sharing Platform (MISP) Integration

Cytomic Orion integrates with the MISP platform _

The integration of the platforms allows you to enrich the MISP platform with Cytomic's proprietary threat intelligence, as well as searching for indicators of compromise related to security incidents received in MISP on the assets protect with the Cytomic platform.

The integration of Cytomic in the MISP platforms allows you to extend the information available in MISP with Cytomic platform's Cyber Threat Intelligence.

If the object that has been queried on the Cytomic platform is seen on the organization's protected assets, this information is included in the extended information.

Likewise, the integration into MISP's taxonomy allows the organization's advanced security team, or its service provider, to search for event attributes in MISP, from other cyber intelligence sources, such as indicators of compromise in the activity of the assets protected by Cytomic solutions.

The search for these attributes (files, IPs, domains, URLs) can be configured in real time and/or retrospectively, up to 365 days, which is the standard retention of telemetry in the Cytomic platform.

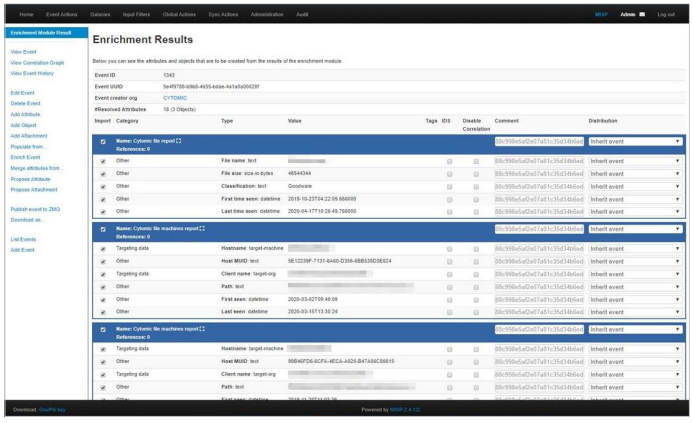

Illustration 1. *Enrichment in MISP with Cyber Threat Intelligence from the Cytomic platform In addition to the classification and prevalence of the entity, the assets of the organization where the entity has been seen and its prevalence are obtained.*

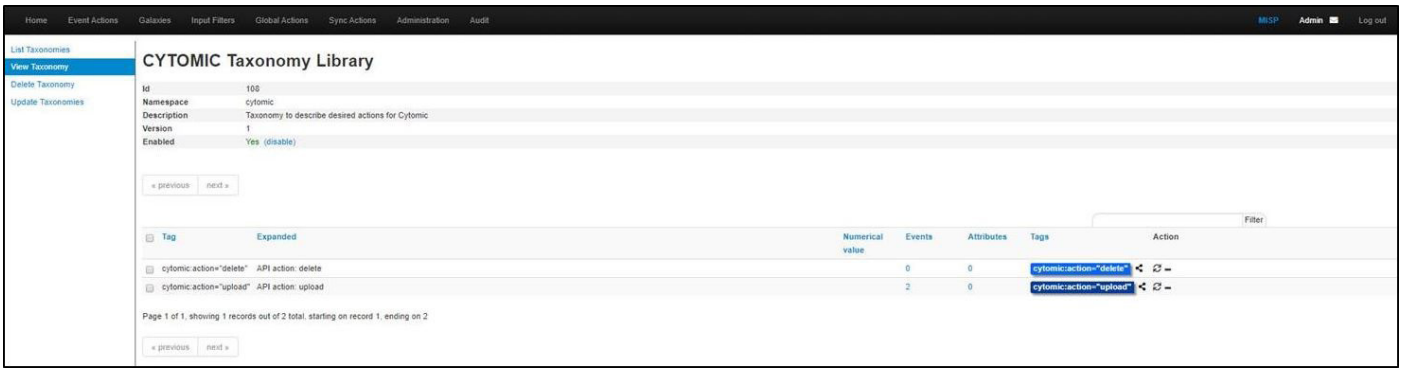

Illustration 2. *MISP enables the search of IOCs in the organization's assets, both in real time and in retrospect, up to 365 days.*

Cytomic Taxonomy allows you to configure the continuous search for attributes from certain trusted feeds or the manual search for events and attributes related to specific incidents.

Benefits for Cytomic and MISP clients_

- Automating the enrichment of information in MISP with Cytomic Cyberthreat Intelligence.
- Immediate information about assets where certain attributes have been seen, which can include malicious applications coming from information from other sources. This way it speeds up the incident response process, before it can lead to a cybersecurity breach.
- Automation of searches for indicators of compromise from events/incidents from other MISP sources. These indicators are searched for in real time and/or retrospectively in the activity collected, up to 365 days, from the organization's assets.

The Cytomic Platform_

The Cytomic Platform provides an advanced endpoint security solution, EDR, patch management, full encryption, and cloud-native detection, hunting, containment and response solution for cyberthreats, all centralized from the cloud and deployed from a single, lightweight agent.

Cytomic protects clients against advanced cyberattacks using artificial intelligence and deep learning, as well as IoAs to stop known and unknown threats in real time.

It also allows efficiently response, from the cloud, to incidents before they become a breach.

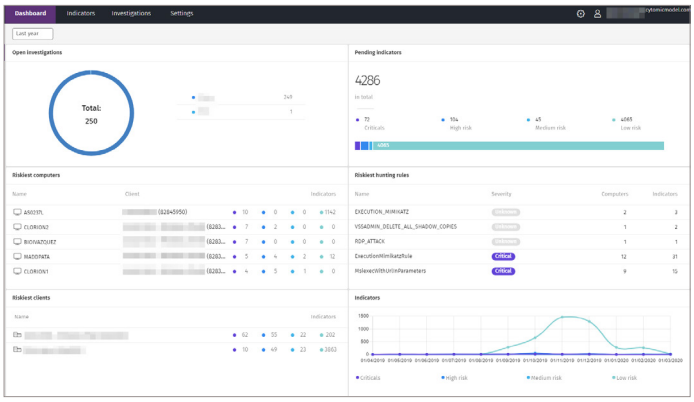

Illustration 3. *Cytomic Orion Operation Dashboard. Suspicious signs of activity, alerts and investigations of security incidents.*

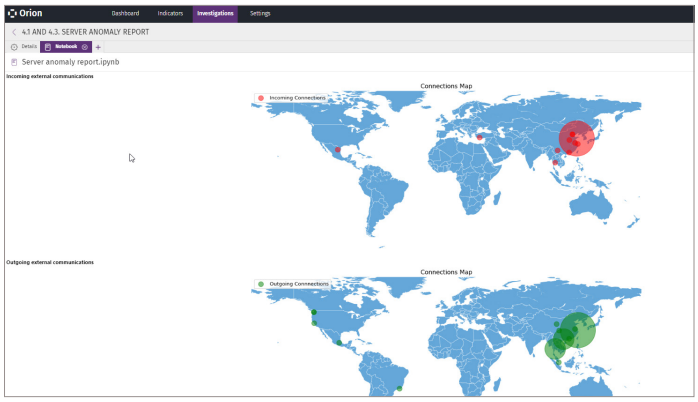

Illustration 4. *Examples of an incident investigation using a Jupyter Notebook that runs event correlation algorithms to determine the source of the security incident.*

Awards and Recognitions_

Common Criteria "EAL2+"
Information Technology Security Evaluation

High "ENS" Classification
Spanish National Security scheme

Qualified IT Security Product
Centro Criptológico Nacional (National Cryptology Center)

Panda Security regularly participates and wins awards for protection and performance from Virus Bulletin, AV-Comparatives, AV-Test, and NSSLabs. Cytomic's portfolio shares technologies, platforms and services with Panda Security's solutions, extending its capacities with managed hunting services and Cytomic Orion.

[AV-Comparatives test Adaptive Defense 360 "This solutions classifies all processes executed and registers any kind of malware"]

CYTOMIC

More info at_
cytomic.ai

Let's talk_
+34 900 90 70 80

cytomic.ai