Threat Intel Triage in MISP. From tags to real IOCs and patch guidance

Overview

In this lab, I performed threat intelligence triage in MISP to turn tagged reporting into a hunt ready package. The objective was to locate the correct event using tags and Galaxies, extract actionable indicators from the Attributes view, validate key artifacts using external references like VirusTotal, and translate vulnerability details into clear defensive scope that a SOC can act on.

SOC handoff summary

Classification: Threat intel triage output, actionable IOC and vulnerability guidance
Priority: Medium, elevate if indicators hit in environment telemetry
Confidence: High
Key outputs
Indicators for blocking and hunting: orangebronze.com, 209.126.69.167:2020
Validated file artifact: SHA256
4b8037a6c293bbdfe0683ddd7d7fa3317838ac8fd5a59bb741aae0cf3abf48296677be7ac0864c4f
124c2e168c0af94
Initial access vector: CVE 2022 29499
Defensive scope: MiVoice Connect 19.2 SP3 and earlier

Platform and sources used

MISP event list and event view, tags, Galaxies clusters, correlation
External enrichment via VirusTotal permalink references when present
Basic mapping to MITRE ATT and CK concepts for communication and reporting

Investigation workflow

1. Scope the dataset quickly
   I started in the MISP event list and narrowed scope using filters. Depending on the question, I filtered by event info or by tags to reduce noise and get into the right neighborhood fast.

2. Pivot through Galaxies when tags were close but not exact
   A key lesson from this lab was tag precision. When the tag string did not match the exact Galaxy cluster naming, results were misleading. I corrected this by pivoting through Galaxies and selecting the correct cluster tag, then returning to the event view.

3. Use the event view as the source of truth
   Once I confirmed the correct event, I relied on the Attributes view to extract concrete indicators. This kept the work evidence based and repeatable. Domains, IPs, file hashes, filenames, and references were all pulled directly from recorded attributes.

4. Validate and enrich using external references
   When VirusTotal permalinks were provided, I used them to confirm artifact context and recover details such as original filename. I treated external enrichment as confirmation, not as the starting point, and I focused only on details that would change the next defensive action.

5. Convert intel into defensive actions
   I translated the observed reporting into two outcomes a SOC can execute immediately.
   Hunt package. The exact domain and IP with port for detection, plus the SHA256 for endpoint blocking and historical search.
   Patch guidance. The exploitation vector, CVE 2022 29499, and the affected product scope, MiVoice Connect 19.2 SP3 and earlier.

Key extracted indicators and defensive scope

Indicators
Domain: orangebronze.com
Network: 209.126.69.167:2020
File hash:
4b8037a6c293bbdfe0683ddd7d7fa3317838ac8fd5a59bb741aae0cf3abf48296677be7ac0864c4f124c2e168c0af94

Vulnerability scope
CVE: 2022 29499
Affected product guidance: MiVoice Connect 19.2 SP3 and earlier

Recommended response actions, production safe guidance

Immediate SOC actions
Add orangebronze.com to DNS and proxy monitoring, alert on resolution or outbound connections.
Add 209.126.69.167 port 2020 to network detections, and check historical egress logs for hits.
Add the SHA256 to endpoint hunting workflows and block lists where policy allows.

Vulnerability actions
Confirm whether MiVoice Connect is present, then validate version and patch status for 19.2 SP3 and earlier exposure.
Prioritize patching or compensating controls if any matching indicators appear in telemetry.

Detection and reporting improvements
Store the indicators as a small hunt package in your case system. Include source event reference, timestamps, and confidence notes.

Map the observed initial access method to ATT and CK terminology for consistent reporting across incidents and stakeholders.

Skills demonstrated
Threat intel triage in MISP using tags, Galaxies, correlation, and event attributes
IOC extraction and normalization for hunting and blocking
External enrichment using VirusTotal references to validate artifacts and recover context
Basic vulnerability triage translating CVE details into clear patch scope
SOC style output focused on actions, not only data