Incident Classification Notes

Incident Classification Notes

Categories:
- Malware: ransomware, trojans.
- Phishing: credential theft via T1566 (MITRE ATT&CK).
- DDoS: service disruption.
- Insider Threat: unauthorized data export.
- Data Exfiltration: transfer of sensitive files.

Frameworks:
- MITRE ATT&CK -> T1566 (Phishing), T1190 (Exploit Public-Facing App).
- ENISA -> Standardized taxonomy for reporting.
- VERIS -> Vocabulary for consistent incident sharing.

Example:
Phishing Email with link -> Classified as "Phishing" -> MITRE ATT&CK T1566 -> Enriched with source IP, affected user, times