Threat Intelligence & ATT&CK Mapping Project — Summary

Author: Velkris (Jared Perry)
Focus: Threat Intelligence / Red Team Alignment
Environment: Controlled lab and open-source threat intelligence analysis
Purpose: Identify and map real-world adversary TTPs (tactics, techniques, and procedures) to the MITRE ATT&CK framework for red-team simulation and defensive validation.

Objective

Correlate and validate threat actor behaviors from open-source intelligence (OSINT) with MITRE ATT&CK Enterprise techniques, supporting red-team scenario development and defensive coverage assessments.

Data Sources

Source	Description
APT28 (Fancy Bear)	Credential theft and initial access behaviors extracted from public reporting
APT29 (Cozy Bear)	Persistence and command/control TTPs used for long-term network access
MITRE ATT&CK	Baseline mapping framework for TIDs and tactic categorization

---

Methodology

- Parsed OSINT reports and extracted TTPs (T1059, T1555, T1078, T1105, etc.)
- Organized techniques by kill chain phase (Initial Access → Persistence → C2)
- Replicated key behaviors in isolated lab environments to confirm feasibility
- Correlated lab telemetry to defensive detection opportunities in Windows logs and EDR output

Tools & Techniques

Python (report parsing) • MITRE ATT&CK Navigator • Sigma rules • Sysmon telemetry • Elastic Stack

Findings

Category	Observation
Coverage Gaps	Limited telemetry on credential dumping and network discovery (T1003, T1046).
Correlation Needs	Detection logic did not fully align with adversary C2 patterns (T1105, T1071).
Improvement Areas	Blue-team mapping focused heavily on known malware families, not behaviors.

Recommendations

- Integrate ATT&CK mapping into routine threat-hunting and detection engineering workflows.
- Shift detection focus from indicators (hashes, IOCs) to behavioral analytics (process lineage, parent-child relationships).
- Maintain living documentation of threat-to-detection mappings for continuous improvement.

Outcome

Produced **threat-behavior mapping tables** aligning APT28/29 behaviors to ATT&CK techniques. Delivered **briefs and dashboards** summarizing detection priorities and simulation recommendations for future red-team exercises.

> This project bridges threat intelligence with adversary simulation, forming a repeatable workflow for red-blue collaboration and coverage analysis.