MNSEC 2025

SEEING THE UNSEEN: VISUALIZING AND ENRICHING CYBER ATTACK

Nyamjargal.T

WHOAMI

Info Sec Plus LLC

- Information Security Analyst
- Master’s Student, National University of Mongolia (NUM)
- Certified Ethical Hacker (CEH Master)
- Microsoft 365 Enterprise Administrator Expert
- Continuous Learner, passionate about cybersecurity & AI & enterprise solutions

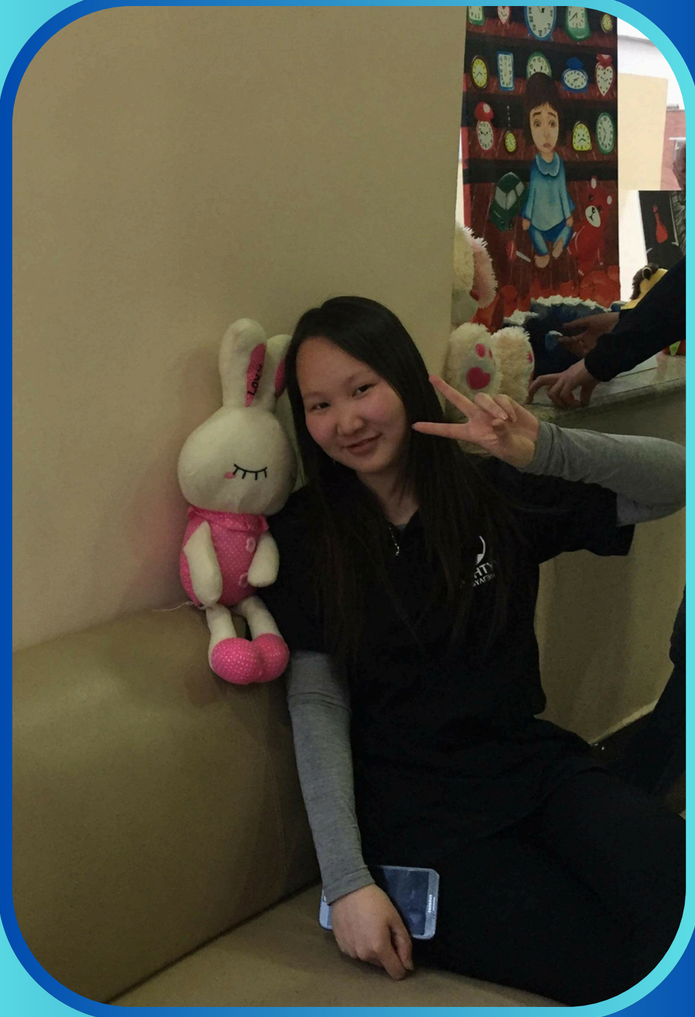
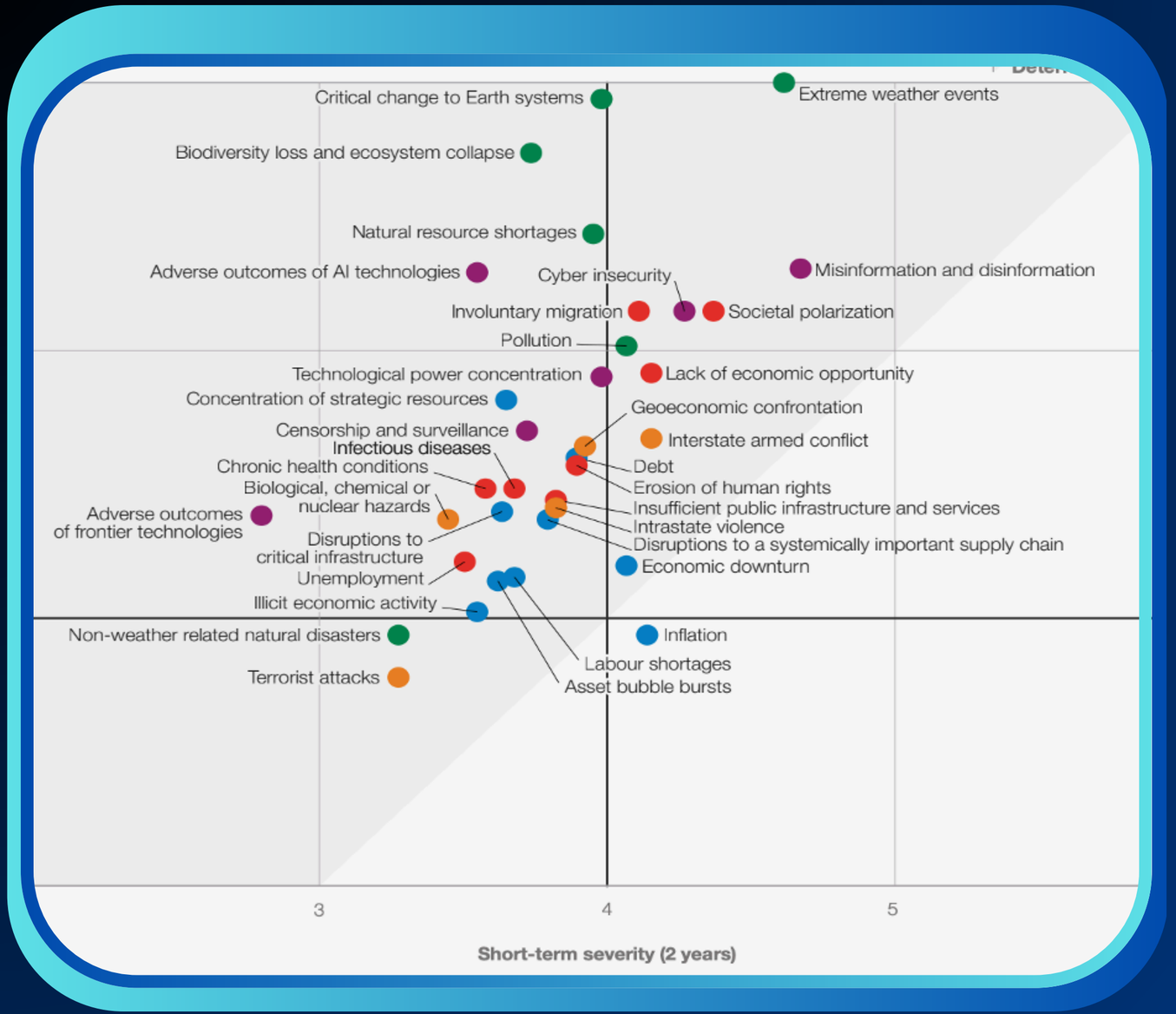


TABLE OF CONTENTS



WHY

The World Economic Forum identifies cyber incidents and their risks as one of the top-ranked risks in the global risk landscape [1].

IBM-Ponemon: Data breach cost increased from $3.86M (2020) to $4.88M (2024) [2].

RISING DATA, RISING RESPONSIBILITIES

- Growing amount of data in organizations
- Multiple responsibilities: collect → process → organize → secure
- Security requires diverse skills: policy, research, analysis, detection, response, improvement

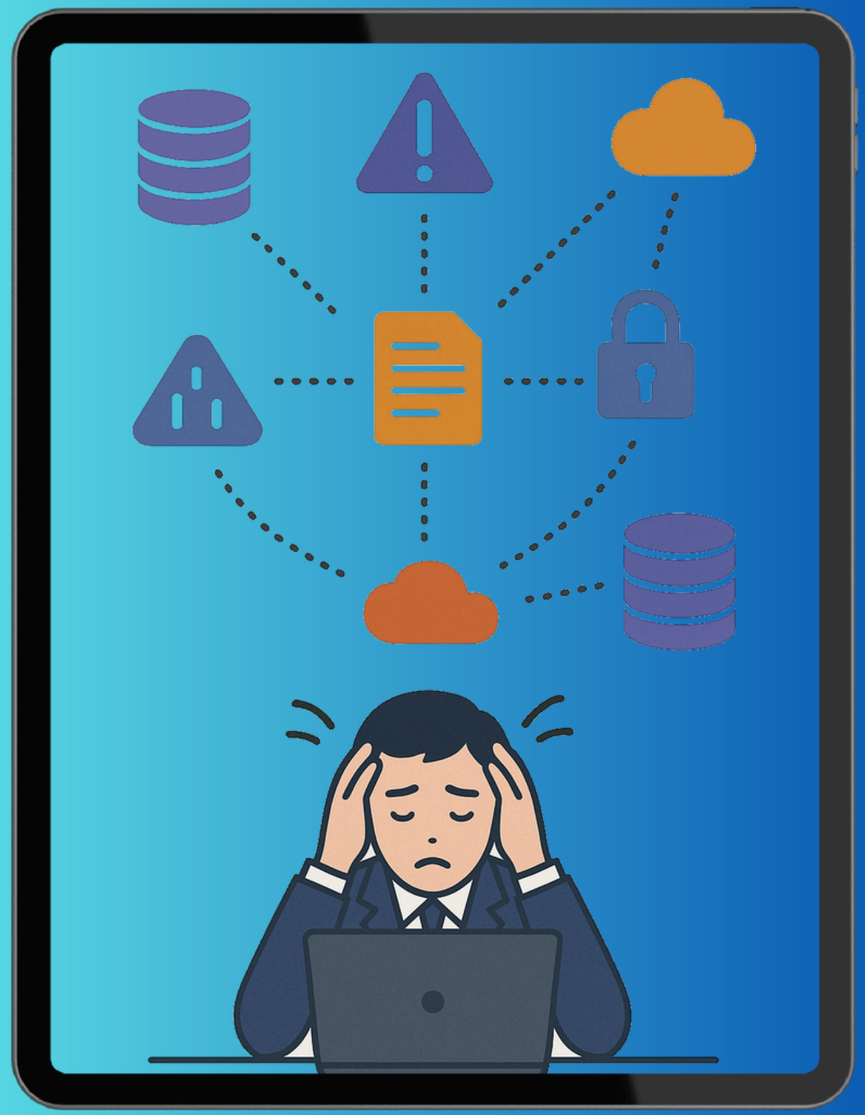
WHY CTI

Timely Response Remains Key

- Real-time detection, analysis, and response reduce breach impact
- CTI = actionable insights on TTPs, threat actors

Proven Benefits

- 40% incident response time
- 50% breach impact

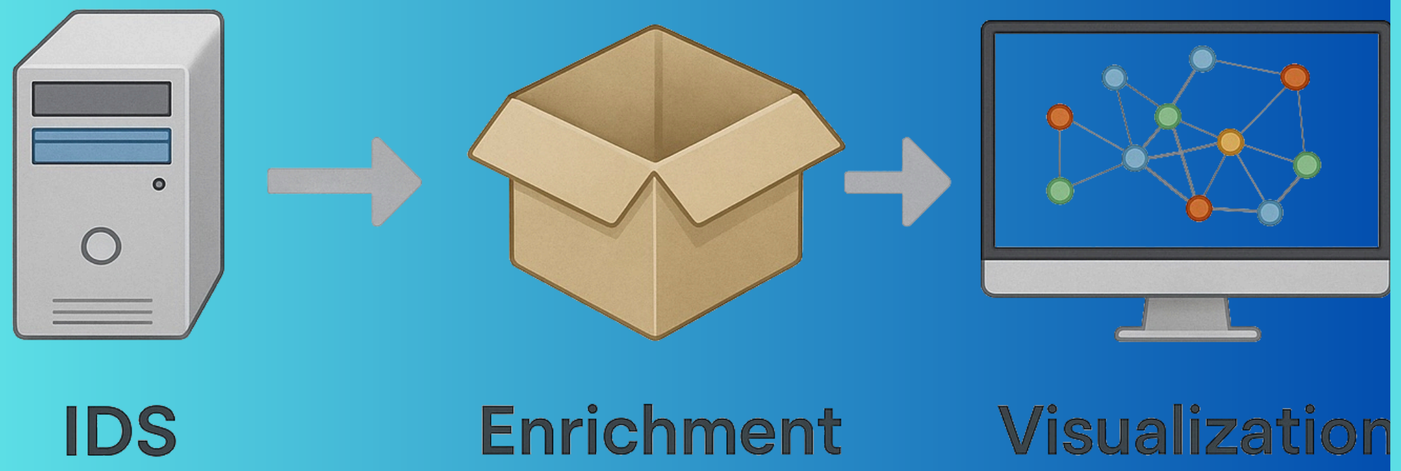


CHALLENGES WITH CTI

- Fragmented CTI data → multiple, unstructured sources
- Limited resources for SMEs → expensive threat intel platforms

Analyst challenges:

- Beyond collection → search + learn + need enrichment + mapping + visualization



RESEARCH OBJECTIVES

- Automate CTI enrichment and visualization
- Integrate IDS alerts with external intelligence
- Provide SOC teams with situational awareness

PROPOSED SOLUTION

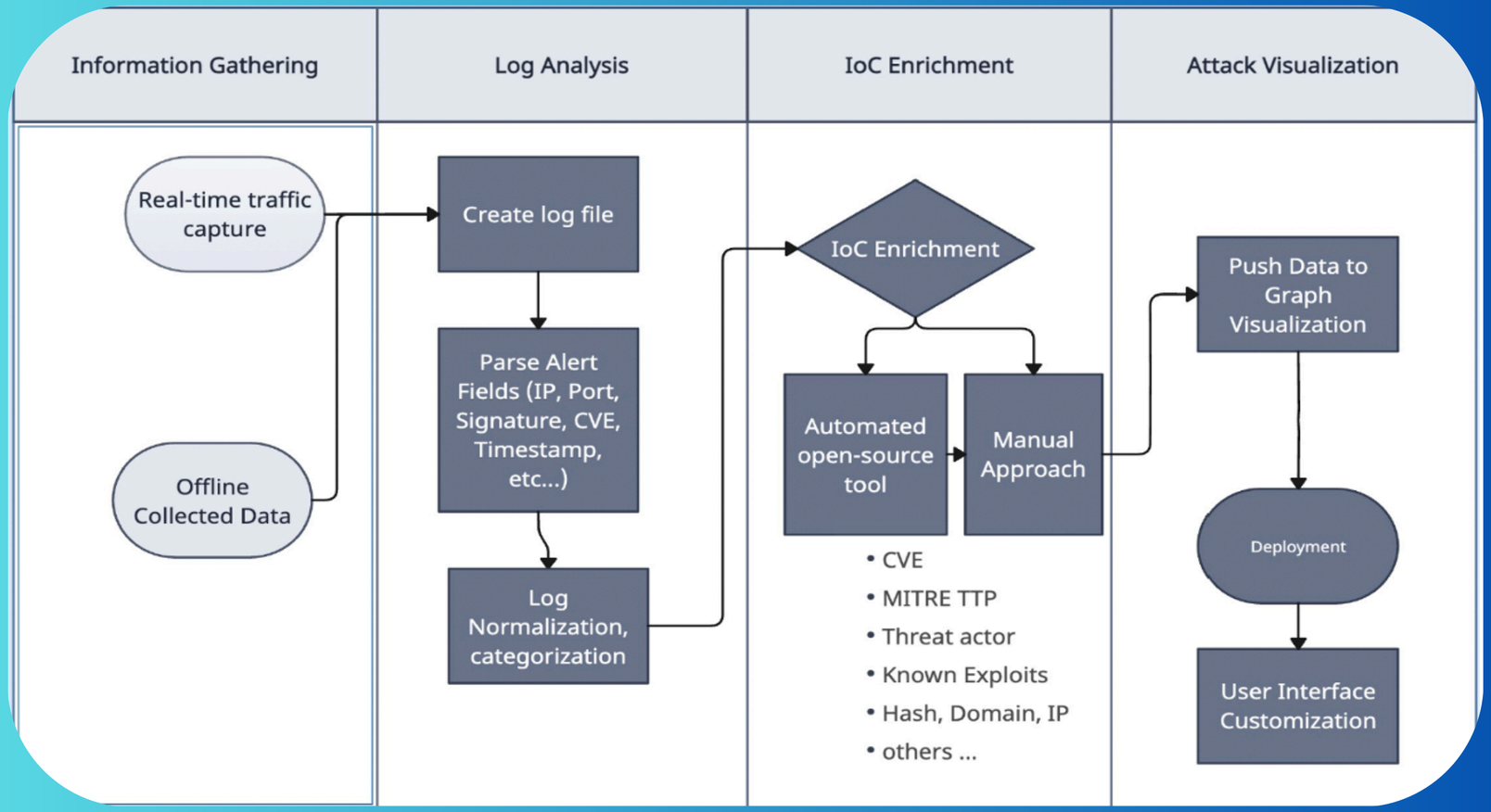


Fig 1. Solution Flow

PROPOSED SOLUTION

- 1. Information Gathering
  - Ingests real-time IDS alerts (e.g., Suricata .eve.json)
  - Offline sources (.pcap, event logs)

```
LOG_FILE = "eve.json"

def load_alerts_to_graph(graph, ip_nodes, sig_nodes, cve_nodes):
```

PROPOSED SOLUTION

- 2. Log Analysis
  - Custom Python parser extracts and normalizes key fields (IPs, ports, CVEs, timestamps)
  - Maps events to MITRE ATT&CK for tactical context
  - Ensures consistency across diverse alert formats
  - Overlaps are handled by deduplicating alerts based on timestamps and IoCs using a Python script that compares hashes of key fields.

```python
def fetch_mitre_ti(mitre_id):
    url = f"https://raw.githubusercontent.com/mitre/cti/master/enterprise-attack/enterprise-attack.json"
    try:
        response = requests.get(url, timeout=5)
        if response.status_code == 200:
            mitre_data = response.json()
            for obj in mitre_data.get("objects", []):
```

PROPOSED SOLUTION

- 3. IoC Enrichment
  - Automated CTI integration (OTX, VirusTotal, CVE/NVD, MITRE, AbuseIPDB)
  - Adds context to IoCs, links to threat actors, campaigns, and techniques
  - Supports manual annotation for deeper insight when needed

```
VT_API_KEY = "
OTX_API_KEY =
```

```
def fetch_nvd_cve(cve):
    url = f"https://services.nvd.nist.gov/rest/json/cve/1.0/{cve}"
    r = safe_get(url)
    if r and r.status_code == 200:
```

```
def fetch_otx_filehash(filehash):
    if not OTX_API_KEY:
        return "[OTX] API key missing"
    url = f"https://otx.alienvault.com/api/v1/indicators/file/{filehash}/general"
    headers = {"X-OTX-API-KEY": OTX_API_KEY}
```

```
def fetch_vt_ip(ip):
    if not VT_API_KEY:
        return "[VirusTotal] API key missing"
    url = f"https://www.virustotal.com/api/v3/ip_addresses/{ip}"
    headers = {"x-apikey": VT_API_KEY}
```

PROPOSED SOLUTION

- **4. Attack Graph Visualization**
  - Uses Tulip to model IPs, CVEs, MITRE TTPs as nodes; relations as edges
  - Timeline-based layout shows attack sequence and lateral movement

```
ef apply_styles(graph):
    label = graph.getStringProperty("viewLabel")
    type_ = graph.getStringProperty("type")
    color = graph.getColorProperty("viewColor")
    size = graph.getSizeProperty("viewSize")
    shape = graph.getIntegerProperty("viewShape")
    border_color = graph.getColorProperty("viewBorderColor")

    node_style_map = {
        "IP": {"color": tlp.Color(0, 200, 100), "size": 18, "shape": tlp
        "Domain": {"color": tlp.Color(255, 165, 0), "size": 16, "shape"
        "Hash": {"color": tlp.Color(200, 80, 200), "size": 14, "shape":
        "Signature": {"color": tlp.Color(255, 80, 80), "size": 20, "shap
        "CVE": {"color": tlp.Color(80, 160, 255), "size": 12, "shape":
        "MITRE": {"color": tlp.Color(200, 80, 255), "size": 14, "shape"
    }
```

```
def create_graph_with_enrichment(event):
    graph = tlp.newGraph()
    graph.setName("Enriched CTI Graph with IP/Domain/Hash")

    label = graph.getStringProperty("viewLabel")
    type_ = graph.getStringProperty("type")
    ti_prop = graph.getStringProperty("TI")
```

CASE STUDY 1

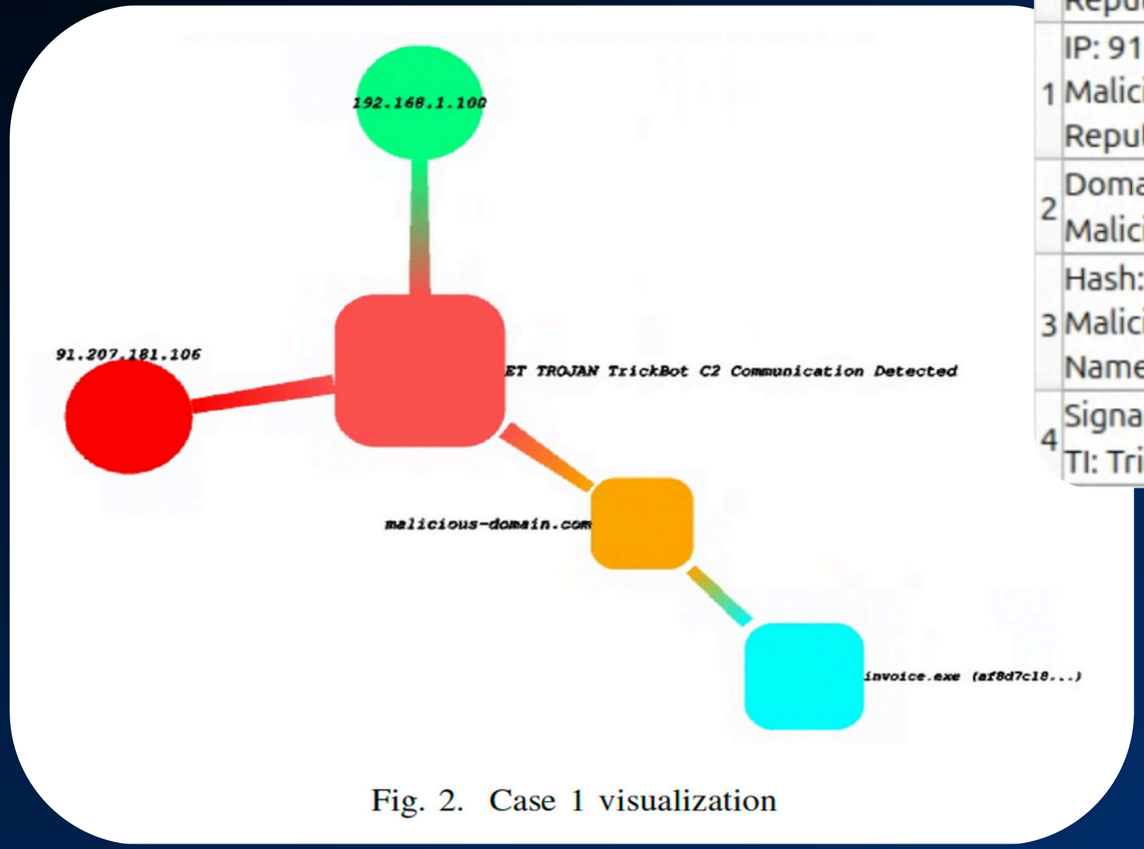


Fig. 2. Case 1 visualization

	TI	type
0	IP: 192.168.1.100 Malicious: 0 Reputation: 1	IP
1	IP: 91.207.181.106 Malicious: 10 Reputation: 0	IP
2	Domain: malicious-domain.com Malicious: 2	Domain
3	Hash: af8d7c18fe97415d7ede0cba166dce004ebbe94eacd1af6f61d8d3527b Malicious: 58 Names: Server.exe, bD0b.exe, unknown, bD0b.bin	File
4	Signature: ET TROJAN TrickBot C2 Communication Detected TI: TrickBot C2 communication detected by Suricata.	Signature

CASE STUDY 2

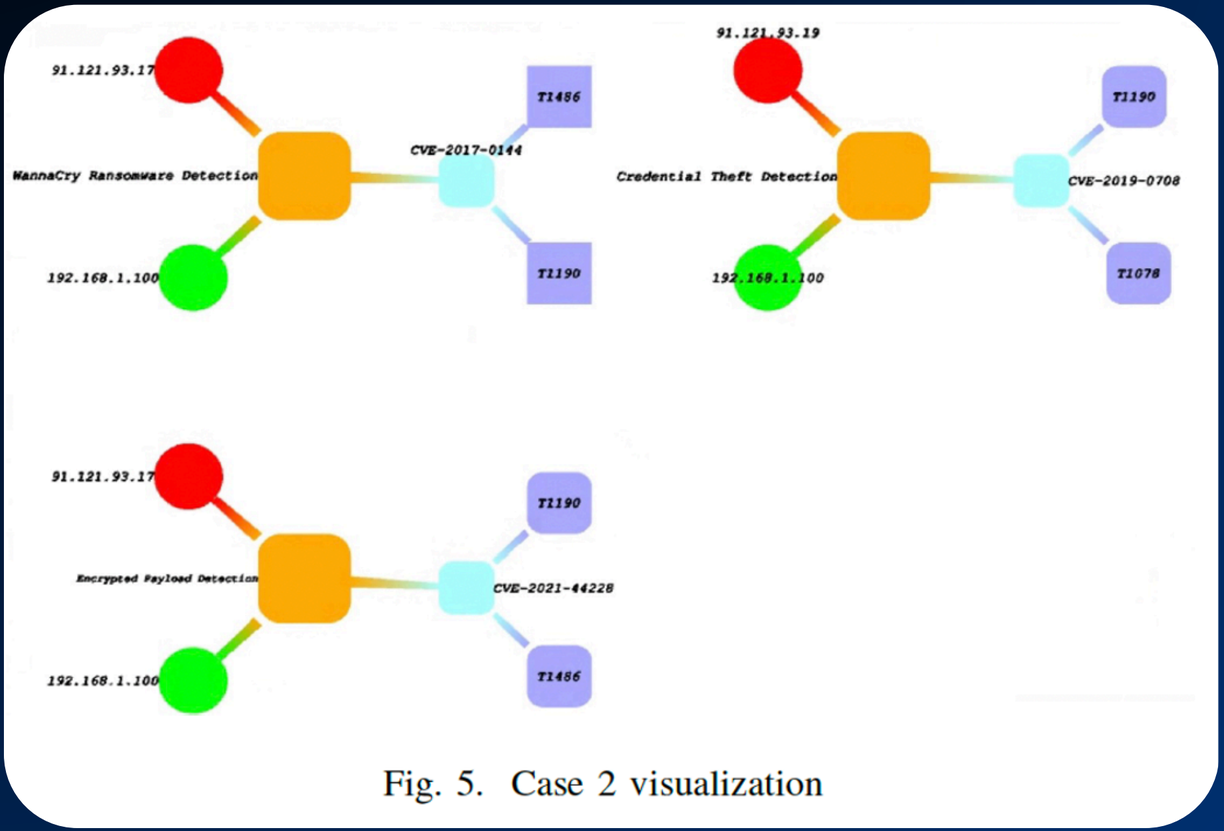


Fig. 5. Case 2 visualization

Fig. 4. Case 2 log file flowchart

CASE STUDY 3

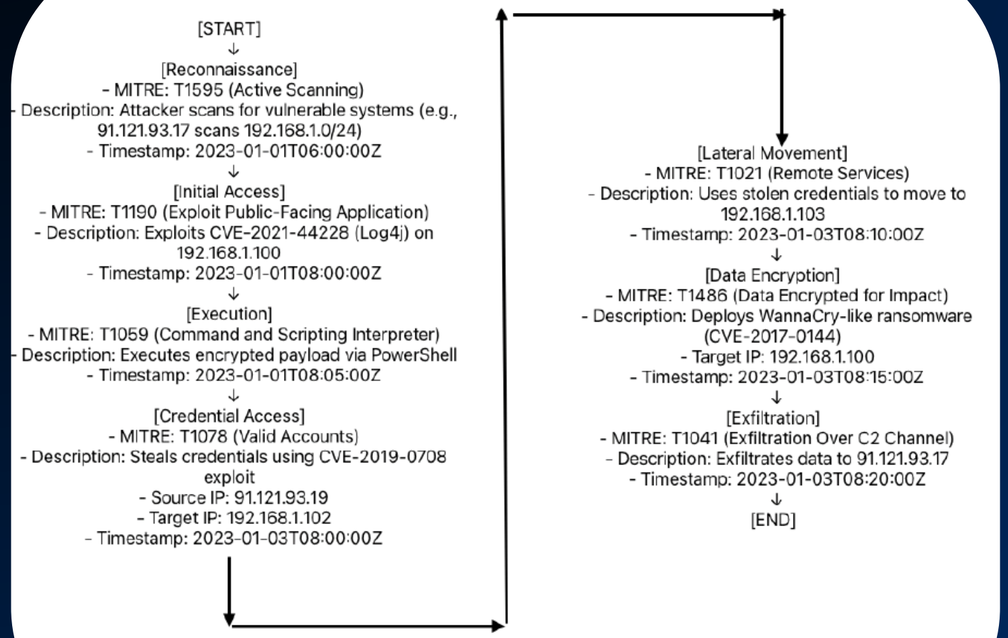


Fig. 6. Case 3 log file flow

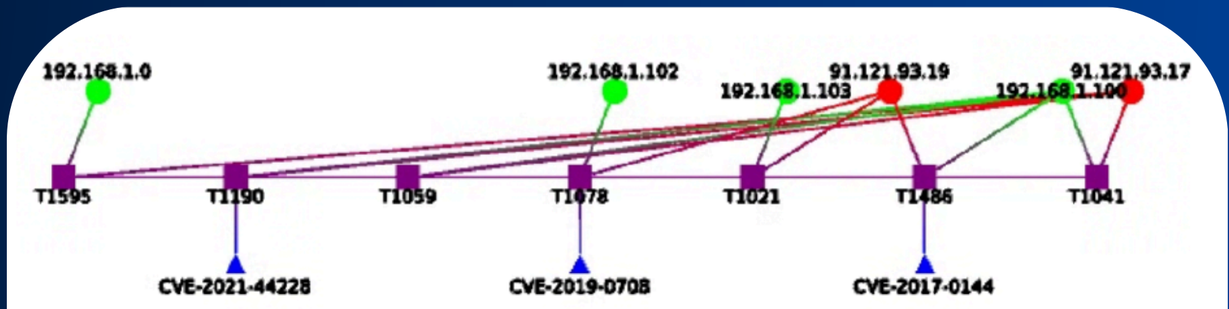


Fig. 7. Case 3 visualization

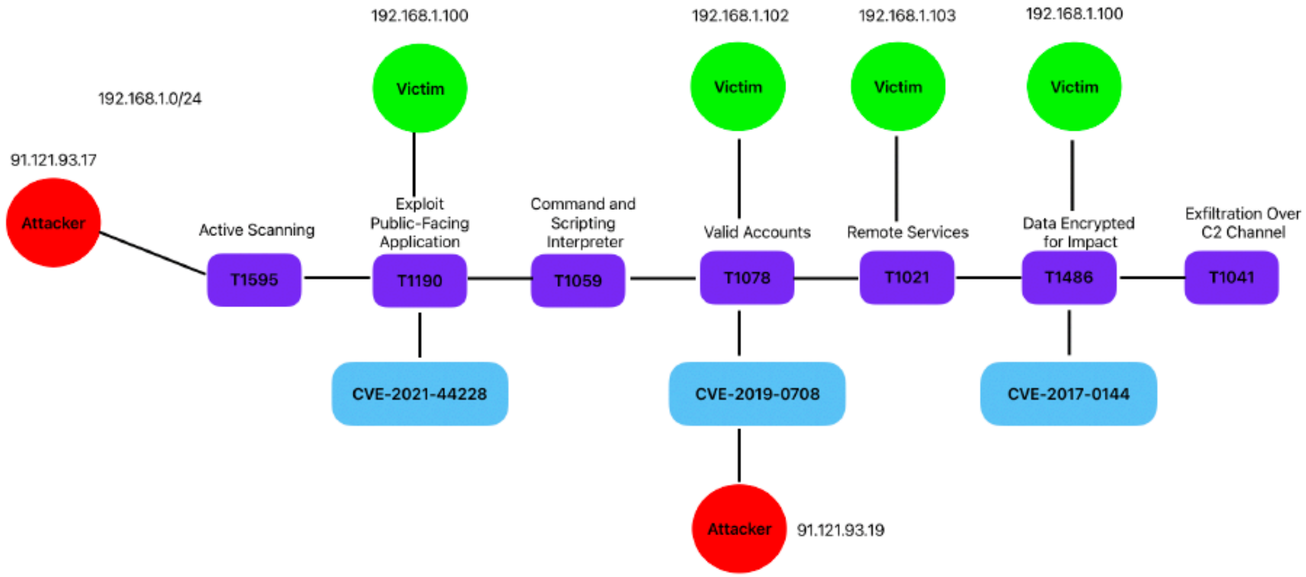


Fig. 8. Case 3 purified and rectified visualization

CONCLUSION

- We developed an automated CTI system integrating IDS alerts, enrichment platforms (e.g., Virustotal, OTX), and graph-based visualization via Tulip.
- The solution transforms raw IoCs into contextualized, time-aware threat intelligence graphs.
- Case studies on ransomware, pivot attacks, and multi-stage scenarios proved its effectiveness and operational value.
- Our system can boosts analyst situational awareness and accelerates incident response across the attack kill chain.

Future Works:

- Test on more types of attacks and alerts
- Develop AI models capable of predicting exploitability
- Collaborative web-based CTI platforms
- Make visibility more convenient

MNSEC 2025

THANK YOU

← Linkedin