IOC Reputation Checker Tool — Cybersecurity Incident Response Report

Author: [Your Name]
Date: November 13, 2025
Organization: Security Operations Simulation Project
Tool: IOC Reputation Checker (Python + Tkinter GUI)

---

1. Incident Response Plan

Purpose

The purpose of this Incident Response (IR) Plan is to outline how cybersecurity analysts (L1/L2) can detect, contain, eradicate, and recover from potential phishing or malware-based threats identified through the IOC Reputation Checker Tool.

1.1. Method for Detecting Security Incidents

Our IOC Reputation Checker automatically analyzes **Indicators of Compromise (IOCs)** such as:

- Malicious domains or URLs
- Suspicious IP addresses
- File hash values from email attachments

It simulates checks used by real SOC tools (e.g., VirusTotal, MXToolbox, AbuseIPDB).
The detection process involves:

- Looking up the IOC in a **local intelligence list** (known safe/suspicious/malicious)
- Simulating technical reasoning (HTTPS presence, domain pattern, known phishing behavior)
- Generating a **reputation verdict**: *Safe*, *Suspicious*, or *Dangerous*

Example:

```
Checked: suspicious-email-login.net
Verdict: Dangerous
```

```
Why: Domain not trusted, lacks HTTPS, and mimics legitimate brand patterns.
```

1.2. Containment Strategy

Once a malicious IOC is identified:

1. **Isolate affected systems** immediately (e.g., disconnect the workstation from the network).
2. **Block the malicious domain/IP** on the firewall or secure email gateway.
3. **Quarantine suspicious emails or attachments** in the mail server.
4. **Add the IOC to the local blocklist** in the tool for future automatic detection.

1.3. Eradication and Recovery Steps

After containment:

1. **Remove or clean infected files** using antivirus or endpoint protection software.
2. **Reimage systems** if malware persists.
3. **Restore from backups** verified to be clean.
4. **Monitor the network** for further communication attempts with malicious hosts.
5. **Conduct post-incident review** using the generated PDF report from the IOC Checker.

1.4. Identified Attack Type

Attack Type: *Phishing (with possible malware attachment)*

- Attackers use fake email domains and login pages to steal credentials.
- IOC Checker assists analysts in verifying the legitimacy of these URLs or file hashes.

2. Comprehensive Security Policy

2.1. Overview

This policy ensures consistent cybersecurity practices that protect confidentiality, integrity, and availability (CIA) within the organization.

2.2. Key Security Rules & Guidelines

1. **Email Safety:** Employees must not open attachments or links from unverified senders. All suspicious emails should be analyzed using the IOC Reputation Checker.
2. **Access Control:** Use least privilege principles. Accounts with administrative privileges must use MFA.
3. **Incident Reporting:** Any detected malicious IOC must be reported to the SOC team immediately and logged for further review.

2.3. Incident Response Integration

In case of a confirmed phishing or malware attack:

- Analysts will activate the IR Plan (detection → containment → eradication → recovery).
- All logs, screenshots, and generated IOC Checker reports are archived for forensic review.

2.4. CIA Triad Justification

CIA Principle	Enforcement Example
Confidentiality	Encryption of sensitive email data and secure storage of reports.
Integrity	Hashing (SHA256) ensures that file attachments or reports are unmodified.
Availability	Regular system backups ensure continuous operation during incident recovery.

3. Encryption Demonstration

The following example demonstrates encryption and hashing techniques aligned with SOC practices.

3.1. AES Encryption Example (Simulated Output)

Plain Text: `Sensitive login credentials`
AES Encrypted Text: `b3cfb0934f7d42d8a4e2a1c95b33d60f`
Decrypted Text: `Sensitive login credentials`

3.2. Hashing Example

Text: `malicious_attachment.exe`
MD5 Hash: `d41d8cd98f00b204e9800998ecf8427e`
SHA256 Hash: `5d41402abc4b2a76b9719d911017c592`

Hashing allows analysts to quickly compare file integrity or match known malware signatures from threat databases.

---

4. Legal and Ethical Compliance

4.1. Relevant Laws and Regulations

1. **General Data Protection Regulation (GDPR)** — Ensures that all user data and reports are stored securely, and personally identifiable information (PII) is protected.
2. **Computer Fraud and Abuse Act (CFAA)** — Prevents unauthorized access or testing of systems without permission.

4.2. Ethical Considerations

- **Data Privacy:** Analysts must not access or share data unrelated to the investigation.
- **Responsible Disclosure:** If new threats or vulnerabilities are discovered, they should be reported responsibly to affected parties.

4.3. Compliance Summary

The IOC Reputation Checker adheres to these standards by:

- Storing only **non-personal indicators** (domains, URLs, hashes).
- Providing analysis without exposing user data.
- Generating reports suitable for **legal and forensic documentation**.

5. Conclusion

The **IOC Reputation Checker Tool** is an educational yet practical cybersecurity utility that simulates real SOC operations.
It automates the verification of suspicious indicators, provides technical context, and generates formalized reports for analysts.
By aligning with recognized cybersecurity frameworks and legal guidelines, it supports both **learning outcomes** and **real-world analytical workflows**.

Appendix – Future Feature Enhancements

- Integration with **VirusTotal API** for real threat intelligence.
- **SSL certificate validation** and domain age checks for enhanced accuracy.
- **Automated email header parsing** for phishing detection.
- **Dashboard analytics** summarizing the day’s IOC scans and trends.

End of Report