| **Indicator** | **Example** | **First Resources** | **Associated IOA or TTP Examples** |
| --- | --- | --- | --- |
| **IPv4 / IPv6** | 45.155.205.3 | • WHOIS (ASN, allocation date) · VirusTotal Relations· Shodan banner scan | IOA: Repeated SSH failures TTP: T1110.003Password Guessing |
| **Domain / FQDN** | malicious-updates[.]net | • WHOIS age · RiskIQ or SecurityTrails passive-DNS · urlscan.io | IOA: surge of DNS queries to a 24-hour-old domain |
| **URL** | hxxp://malicious-updates[.]net/login | • URLhaus reputation · urlscan.io behaviour graph · Any.Run dynamic run (network off) | IOA: Browser POST to /gateway.php with payload |
| **File hash** | e99a18c428cb38d5… | • VirusTotal static & dynamic · Hybrid-Analysis · MalShare corpus | TTP: T1055 Process Injection into regsvr32.exe |
| **E-mail address** | billing@evil-corp.com | • MXToolbox header analysis • Have I Been Pwned | IOA: SPF failure plus recent domain registration |
| **Local artefact** | HKCU\Software\Run\updater.exe | • Sigma rules · EDR prevalence query · Vendor knowledge bas | TTP: T1060.001 Registry Run Keys |

Intro to Cyber Threat Intel

## 📓 **Notes – Intro to Cyber Threat Intel**

**Lab Name:** Intro to Cyber Threat Intel

**Summary:**  
This lab introduces the concept of **Cyber Threat Intelligence (CTI)** — the process of collecting, analyzing, and sharing information about current and potential threats. CTI helps SOC analysts proactively detect and respond to attacks by understanding the threat landscape and adversary behavior.

**Key Concepts Learned:**

* **Types of CTI:**
  1. **Strategic** – High-level, long-term threat trends for executives.
  2. **Operational** – Information about specific attacks or campaigns.
  3. **Tactical** – Technical indicators (IOCs like IPs, hashes) for security tools.
  4. **Technical** – Raw technical data like malware samples or exploit code.
* **Sources of CTI:**
  1. Open-source intelligence (OSINT)
  2. Commercial feeds
  3. Industry sharing groups (ISACs)
  4. Threat intel platforms (MISP, OpenCTI)
* **Benefits for SOC Analysts:**
  1. Enriches SIEM alerts with context.
  2. Helps prioritize threats based on relevance.
  3. Enables detection of attacker TTPs earlier in the kill chain.

**Practical Takeaway:**

* Integrating CTI into SOC operations improves accuracy and speed of investigations.
* Focus on relevance — not all threat intel applies to your environment.

