Cyber Threat Intel

It is a process to give a context to the analyst of the events going on by connecting the dots to identify the threats and deal with on the basis of the type of threat it is and accordingly take decisions to solve the situation.

```
In concrete terms, CTI seeks to answer three essential questions:

1. Who, or what, is on the other end of this alert indicator?
2. What was their behaviour in the past?
3. How does my organisation respond, and what should I do about it right
now?
```

Connection of dots....

Layer	Definition	Alert-queue example	SOC L1 action
Data	An unprocessed observable	`45.155.205.3 :443`	Capture the artefact.
Information	Data plus factual annotation	*IP registered to Hetzner, first seen 2023-07-14*	Record attributes.
Intelligence	Analysed information that answers *so-what*	*IP belongs to the current BumbleBee C2; block immediately*	Escalate or suppress.

- **IOC (Indicator Of Compromise)** : It is a sequence of events that occurs or we can say that they are the evidence of breach e.g. C2 address in the logs.
- **Indicator of Attack (IOA)**: A malicious action, such as PowerShell launching an unknown service, is underway.
- **Tactics, Techniques, and Procedures (TTP)**: An adversary's detailed methodologies expressed in MITRE ATT&CK IDs and descriptions.

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: `T1110.003` Password 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

---

IPv4 : WHOIS (asn ,allocation date) , Virustotal , Shrodan banner Scan
Domain :WHOIS age · RiskIQ or SecurityTrails passive-DNS · urlscan.io
URL: URLhaus reputation · urlscan.io behaviour graph · Any.Run dynamic run (network off)
File Hash : VirusTotal static & dynamic · Hybrid-Analysis · MalShare corpus
E-mail address: MXToolbox header analysis • Have I Been Pwned

Platform: A structured repository that stores indicators, tracks enrichment, maps relationships, and enforces sharing permissions. MISP and OpenCTI are leading open-source examples.

- **Internal telemetry:** SIEM logs, EDR detections, phishing-mailbox submissions provide the highest immediate relevance.
- **Commercial services:** Vendor premium feeds, paid sandboxes**,** and closed-source analytics. These provide high fidelity, but may have export and sharing limits based on licensing.
- **Open-source intelligence (OSINT):** AbuseIPDB, URLhaus, public blogs with IOCs, and academic research. Before applying, information from these sources will need to be cross-confirmed.
- **Communities & ISACs:** Sector-specific lists marked with labels and rich context (e.g., FS-ISAC)

Threat Intelligence Classifications

Threat intelligence is geared towards understanding the relationship between your operational environment and your adversary. With this in mind, we can break down threat intel into the following classifications:

- **Strategic intel**: High-level intelligence that looks into the organisation's threat landscape and maps out the risk areas based on trends, patterns and emerging threats that may impact business decisions. An example is an annual ransomware trends report predicting a shift to data-wiping extortion in healthcare.
- **Tactical intel**: Assessments of adversaries' behaviours through analysis of tactics, techniques, and procedures (TTPs). This can be in the form of Advisory notes, such as detailing new T1059.005 (Visual Basic) abuse in malspam.
- **Operational intel**: Campaign-specific details about the motives and intent to perform an attack. This is useful for understanding the critical assets available in the organisation (people, processes, and technologies) that may be targeted.

- **Technical intel**: Atomic indicators and artefacts such as IPs and hashes related to an attack.

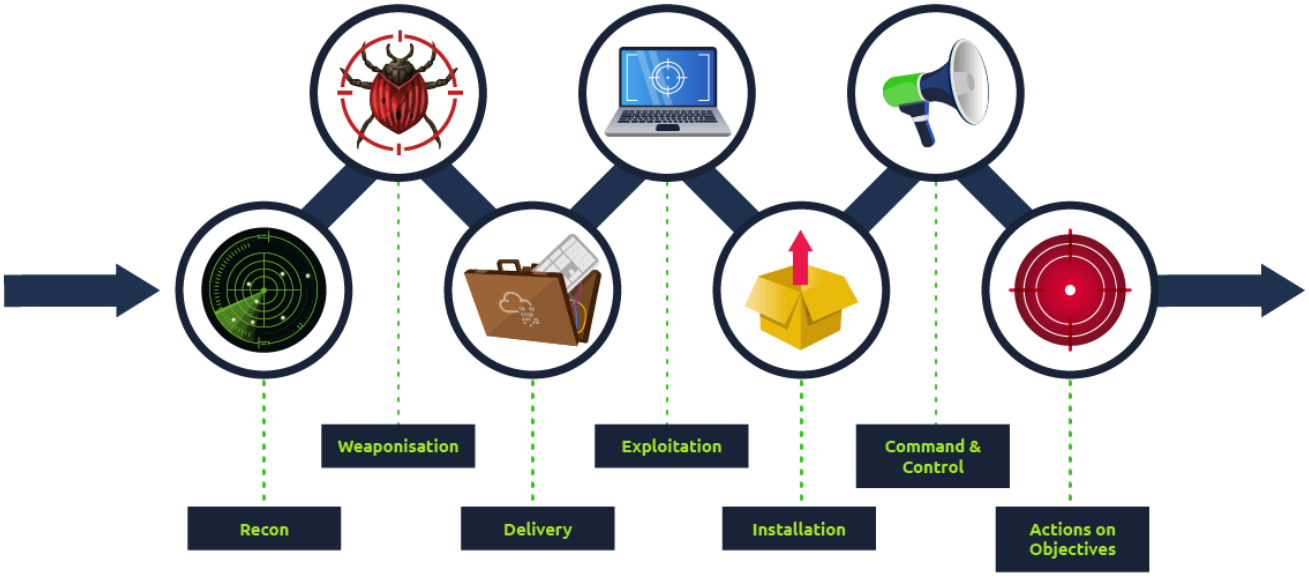
Threat Intel Life Cycle

- **Planning & Direction** : This is were the stakeholders will define the requirements, like what assets are critical , what threats to monitor and what decision the threat intel should support.
- **Collection :** This is where we will be collecting all the raw logs from various places like like firewalls , EDR , endpoint devices , OSINT , dark web all this things are collected .
- **Processing**: This is were we will be taking the logs from various platforms and normalizing it so that it can be visualized and reduce the noise from the logs that are been or data that is been provided.
- **Analysis**: This is were from the processing we try to connect the dots and understand the events which will make us understand the steps taken by the threat actor or the kind of communication taking place to segregate it as a true positive or a false positive .
- **Dissemination**: Then after all the analysis we will be creating the documentations and reports involving the graphs , pie charts and all the required presentation which will be given to the stake holder to make them understand about the threat effectively and efficiently .

- **Feedback:** This is were we will be getting the improvements and make sure that we will enhance the security .

CTI Standards and Frameworks

- MITRE ATT&CK
- MITRE D3FEND : **D3FEND** catalogues how defenders respond. Each entry maps to defensive tactics such as Credential Hardening or Data Obfuscation.
- Cyber Kill Chain : This breakdown helps analysts and defenders identify which stage-specific activities occurred when investigating an attack. The phases defined are shown in the image below.



CVE , CVSS , NVD

CVE : Common Vulnerabilities and Exploits are the set of database for all the known vulnerabilities which are been known now or we can say discovered .

CVSS: This is were we will be having the score for the vulnerabilities based on the potential of damage it has it ranges from 0-10 .

NVD : National Vulnerability Database it's a repo that links CVE numbers to the scores , exploits and affected products .

File and Hash Threat Intel

File Path Analysis

- `C:\` (System drive) can be a common target for persistence mechanisms.
- `C:\Users\Public` profile can enable cross-user access of detonated adversary tools.

- `C:\Users\Public\Public Downloads` provides a high-traffic directory that would often evade strict monitoring.
- Utilizing temporary directories such as `C:\Windows\Temp\` for ephemeral payloads.
- Placing payloads in writable system paths, such as `C:\ProgramData\` for stealth persistence.

Filename Heuristic Indicators

Attackers are also known to modify filenames to escape detection through implementing various types of heuristic indicators, including:

- **Double extensions** - An example of this would be `invoice.pdf.exe`, which leverages default Windows settings that hide file extensions.
- **System binary impersonation** - A filename such as `scvhost.exe` abuses the user's familiarity with core system processes. Defenders should include legitimate locations for system processes in an allow list, rather than standalone filenames.
- **High-entropy Strings** – A filename such as `jh8F21.exe` suggests automated packing or polymorphic generation, which is commonly used in a high-churn phishing operation.
- **Masquerading** - Filenames such as `backup-2300.exe` can blend with routine files, thus leveraging on reduced suspicion. Another example is a single character substitution, which can bypass detection while looking visually legitimate to an unsuspecting employee.

File Hash Lookup

1. If found a file that looks malicious so make sure to take hashes of the file found.

```
Use the tools like:

sha256sum bl0gger.exe
Get-Filehash -Algorithm SHA256 bl0gger.exe

which will give you hashes
```

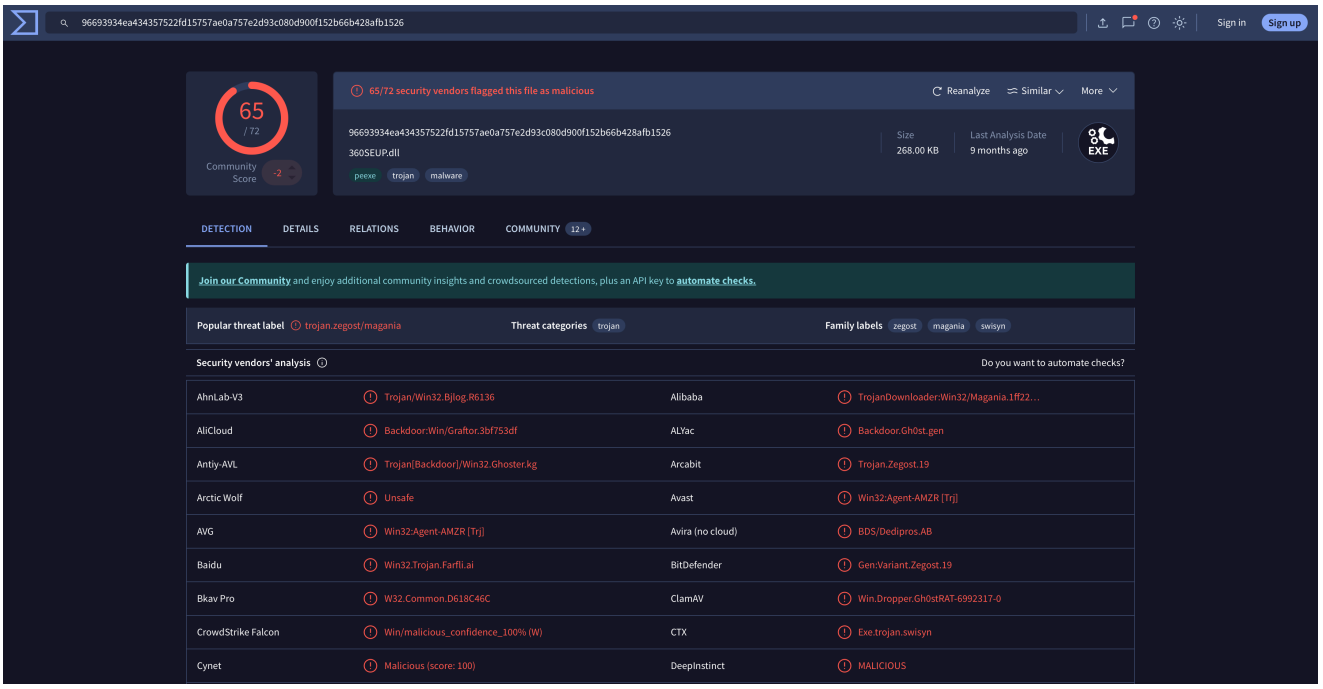
2. Analysis with VirusTotal

```
Using VirusTotal, we can obtain information about our file using the SHA256
hash. Navigate to the website, enter the hash in the search and observe the
file's detection details.
```

here are several items from the search results that would be worth taking note of. These include:

- **Detection score**: This represents a crowdsourced security verdict from various vendors displayed as a ratio. The higher the number, the higher the confidence threat.

- **Threat labels and categories**: These are vendor-specific classifications of the threat, which help confirm the threat's attribution among vendors.
- **Detection rules**: These are the technical signatures used by AV engines to identify threats. Typical classifications are YARA rules, Heuristic patterns, and behavioral triggers.
- **Properties**: This is where the core metadata about the file is found, including the file type, size, and compiled timestamp.
- **Contained domains and IPs**: This information covers the malware's network infrastructure.
- **Contained files**: This section details any files embedded or dropped during the malware's execution.



We can break down the process above into granular steps that ensure VirusTotal becomes a tactical threat intelligence platform for the SOC to pivot towards actionable defense measures.

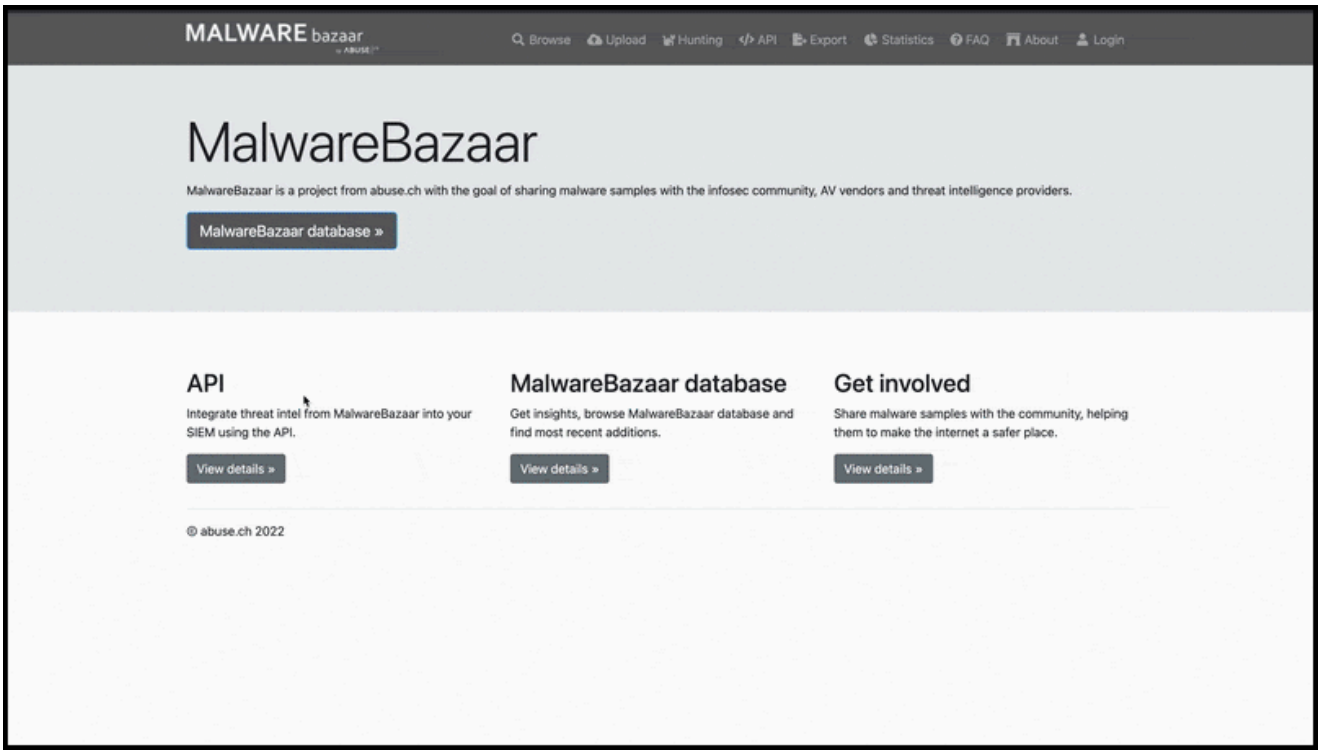
We will be checking for the following things in the Virustotal for the file.

Detection Score and Threat Labels	How many vendors detect this file as malicious?	• Five or more solid vendors flag it • Conflicting classifications (e.g., "Trojan" vs "PUA") • No consensus among the top 3 vendors	• New malware often has low initial detection • Recheck after 24h for updated results • Look at the classification of the malware family name or capability name
Upload Time	When was the file first submitted?	• Uploaded seven days ago with more than 10 detections • Sudden detection spike after days/weeks	• Vendors need 48-72 hours for full analysis • Historical detection growth indicates malware ageing
Signatures	Is the file properly signed?	• Invalid/missing certificate • Certificate issued to an unrelated entity	• Even valid certs can be stolen/abused • Check cert chain expiration dates
Properties	Are there anomalies in the file data?	• Compile timestamp at odd hours (e.g., 3 AM) • High entropy (>7.5) in non-media files	• Some legitimate packers (UPX) increase entropy • Compare with known-good versions

Relations	What infrastructure does the malware connect to?	• Known-bad IPs in VirusTotal's graph • DGA-like domains (e.g., xk8f92.xyz)	• Legitimate CDNs may host malware • Check IPs in Shodan for open ports
Behavioral	What post-execution actions occur?	• Modifies critical registry keys • Attempts process injection	• Some admin tools modify registries legitimately • Correlate with endpoint logs

Cross-Reference With MalwareBazaar

- **Malware Samples Upload:** Security analysts can upload their malware samples for analysis and build the intelligence database. This can be done through the browser or an API.
- **Malware Hunting:** Hunting for malware samples is possible through various elements, such as :
  - **Malware Family tagging:** You will find files classified by their malware families. An example of this use is a file with only 5/70 detections on VirusTotal, but tagged as `#IcedID` in MalwareBazaar, should be treated as malicious.
  - **YARA rule integration:** Many submissions will include rules that detect related samples. As an analyst, you should take note of these rules to be added to the EDR/SIEM for future hunting.
  - **Campaign attribution:** Tags such as `#TA551`, which belong to a threat actor group, help link observed incidents to known adversaries. This can help identify coordinated attacks against an environment.
  - **Sample Availability:** Malware samples are available for download and analysis. Reanalysing samples in a sandbox is best practice, which we shall cover in the next task.



IP and Domain Threat Intel

DNS Checks

The **Domain Name System (DNS)** is like the internet's phonebook. It converts easy-to-remember website names (like *www.tryhackme.com*) into IP addresses that computers use to communicate.

Because DNS sits at the center of internet traffic, attackers often misuse it. They create malicious domains to host malware, control infected systems, or run phishing campaigns.

For security analysts, DNS data is extremely valuable because it provides **early warning signs** of attacks. Suspicious domains often appear in alerts before we even know the malware file or payload hash.

Attackers frequently:

- Register new domains quickly
- Change their IP addresses often
- Abandon domains once detected

So our job is to investigate a domain and add context, such as:

- Who registered it?
- Which IPs it resolves to?
- How often those IPs change?

- Whether its behavior looks legitimate (like a CDN) or suspicious (temporary attacker infrastructure)?

Core DNS Records for Triage

When you enrich a domain, these are the records that matter most:

When investigating a domain, analysts check a few key DNS records to understand if it's suspicious or normal.

A / AAAA Records (IP Mapping)

- These records map the domain to IP addresses.
- **A = IPv4**, **AAAA = IPv6**.
- If the domain keeps resolving to many different IPs (rapid rotation), it can be suspicious.
- Analysts often copy the IP and check it on threat intel platforms (like VirusTotal).

NS Records (Nameservers)

- Show which servers manage the domain's DNS.
- Recently changed or unusual nameservers may indicate a newly created attacker domain.
- For L1 triage, just note the provider (no deep investigation needed).

MX Records (Mail Servers)

- Define which servers handle the domain's email.
- Attackers configure MX records for phishing campaigns.
- If the alert is web-related, just record whether MX exists or not.

TXT Records (SPF / DKIM / Verification)

- Store email security settings and verification tags.
- Missing or weak SPF/DKIM can increase phishing risk.
- Mostly relevant for email investigations.

SOA Record (Start of Authority)

- Identifies the primary DNS authority for the domain.
- Includes admin/contact and serial number.
- Helps build basic ownership context.

TTL (Time To Live)

- Shows how long DNS responses are cached.
- Very low TTL (seconds/minutes) = frequent IP changes → suspicious indicator.

Attack Techniques Using DNS

1. Fast Flux Hosting

- The domain keeps changing its IP address very quickly.
- Uses many IPs with very short TTL (cache time).
- Purpose: Avoid blocking and stay online even if some servers are taken down.

What analysts do:
Record the rotating IPs and escalate the domain as suspicious.

2. CDN Abuse

- Legitimate CDNs (like Cloudflare or Akamai) also rotate IPs.

- But their IPs usually stay within the same provider network (ASN).

How to judge:

- If IPs belong to a major CDN → likely normal.
- Still perform reputation and ownership checks.

3. Typosquatting

- Fake domains that look like real brands.
- Small spelling tricks fool users.

Examples:

- `paypa1.com` (1 instead of l)
- `micros0ft.net` (0 instead of o)

Risk: Phishing, credential theft.

Action: Treat as high risk and escalate.

4. IDN Homograph Attacks (Unicode Abuse)

- Uses special Unicode characters to create look-alike domains.
- Appears normal to humans but different technically.

Example:

- `xn--ppaypal-3ya.com` → Punycode format
- Decodes to a fake PayPal look-alike

What analysts do:

- Decode Punycode using online tools.
- Compare with real brand domains.

IP Enrichment Within the SOC

In most **SIEM or EDR alerts**, you will see at least one IP address.

But an IP alone doesn't tell you much.

It could belong to:

- A hacked home router
- A cloud server (AWS, Azure, GCP)

- A CDN edge node
- A real attacker C2 server

So if we react without checking, we might:

- Block legitimate services (business impact)
- Ignore real threats (security risk)

That’s why we do **IP enrichment**.

What is IP Enrichment?

IP enrichment means adding context to an IP so we can make the right decision.

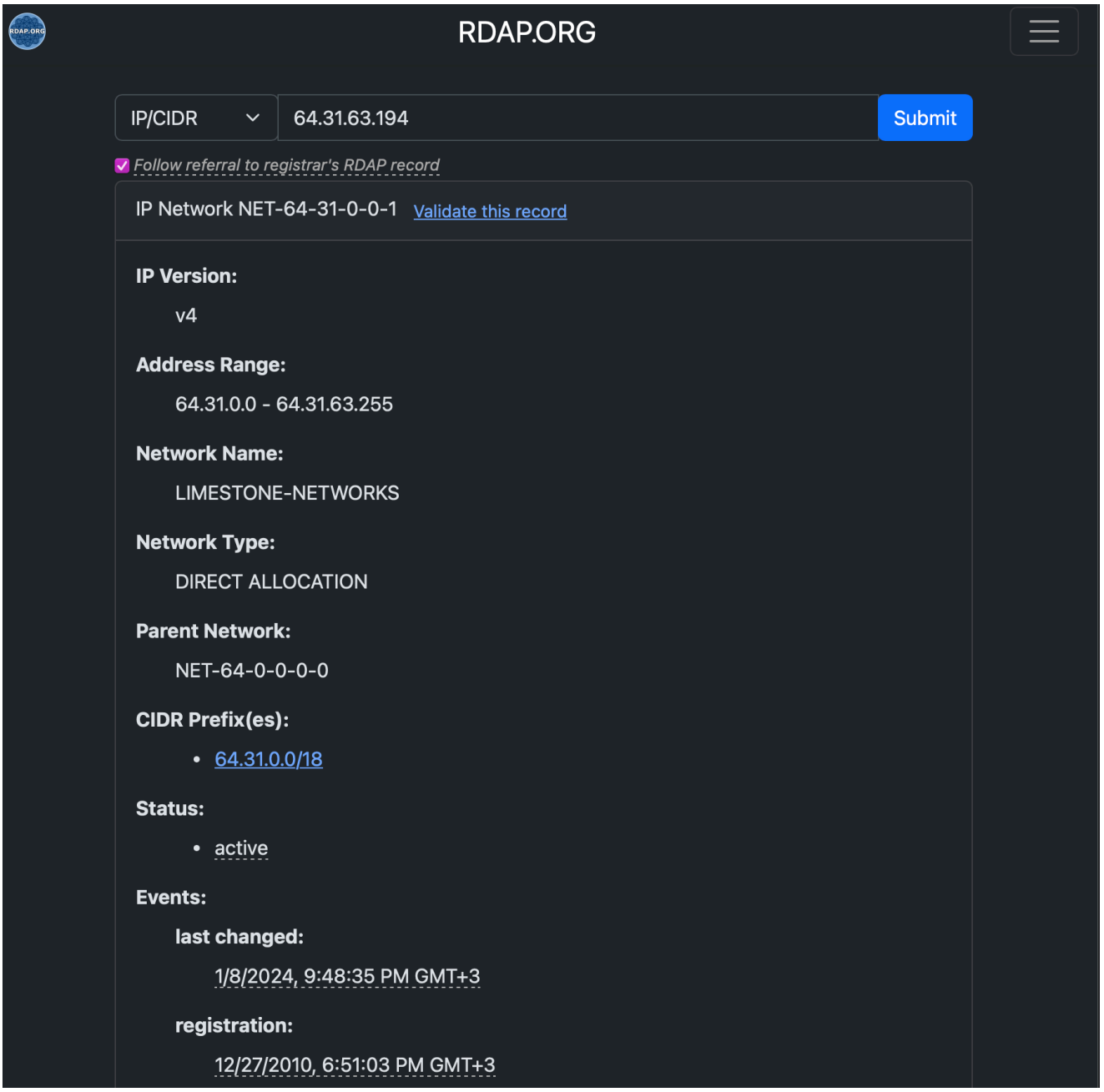
We look for:

- Owner (company or ISP)
- ASN (network provider ID)
- Geolocation (country/city)
- Service type (hosting, broadband, mobile)

This helps us understand:

Is this normal infrastructure or attacker infrastructure?

The Role of RDAP



RDAP = Registration Data Access Protocol

It is the **official source** for IP ownership data.

Maintained by Regional Internet Registries (RIRs), such as:

- RIPE NCC → Europe
- ARIN → North America
- APNIC → Asia Pacific

RDAP is more reliable than **GeoIP** tools because it shows who actually owns the IP block.

What Information RDAP Gives

When you search an IP in RDAP, you get:

1. NetRange

The range of IPs assigned.

Example:
`64.31.0.0 – 64.31.255.255`

Shows the full block ownership.

2. Organisation

Who owns the IP block.

Examples:

- Amazon AWS
- Microsoft
- Vodafone
- Cloudflare

This helps decide legitimacy.

3. Remarks / Description

Explains how the IP range is used.

Examples:

- Cloud hosting
- Residential broadband
- Mobile network
- Data center

4. Abuse Contact

Official email for reporting incidents.

Example:
`abuse@provider.com`

Used for takedown or investigation.

Example Investigation

Let's say your alert shows this IP: `64.31.63.194`

Step 1 — Check RDAP

You find:

- **Org**: Hosting Provider
- **Remarks**: VPS / Cloud hosting
- **Country**: US

Step 2 — Analyst Thinking

Cloud hosting IPs are high risk because attackers rent servers there.

So you pivot to:

- Domains hosted on the IP
- SSL certificates
- Malware reports

Pivoting (Next Investigation Steps)

If traffic looks suspicious, investigate further:

- Which domains resolve to this IP?
- Any malicious certificates?
- Seen in malware campaigns?

This narrows scope from **IP → attacker infrastructure**.

Evidence Preservation

Always save RDAP results as proof.

Best practice:

- Export raw RDAP JSON
- Attach to ticket/case

Why?

Because:

- Data may change later
- Hosting ownership may rotate

Preserving raw data keeps audit integrity.

Autonomous Systems (ASN) & Heuristics

What is an Autonomous System (AS)?

An **Autonomous System (AS)** is a large network owned and managed by one organization.

Each AS has a unique number called an **ASN (Autonomous System Number)**.

Think of it like this:

> **ASN = Network owner ID**

It tells us which company controls that IP range.

Why ASN Matters in SOC Investigations

When you see a suspicious IP, checking its ASN helps you understand:

- Who owns the network
- What type of infrastructure it is
- How risky it might be

This helps avoid wrong decisions like blocking legitimate services.

Types of ASNs Analysts Commonly See

1. Hosting Provider ASNs

Examples: Small hosting companies, VPS providers.

Characteristics:

- Many small IP ranges
- Servers rented by different customers
- High attacker abuse rate

Risk level: 🔴 High

Attackers often host:

- Malware servers
- Phishing sites
- C2 infrastructure

2. Residential ISP ASNs

Examples: Vodafone, Airtel, Jio, Comcast.

Characteristics:

- Huge IP ranges
- Used by home users
- Dynamic IP allocation

What alerts mean:

Usually indicates:

- Compromised home router
- Infected laptop/IoT device

Not attacker infrastructure — just infected users.

Risk level: 🟡 Medium

3. Cloud / CDN ASNs

Examples: AWS, Azure, Cloudflare, Akamai.

Characteristics:

- Global infrastructure
- Shared servers
- Anycast routing
- Many tenants

Blocking entire ASN = breaks internet services.

Risk level: Context-based

Investigate specific domain/IP instead.

Heuristic Examples (How Analysts Think)

Example 1 — AS32934 (Meta / Facebook)

If traffic comes from this ASN:

- Likely social media infrastructure
- Abuse may relate to fake accounts or phishing pages

Not malware hosting usually.

Example 2 — AS16509 (Amazon AWS)

Very common in alerts.

Why?

Attackers love cloud servers because:

- Easy to rent
- Anonymous signup
- Short-lived infrastructure

Action:

Do NOT block whole ASN.

Instead block:

- Specific IP
- Domain
- CIDR range

Example 3 — AS124888 (Vodafone ISP)

If malicious traffic comes from here:

Likely cause:

- Infected home user
- Botnet device

- Compromised router

Response:

- Monitor
- Rate-limit
- Notify ISP if needed

Not treated as attacker-owned infra.

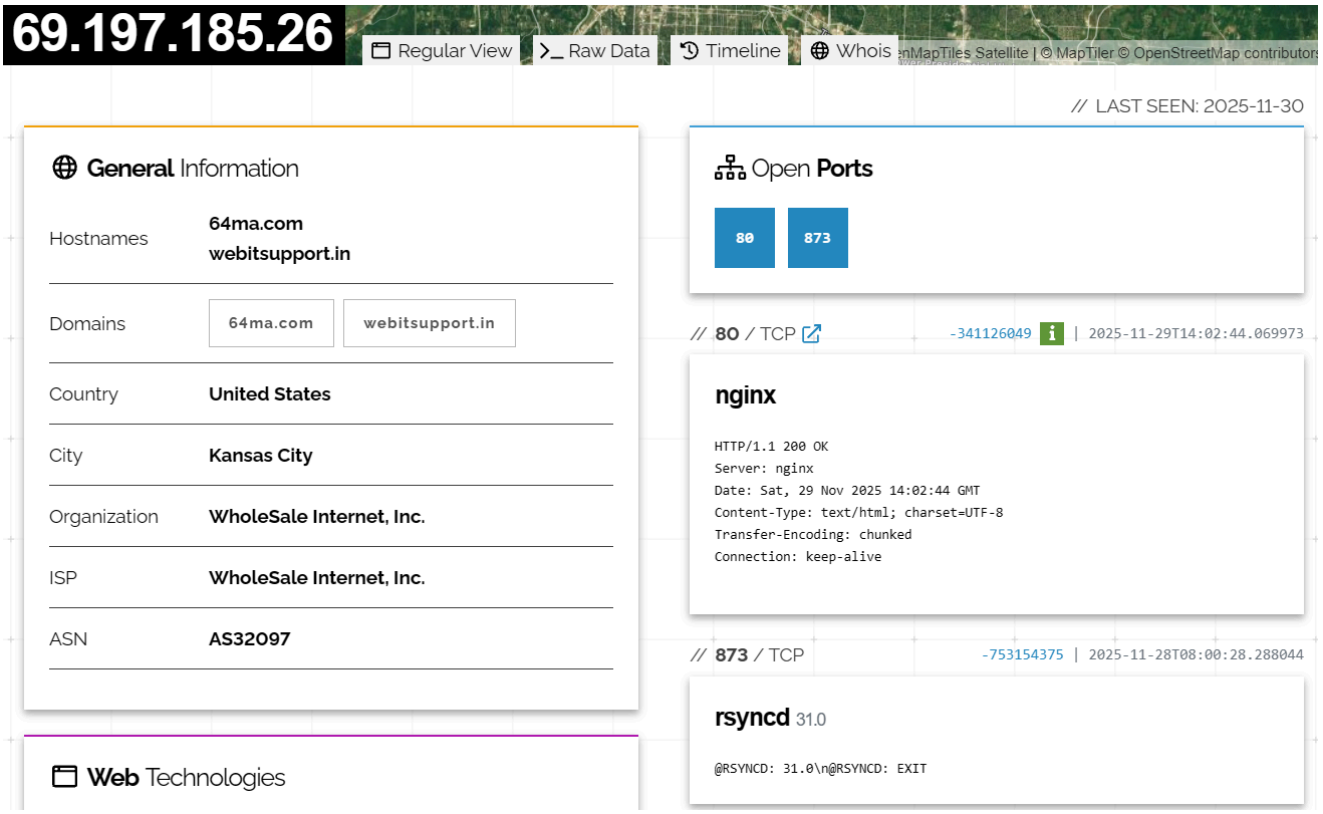
SOC Analyst Workflow

At this stage, our workflow in the SOC could resemble the following, though it may vary depending on established organisational processes and practices.

- **Start with RDAP**: Confirm netrange, org, ASN, and abuse contacts.
- **Add ASN Context**: Check bgpview.io or ipinfo.io for ASN details and role.
- **Check Geolocation**: Capture country from at least two sources. Record mismatches.
- **Look for rDNS Patterns**: Reverse DNS can hint at hosting type (e.g., *[.]btcentralplus[.]com = UK broadband). Do not base decisions solely on rDNS.
- **Consult Internal Logs**: Has this IP appeared in the last 30 days? If yes, in what context?
- **Classify Role**: Hosting, residential, CDN, or cloud. Record reasoning.
- **Plan Outreach**: If confirmed malicious and in a cooperative ASN, prepare a report for the abuse contact.

Shodan Reconnaissance

Shodan is a powerful reconnaissance tool for IP address analysis. By indexing internet-connected devices and services, Shodan provides detailed information about open ports, running services, and system configurations.

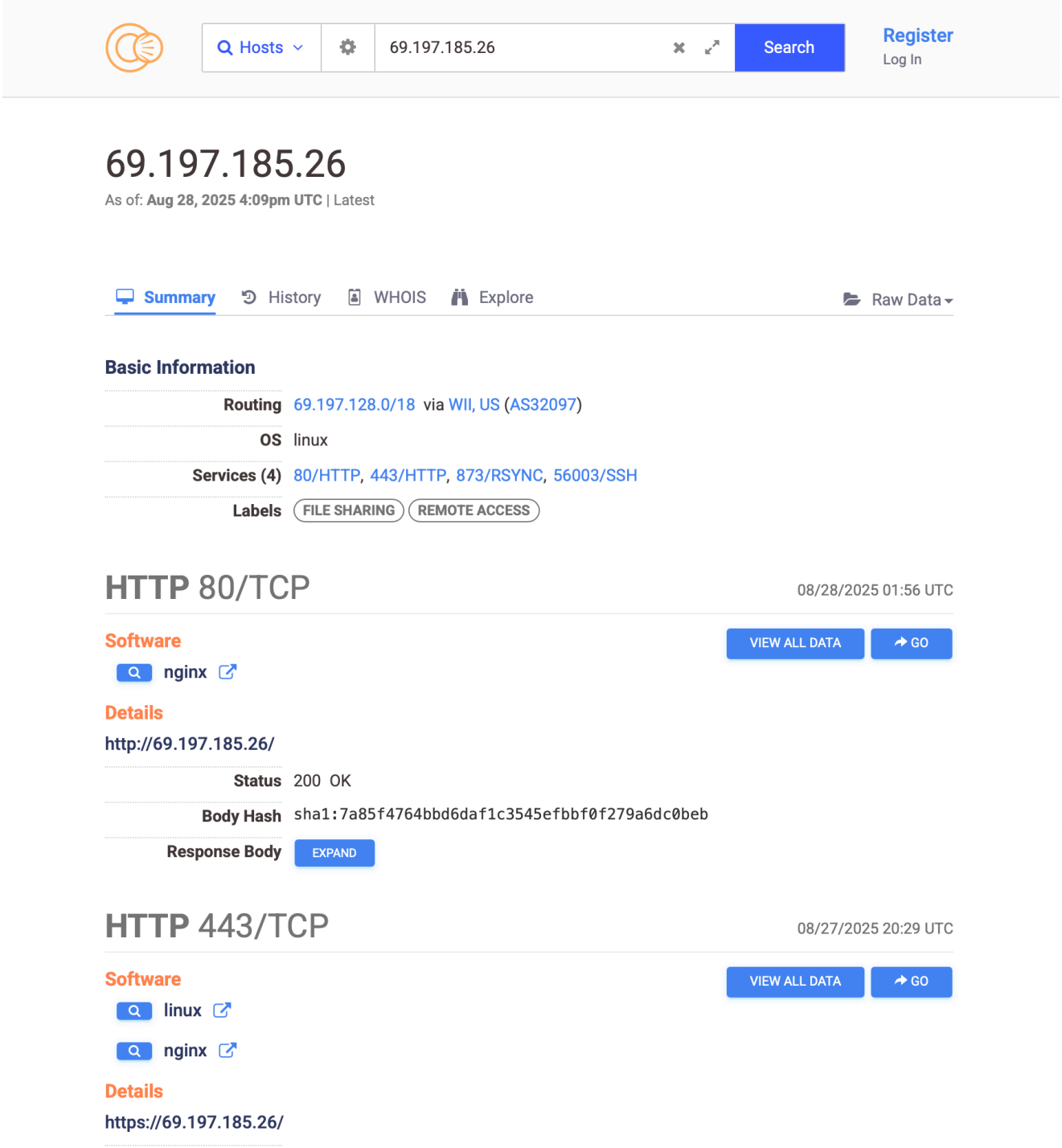


crt.sh : TLS certificate information

- **Issuer**: This field provides details on who signed the certificate. For example, Let's Encrypt is a common but neutral vendor. A self-signed certificate may be a sign of a hastily deployed system.
- **Validity Period**: Short-lived certificates of up to 90 days are normal for usage. Analysts must look for bursts of reissued certificates and investigate suspected phishing infrastructure.

Censys Search

Censys.io can be a good alternative to Shodan for blue teams, as it shows exposed services even on non-standard ports and provides some advanced search capabilities.



SOC Analyst Workflow

At this stage, our workflow in the SOC could resemble the following, though it may vary depending on established organisational processes and practices.

- **Check Shodan/Censys banners**: Identify exposed services and possible misconfigurations.
- **Review TLS certificates**: Ensure to record issuer, SANs, and validity period.
- **Look for anomalies**: Instances of multiple SANs, brand look-alikes or sudden bursts of issuance.
- **Pivot**: Utilise the certificate or banner artefacts to uncover related infrastructure.
- **Assess blast radius**:
    - RDP/SSH on residential ASN → shows a likelihood of a compromised endpoint.

- TLS with many unrelated SANs on CDN ASN → shared infrastructure, avoid IP block.
- Self-signed TLS on small ranges → shows likelihood of attacker panels or proxies.