PRACTICAL 4

Date: 10/02/2025

AIM: To develop skills in intelligence analysis, IOCs, and CTI sharing and collaboration.

Theory:

IP (Internet Protocol):

- An IP address is a unique identifier for a device on a network. In the context of cyber threat analysis, an IP address can be associated with malicious activities (e.g., botnet command and control, DDoS attacks, etc.).

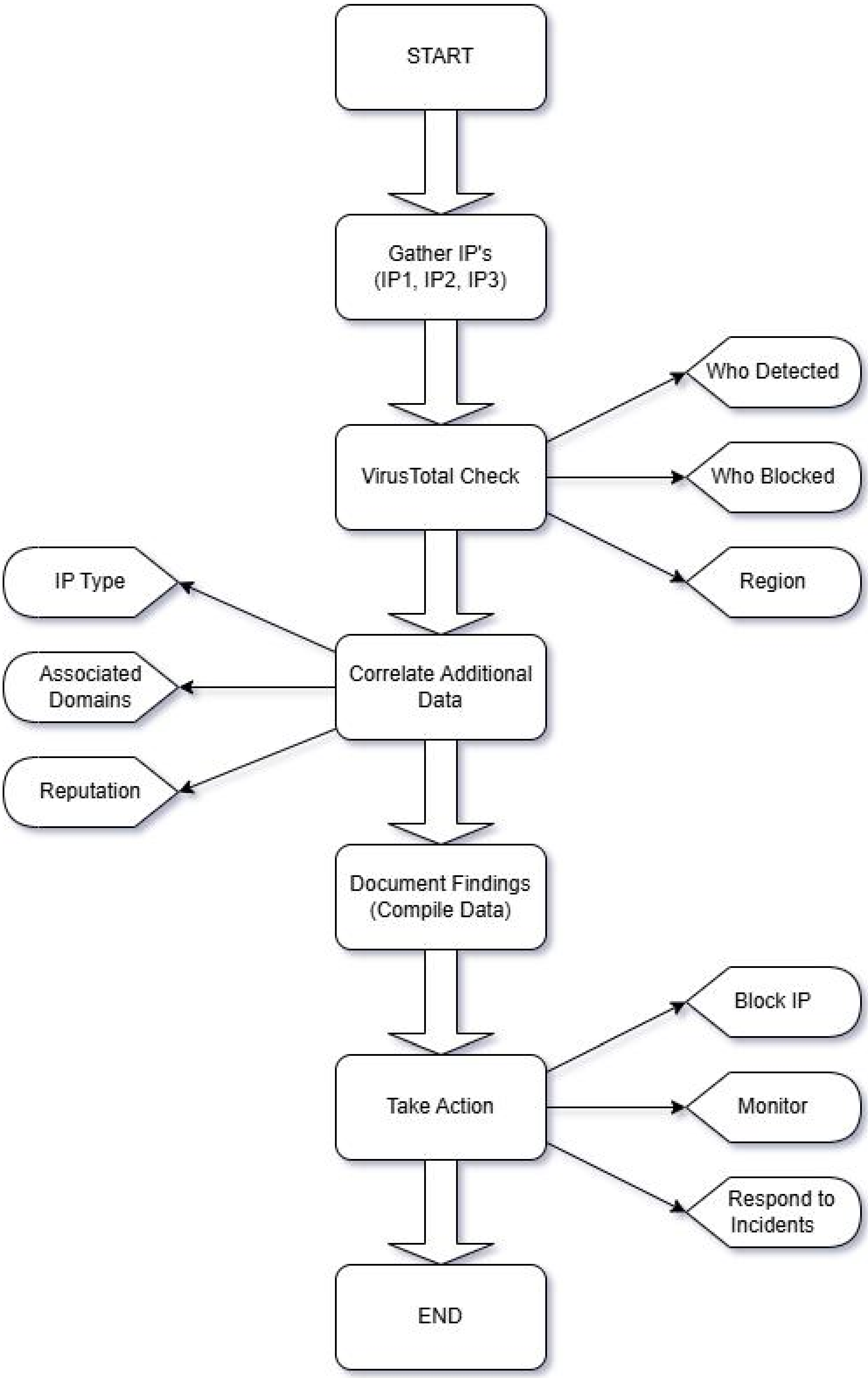
Virus Total:

- VirusTotal is a free online tool that analyzes files and URLs to detect malware, viruses, trojans, and other types of malicious content.
- **Use in Threat Intelligence:** By uploading files (e.g., executables or suspicious documents) or providing URLs to VirusTotal, you can quickly gather intelligence on potential threats, learn more about their behavior, and share your findings with the security community.

Nmap (Network Mapper):

- Nmap allows security professionals to scan networks for vulnerabilities or suspicious activities, such as unauthorized open ports or services that might be exploited by attackers.

Steps:


START
Gather IP's
(IP1, IP2, IP3)
VirusTotal Check
Who Detected
Who Blocked
Region
IP Type
Associated Domains
Reputation
Correlate Additional Data
Document Findings
(Compile Data)
Block IP
Monitor
Respond to Incidents
Take Action
END

Scope	IP1(73.32.175.15)	IP2(31.3.96.40)	IP3(45.84.107.198)
From Where You Get	MaxMind	Google	MaxMind
Who Blocked	-	-	-
Who Detected	MalwareURL	MalwareURL	Criminal IP
Attacks	-	-	-
Region	US	NetherLand	Sweden
Service	ftp	https	tor-orport
Open Ports	21/tcp	80/tcp	443/tcp
Version	-	Apache httpd	Tor 0.3.1.1 or later