Comprehensive Coverage of Data in CTI: What You Need to Collect

Chintan Gurjar

Areas to be covered in CTI

Strategic Intel	Tactical Intel	Operational Intel	Bulletins	IoCs/IoAs	Threat Actor Profile	Malware Analysis Report
DFIR Report	Vulnerability Intelligence	TTPs	Phishing Intel	Security Blog Posts	News & Articles	Threat Maps
Social Media Intel	Threat Database	Botnet Tracking	DNS Data	IDS Alerts	Threat Hunting Reports	TIP Feeds
Government Advisories & Alerts	OSINT	Geo-political intel	Behavioral Analytics Reports	Third-Party/Vendor Risk Report	NVD Report	CERT Report
Honeypot/Honeynet data	SOAR data	Espionage Intel	Credential Leakage Report	Zero-day Intel	SIEM Alerts	Ransomware Intel

Areas to be covered in CTI

IP Addresses	Domain Names	File Names	File Hashes	URLs	Email Addresses
User Agents	Malware Artifacts	DNS Requests	Network Connections	Historical & Predictive Intel Reports	C2 Servers
Binary Code/Executables	Cryptocurrency Wallet Addresses	Credential Dumps	Detected Exploits	Hostnames	API Keys
Usernames	Process Names	Botnet data	Zero-day Exploits	Sandboxing Report	APT data
	Darkweb/Darknet data	Code Snippets	Ports	Certificates	