Intelligear
Managed Threat Intelligence

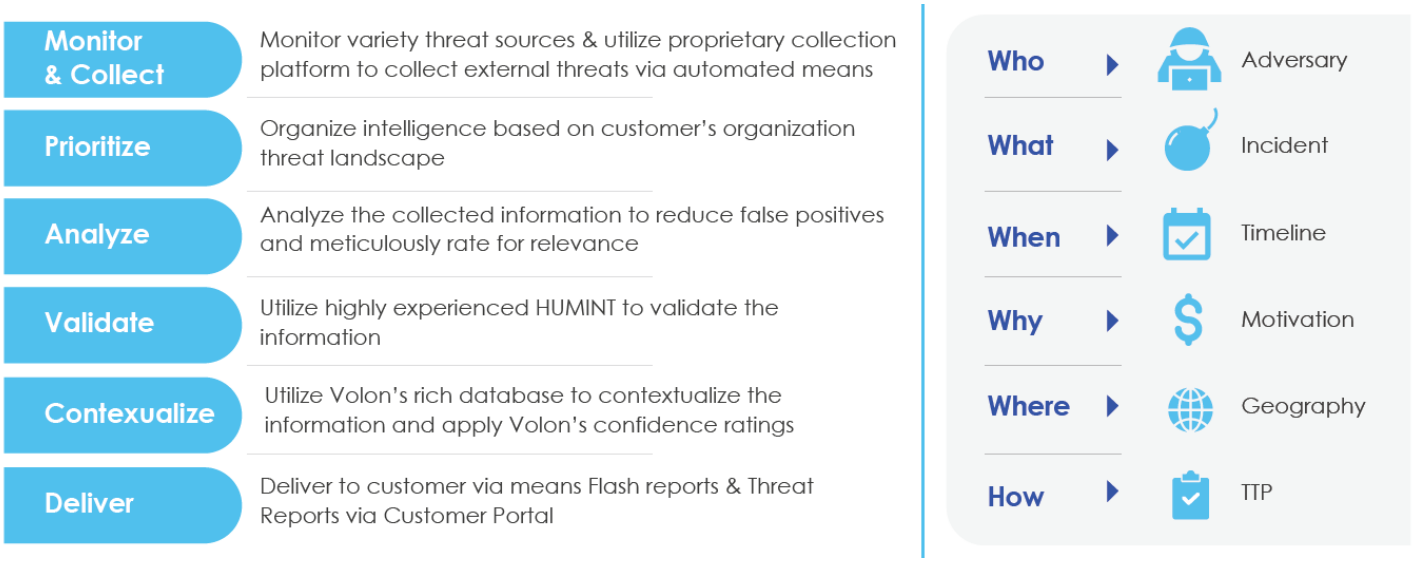
Adversary Centric Intelligence

VOLON

CONTENTS

IntelliGear: Adversary Focussed Intelligence

Volon's Intelligear benefits organizations by providing Adversary Focused Intelligence, which includes contextual insights into imminent threats. This helps them to respond faster to incidents, better understand their attackers and get ahead of the adversaries by safeguarding their assets.



Adversary Focused Intelligence Components

Adversary Centric intelligence provides comprehensive coverage of Dark Web, Open Source and Technical Threat Indicators from dominant and emerging threats. The intelligence includes threat actor insights to help organizations proactively assess risks, look for vulnerabilities in the existing setup and increase the security awareness of their staff.

The Adversary centric intelligence includes

- Darknet/Deep web monitoring
- Human intelligence (HUMINT)
- Open-Source Intelligence (OSINT)
- Technical Intelligence (TECHINT)

DARKNET/ DEEP WEB MONITORING

Volon collect, categorize and disseminate threat intelligence based upon Organization profile and relevance from various Darknet Forums/Sites/IRC/I2P sites. This helps Organization to identify, profile and mitigate the risks.

HUMINT (Human Intelligence)

Volon deploys Human Intelligence, which involves direct human interaction and engagement with threat adversaries in Darknet in the exclusive 'invite only forum'. It also includes 121 interaction with Darknet threat actors to obtain direct & exclusive intelligence and supporting information/evidence in order to build more context to the intel finding.

OSINT (Open-Source Intelligence)

Volon collection experts will collect and prioritize intelligence using OSINT and sum it up with all possible contextual information which is collected via other private sources, which will allow Organization to correlate the information which is being spoken in public media with solid context provided in our reporting.
The various avenues from where open-source data will be collected are

- Social Media
- Instant Messaging (IRC/Jabber)
- Pastie Sites (like Pastebin)
- GitHub Repositories
- Blogs & News sites

TECHINT (Technical Intelligence from various campaigns)

Volon monitors campaigns and report detailed IOCs, technical information for direct consumption by Organization's SOC team. This helps to protect against campaigns such as:

- Phishing Attacks
- Ransomware attacks
- APT (Advanced Persistent Threats) group campaigns
- Malwares campaigns
- Vulnerability exploitation

The TECHINT reports published on the Intelligear portal also have mapping with MITRE ATT&CK Framework.

Deliverables

Sr no.	Service Component	Deliverable
1	Darknet monitoring	A finished intelligence report with confidence ratings based upon relevance to targeted organization. The report shall contain collected evidence (threat actor claims, credential leaks, exploits/vulnerability info, access proofs etc), nature of threat and our analysis on the same.
2	HUMINT	A finished intelligence report with confidence ratings based upon relevance to targeted organization. The report shall contain collected evidence (chat transcript, proof of attack, methods of breach etc), nature of threat and our analysis on the same.
3	OSINT	The OSINT reports which are published will contain extensive coverage of Motivations such as Hacktivism, Defacement and latest attack vectors along with actionable IOC, which will allow Organization to correlate the information which is being spoken in public media.
4	TECHINT	The TECHINT reports covers actor motivations (Cybercrime/Cyber espionage) , tools and infrastructure which will contain observables like • IP Address • Malware Hash • URL • Domain Malware analysis /reverse engineering technical report will also be provided on Organization request.

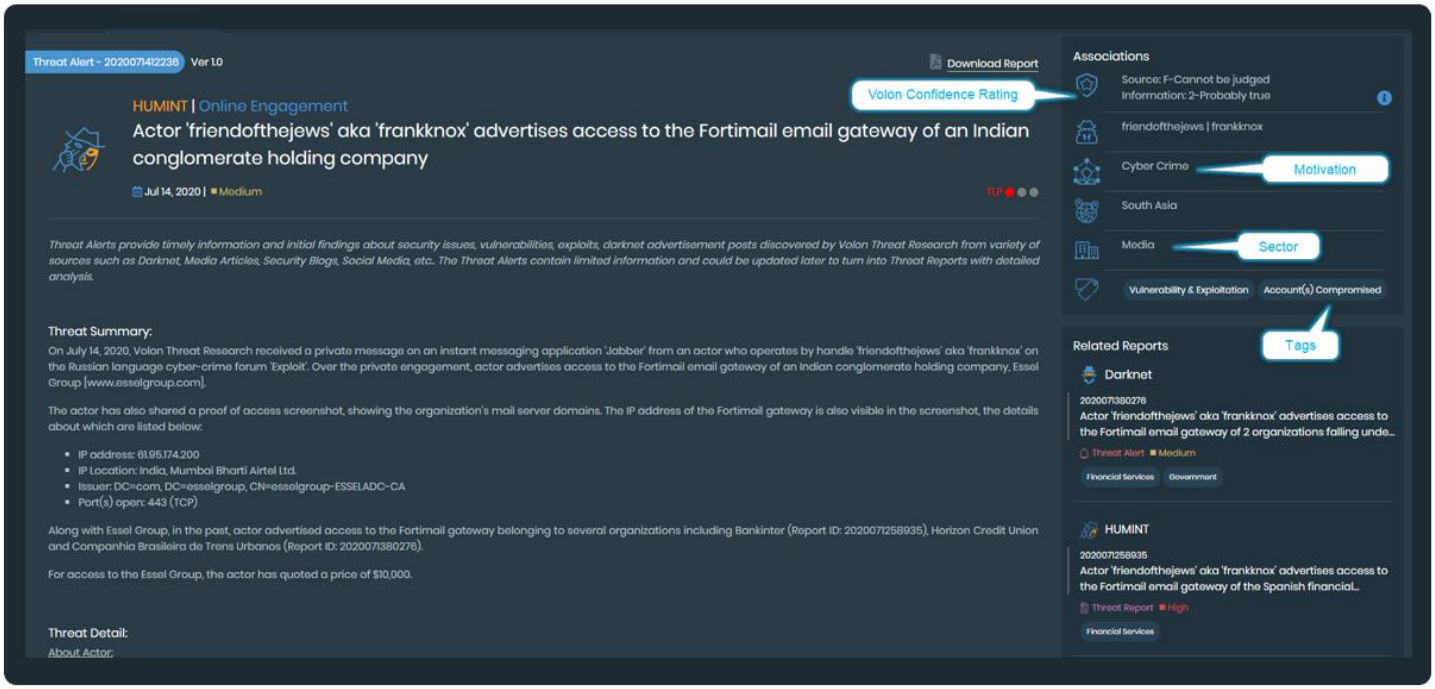
Adversary Focussed Intelligence Portal

Volon deliver intelligence via customised Customer Portal which is focused on customer profile and sector, overall aim is to provide relevant and actionable intelligence with ability to be consumed by multiple teams of a security organisation of the Organization.

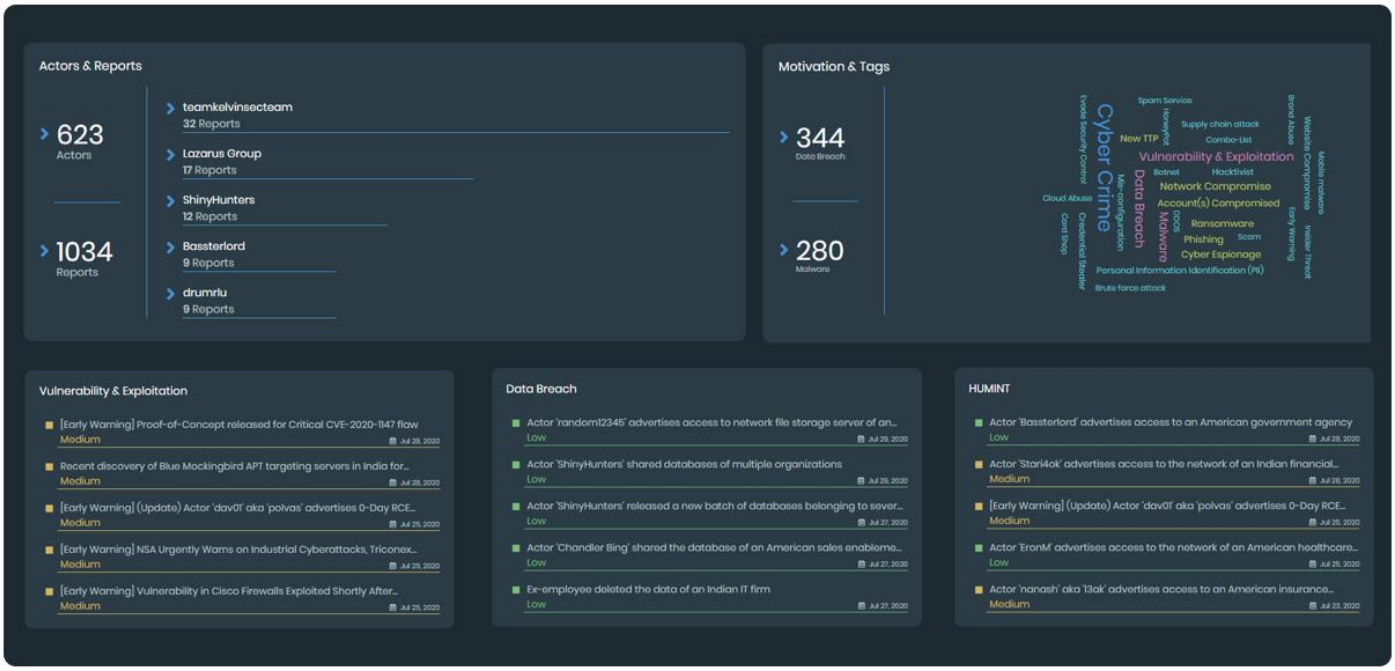
Dashboard

Dashboard provides a single view with summary of all threats for the customer, this include reporting from Darknet, Credential Leaks, Technical Intelligence. Flash reports with “High “relevance is also available for customers to view directly.

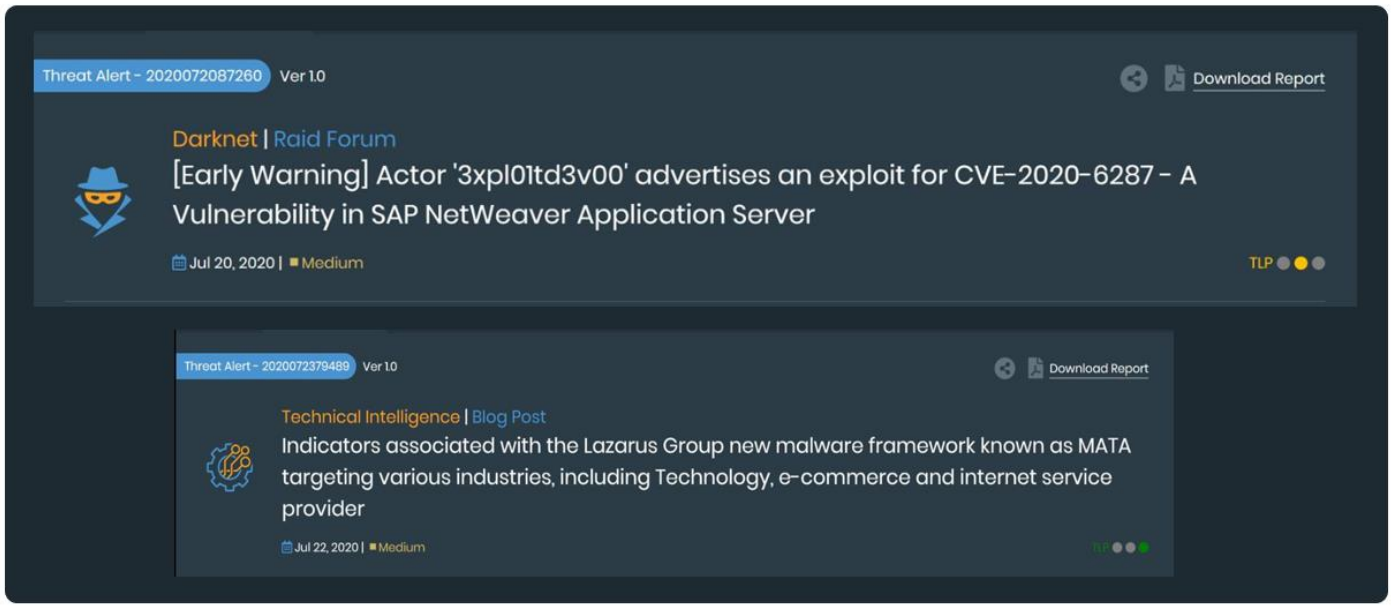
Threat Report



Threat Actors/Motivations



Early Warning Reports



Integrations

Volon's modular intelligence output enables third party integration utilizing much easier connection methods. These industry standard methods such as REST API / STIX/TAXII provide easy methods to ensure data flow across multiple systems.

Dashboard Integration

Volon can provide integration options to ensure Volon's intelligence data is able to ingest in the Intelligence aggregator platforms or third party TIP (Threat Intelligence Platforms) to help customer in order to remove dependency for additional layer of dashboard and enable Customer to collect and analyse all intelligence information at single console

SIEM & SOAR Integration

Technical IOCs can be integrated with any SIEM with the help of RESTful API or STIX/TAXII distribution system. Volon can provide steady contextualized Intelligence feeds to SIEM and SOAR to enable SOC analyst link the indicators identified from internal system to External intelligence provided by Volon.

Volon Cyber Security
www.volon.io