vehere

WHITEPAPER

Cyber Security for Power Sector

Powered By Vehere's CSA Platform

Author: Vipul Kumra
vipul.kumra@vehere.com

Overview – Cyber Situational Awareness (CSA) Platform

Cyber Situational Awareness (Cyber SA) is the immediate knowledge of friendly, adversary and other relevant information regarding activities in and through cyberspace. Cyber SA is the capability that helps security analysts and decision makers:

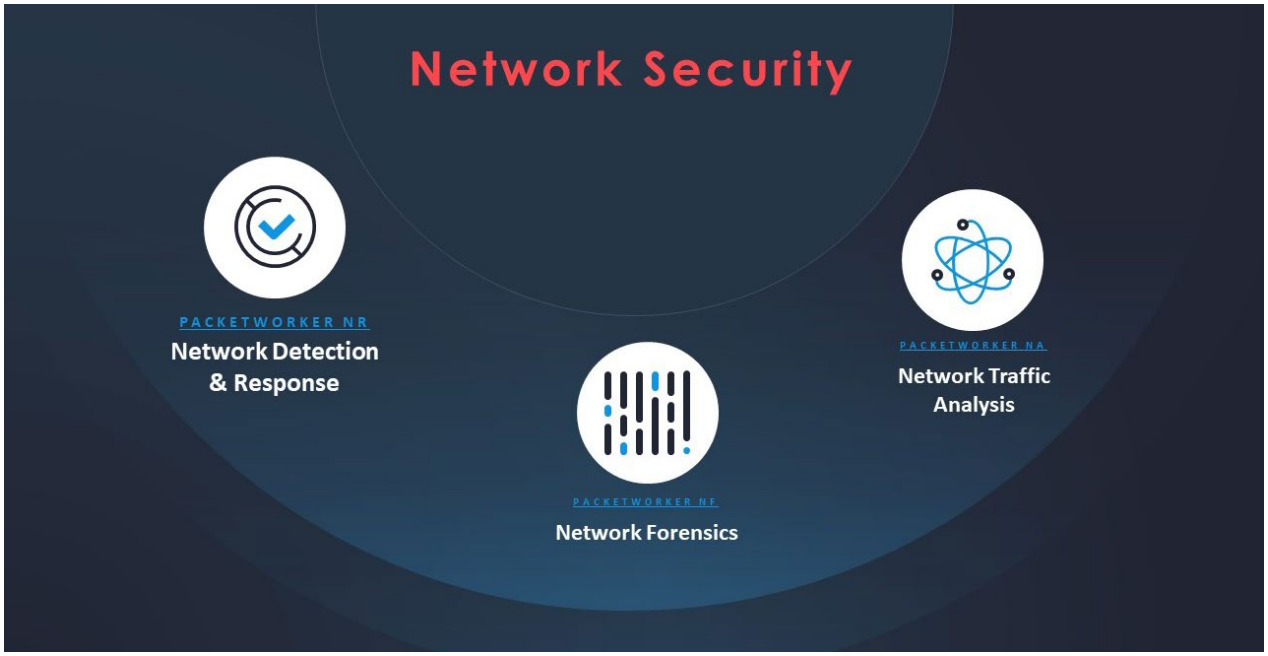
- Visualize and understand the current state of the IT infrastructure, as well as the defensive posture of the IT environment
- Identify what infrastructure components are important to complete key functions
- Understand the possible actions an adversary could undertake to damage critical IT infrastructure components
- Determine where to look for key indicators of malicious activity.

Cyber situational awareness involves the normalization, deconfliction, and correlation of disparate sensor data, and the ability to analyze data and display the results of these analyses. Situational awareness (SA) is an integral part of an information assurance (IA) common operational picture. Such a picture provides a graphical, statistical, and analytical view of the status of computer networks and the defensive posture.

Situational awareness is the key to effective computer network defense. A robust situational awareness capability is necessitated by the highly interconnected nature of information systems and computer networks, the degree to which they share risk, and the coordination and synchronization requirements of response efforts.

Analysts and decision makers must have tools enabling timely assessment and understanding of the status of the networks and systems that make up the IT infrastructure. This situational understanding must be presented at multiple levels of resolution:

- A top-level, global indication of system health
- Exploration of various unfolding threat scenarios against various components of the system
- More local-level details of recognizable or previously unseen anomalous activities



Objective of issuing Guideline:

- Creating cyber security awareness
- Creating a secure cyber ecosystem,
- Creating a cyber-assurance framework,
- Strengthening the regulatory framework,
- Creating mechanisms for security threat early warning, vulnerability management and response to security threats,
- Securing remote operations and services,
- Protection and resilience of critical information infrastructure,
- Reducing cyber supply chain risks,
- Encouraging use of open standards,
- Promotion of research h and development in cyber security,
- Human resource development in the domain of Cyber Security,
- Developing effective public private partnerships,
- Information sharing and cooperation
- Operationalization of the National Cyber Security Policy

While Vehere's Cyber Situational Awareness Platform can help meet most of these objectives either directly or indirectly, however, it has a direct applicability in the below mentioned objectives

- Creating cyber security awareness
- Creating a secure cyber ecosystem,
- Creating a cyber-assurance framework,
- Strengthening the regulatory framework,
- Creating mechanisms for security threat early warning, vulnerability management and response to security threats,
- Securing remote operations and services,
- Protection and resilience of critical information infrastructure,
- Reducing cyber supply chain risks,
- Information sharing and cooperation
- Operationalization of the National Cyber Security Policy

Functional requirement derived from CEA (Cyber Security in Power Sector) Guidelines, 2021

Background: Cyber intrusion attempts and Cyber-attacks in any critical sector are carried out with a malicious intent. In Power Sector it's either to compromise the Power Supply System or to render the grid operation in-secure. Any such compromise, may result in malicious operations of equipment's, equipment damages or even in a cascading grid brownout/blackout. The much hyped air gap myth between IT and OT Systems now stands shattered. The artificial air gap created by deploying firewalls between any IT and OT System can be jumped by any insider or an outsider through social engineering. Cyber-attacks are staged through tactics & techniques of Initial Access, Execution, Persistence, Privilege Escalation, Defence Evasion, Command and Control, Exfiltration. After gaining the entry inside the system through privilege escalation, the control of IT network and operations of OT systems can be taken over even remotely by any cyber adversary. The gain of sensitive operational data through such intrusions may help the Nation/State sponsored or non-sponsored adversaries and cyber attackers to design more sinister and advanced cyber-attacks.
References to the requirements where Vehere's platform can help:

- Help in ensuring that there is hard isolation of OT Systems from any internet facing IT system. (Article 1. a. i. – Page 8)
- Helps validating that there is only one of the IT systems facing Internet at any of their site/location if required which is isolated from all OT zones and kept in a separate room under the security and control of CISO. (Article 1. a. ii. – Page 8)
- Validating that Downloading/Uploading of any data/information from the Internet facing IT system is done only through an identifiable whitelisted device and for all such activities digital logs are maintained and retained under the custody of CISO for at least 6 months. The log shall be readily to carry out the forensic analysis if asked by investigation agency. (Article 1. a. iii. – Page 8)
- Ensuring each firewall is allowing communication with the whitelisted IP addresses only. (Article 1. a. iv. – Page 8)
- The Responsible Entity shall submit to NCIIPC through Sectoral CERT, details of Cyber Assets which uses a routable protocol to communicate outside the Electronic Security Perimeter drawn by the Responsible Entity or a routable protocol within a control centre and dial-up accessible Cyber Assets, within 30 days from the date of their commissioning in the System. (Article 3. a) – Page 9)
- The Responsible Entity shall review their declared/notified CIIs at least once a year to examine changes if any in the functional dependencies, protocols and technologies or upon any change in security architecture. The Responsible Entity shall review their declared/notified CIIs once in every 6 months, in case if NCIIPC has directed them to constitute an Information Security Steering Committee. (Article 3. c) – Page 9)
- The Responsible Entity shall ensure that all cyber assets of their identified/notified CIIs are recorded in the asset register and considered for risk assessment as well as for finalization of controls in statement of applicability. (Article 3. d) – Page 9)
- has timely acted upon the advisories, guidelines and directive of NCIIPC, CSK, CERT-In and Sectoral CERTs. (Article 5. c). 2 – Page 10)
- Has deployed an Intrusion Detection System and Intrusion Prevention System capable of identifying behavioural anomaly in both IT as well as OT Systems. (Article 5. c). 3 – Page 10)
- Shares reports on incident response and targeted malware samples with CERT-In. (Article 5. c). 4 – Page 10)
- Enables only those ports and services that are required for normal operations. In case of any emergency the procedure as laid in Access management be followed. (Article 5. c). 6 – Page 10)
- Maintains firewall logs for the last 6 months duration. Firewall logs shall be analysed and all critical and high severity comments shall be addressed for effective closure. (Article 5. c). 7 – Page 10)
- Maintains all cyber logs and cyber forensic records of any incident for at least 90 days. (Article 5. c). 9 – Page 10)

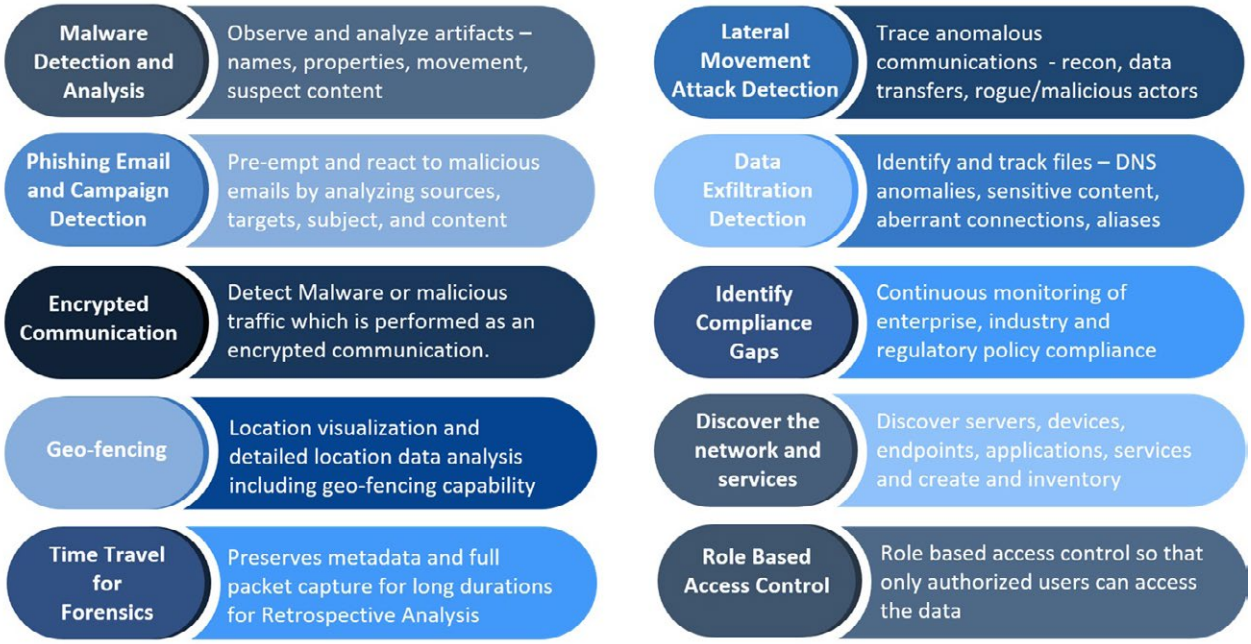
Other Critical Functionalities¬

- Ability to capture, index, record and analyse gigabit-rate data-streams in real time to identify & track nation/state adversaries

- Time Travel for Retrospective Analysis: Ability to preserve metadata and full packet capture (content) for durations spanning several months/years for forensics analyses as and when required
- Ability to comply with regulatory mandates and security best practices/standards.
- Role based access control so that only authorized users can access the data
- Location visualization and detailed location data analysis as these networks can be geographically spread.

Technical use-case mapping

This section maps the high-level functional requirements to technical use cases / capabilities. The purpose of this document is describe these use cases / capabilities along with other capabilities of Vehere's cyber situational awareness solution – PacketWorker.



Malware Detection and Analysis

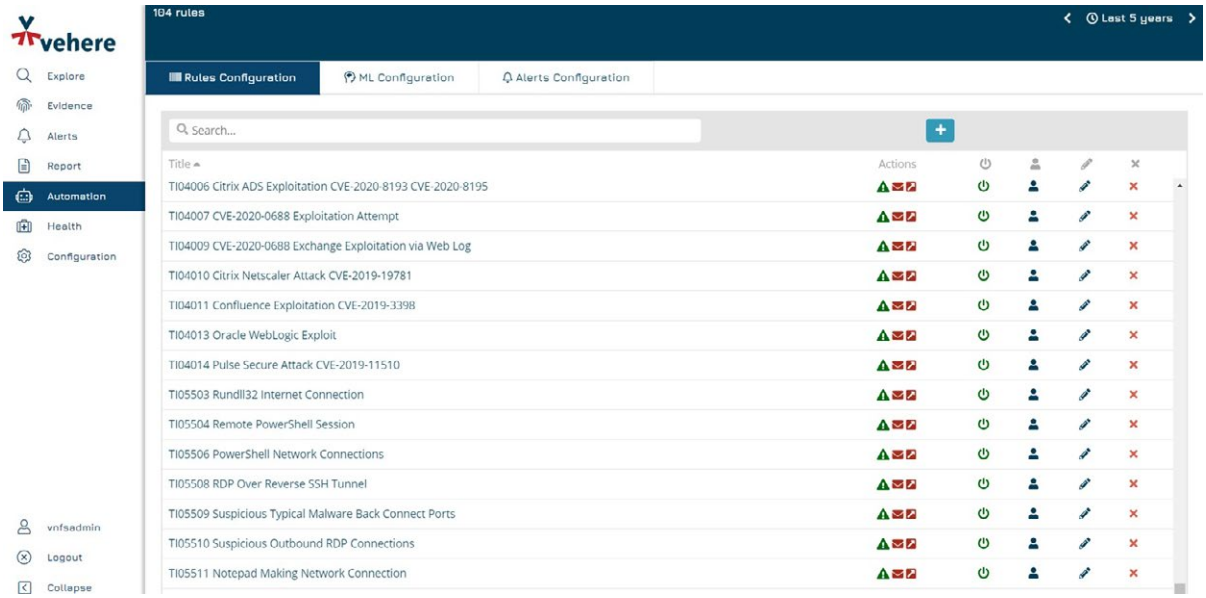
Reconnaissance – Reconnaissance is the first step in any cyber Criminals activity wherein the attackers scout for targets to compromise. Using behavioural indicators, the solution can detect reconnaissance attempts.
Exploit/Malware – Detect exploits or malware being carried in communication using hash matches with the blacklist.
Dynamic Analysis – Subject artifacts to sandboxes for dynamic analysis to detect zero-day threats or targeted attacks.
Content Categorization – Instead of which IP accesses which web-site, this capability enables consolidated assessment about which node is communicating with generally risky Internet Sites so that a comprehensive analysis is concluded at a glance.
Cyber Bullying – Use natural language processing to detect potentially bullying communication so as to avoid minor abuse.
Ransomware – Perhaps the biggest scourge for a user as it brings all things to a standstill often compromising many days of hard work. Detection is based on hash/checksum match, domain matches, DGA detections or, dynamic analysis.

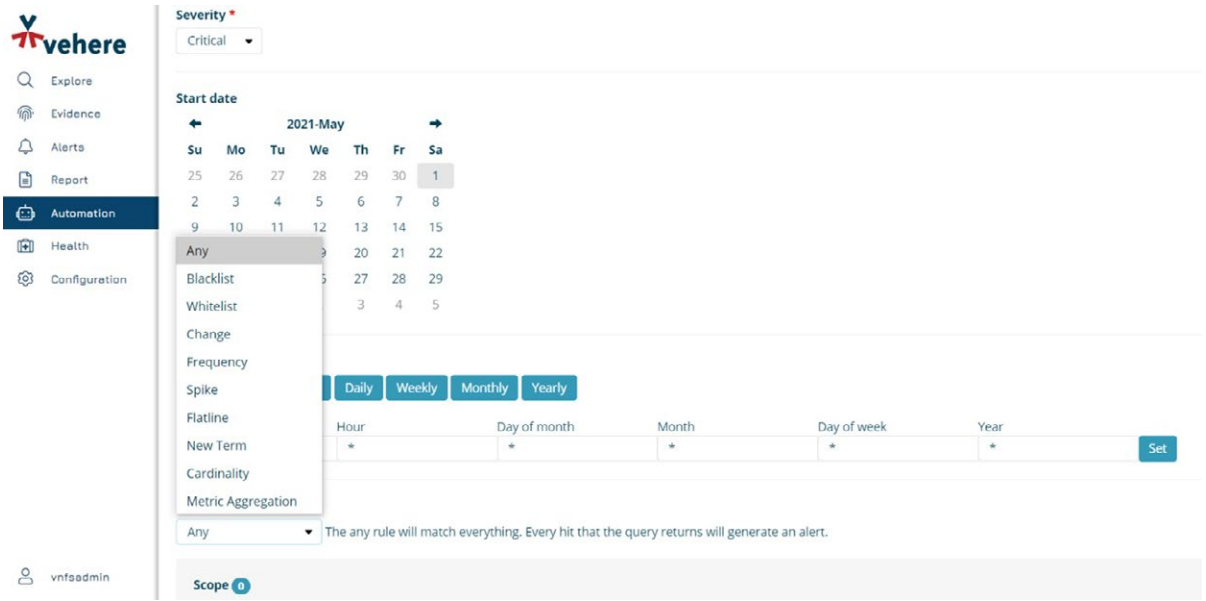
Machine learning plays an important role in detection of unknown malware and threat hunting also heavily relies on advanced Machine learning algorithms.

- During Machine Learning analysis, the system infers a probabilistic behavioural model of each network node using 'topic modeling'.
- Topic modeling is a natural language processing technique with a design principle that offers responses to one question – What is the probability that observed session adheres to a behaviour?
- Vehere relies on Latent Dirichlet Allocation (LDA) model among other machine learning techniques.

Rules Based Detection plays an important role in detection of known as well as unknown malware with known tools, techniques and procedures (TTPs) and indicators of compromise (IOC)/ indicators of attacks (IOA) and also greatly helps in threat hunting.

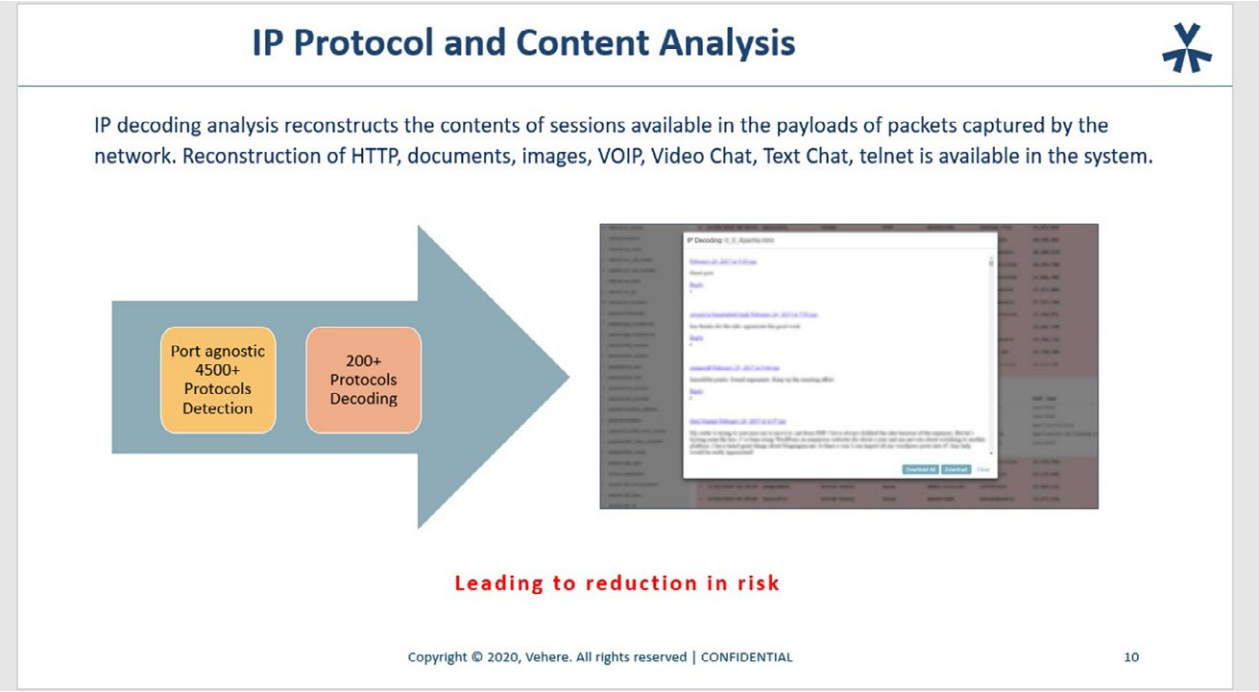
- Rule based detection involves the use of rules for identifying known penetrations or penetrations that would exploit weakness
- Rules can also be defined that identify suspicious behaviour
- Anomaly detection rules, Threshold rules, Behavioural rules

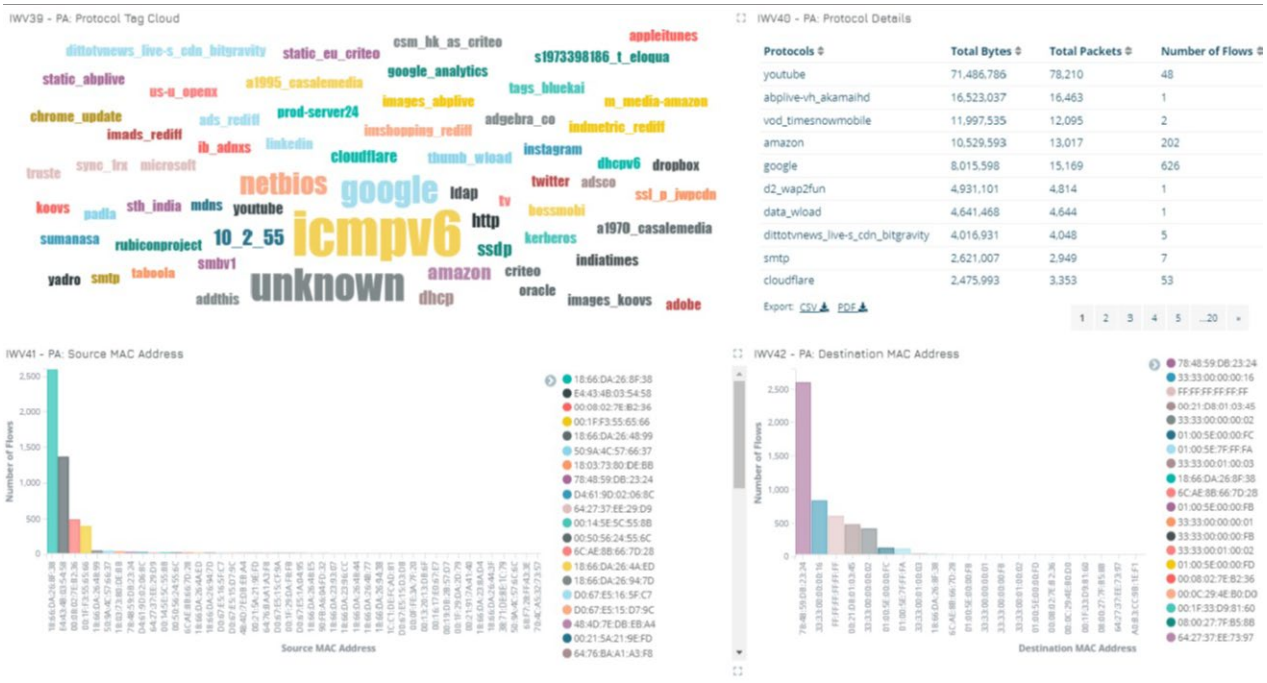




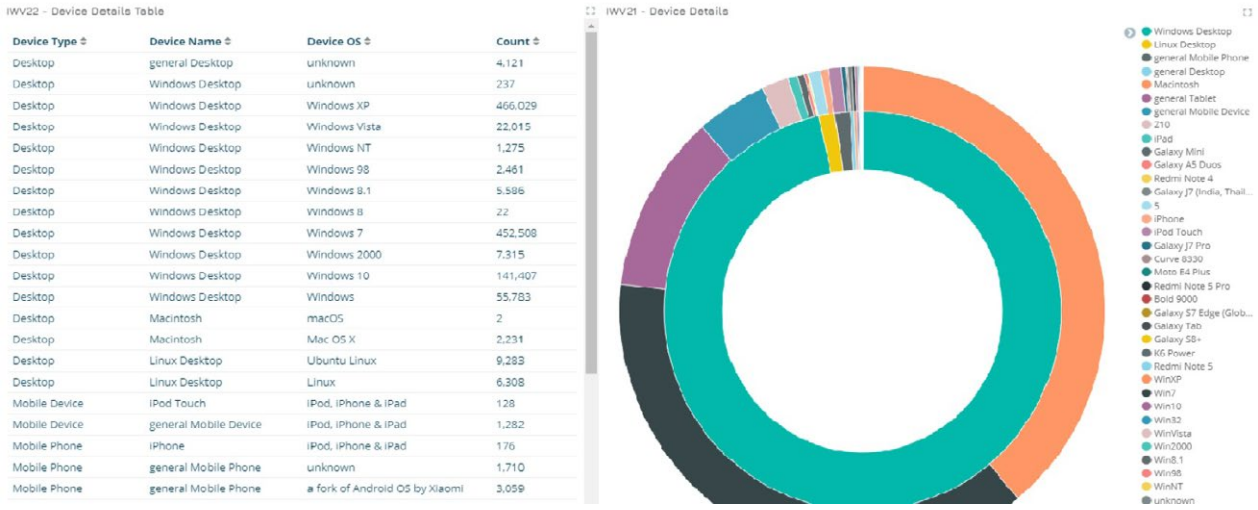
Discover Assets, Applications, Protocol and Content Analysis

- Rather than relying on connection's server port for detection of protocols, Vehere's solution can do the protocols analysis independently of ports using various techniques such as using a set of signatures which match typical protocol dialogues.
- Tunneled protocol detection analyses traffic to discover protocols that are tunneled over HTTP and HTTPS. Traffic that is allowed to tunnel over specific ports is also analysed. This feature helps to detect protocols used for malicious applications, instant messaging, peer-to-peer applications, and proxy avoidance.
- HTTP tunneling occurs when applications that use custom protocols for communication are wrapped in HTTP (meaning that standard HTTP request/response formatting is present) in order to use the ports designated for HTTP/HTTPS traffic. These ports are open to allow traffic to and from the Web. HTTP tunneling allows these applications to bypass firewalls and proxies, leaving a system vulnerable.





- Device details like device type, device name, device operating system and count are some of the data points captured



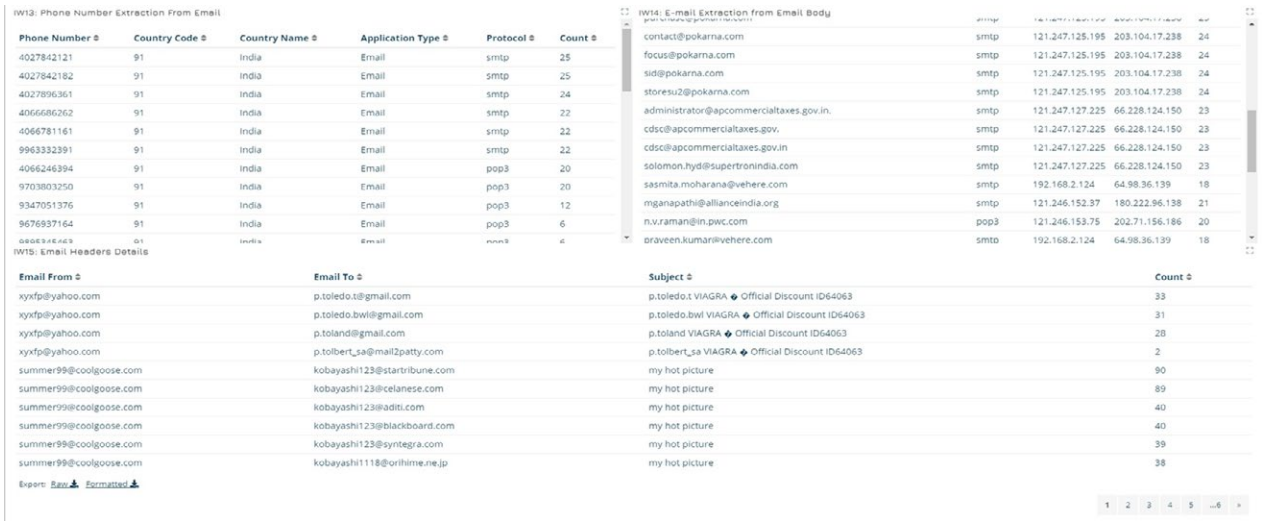
IWV22 - Device Details Table

Device Type	Device Name	Device OS	Count
Desktop	general Desktop	unknown	4,121
Desktop	Windows Desktop	unknown	237
Desktop	Windows Desktop	Windows XP	466,029
Desktop	Windows Desktop	Windows Vista	22,015
Desktop	Windows Desktop	Windows NT	1,275
Desktop	Windows Desktop	Windows 98	2,461
Desktop	Windows Desktop	Windows 8.1	5,586
Desktop	Windows Desktop	Windows 8	22
Desktop	Windows Desktop	Windows 7	452,508
Desktop	Windows Desktop	Windows 2000	7,315
Desktop	Windows Desktop	Windows 10	141,497
Desktop	Windows Desktop	Windows	55,783
Desktop	Macintosh	macOS	2
Desktop	Macintosh	Mac OS X	2,231
Desktop	Linux Desktop	Ubuntu Linux	9,283
Desktop	Linux Desktop	Linux	6,308
Mobile Device	IPod Touch	IPod, iPhone & iPad	128
Mobile Device	general Mobile Device	IPod, iPhone & iPad	1,282
Mobile Phone	iPhone	IPod, iPhone & iPad	176
Mobile Phone	general Mobile Phone	unknown	1,710
Mobile Phone	general Mobile Phone	a fork of Android OS by Xiaomi	3,059

IWV21 - Device Details

Phishing Email and Campaign Detection

Fraud Analysis – Use NLP to analyse content and proactively detect fraudulent communication or a new phishing campaign.
Email Analytics – Pre-empt and react to malicious emails by analysing sources, targets, subject and content.



IW13: Phone Number Extraction From Email

Phone Number	Country Code	Country Name	Application Type	Protocol	Count
4027842121	91	India	Email	smtp	25
4027842182	91	India	Email	smtp	25
4027896361	91	India	Email	smtp	24
4066686262	91	India	Email	smtp	22
4066781161	91	India	Email	smtp	22
9963332391	91	India	Email	smtp	22
4066246394	91	India	Email	pop3	20
9703803250	91	India	Email	pop3	20
9347051376	91	India	Email	pop3	12
9676937164	91	India	Email	pop3	6

IW14: E-mail Extraction from Email Body

contact@pokarna.com	smtp	121.247.125.195	203.104.17.238	24
focus@pokarna.com	smtp	121.247.125.195	203.104.17.238	24
sid@pokarna.com	smtp	121.247.125.195	203.104.17.238	24
storesu2@pokarna.com	smtp	121.247.125.195	203.104.17.238	24
administrator@apcommercialtaxes.gov.in.	smtp	121.247.127.225	66.228.124.150	23
cdsc@apcommercialtaxes.gov.	smtp	121.247.127.225	66.228.124.150	23
cdsc@apcommercialtaxes.gov.in	smtp	121.247.127.225	66.228.124.150	23
solomon.hyd@supertronindia.com	smtp	121.247.127.225	66.228.124.150	23
sasmita.moharana@vehere.com	smtp	192.168.2.124	64.98.36.139	18
mganapathi@allianceindia.org	smtp	121.246.152.37	180.222.96.138	21
n.v.raman@in.pwc.com	pop3	121.246.153.75	202.71.156.186	20
praveen.kumar@vehere.com	smtp	192.168.2.124	64.98.36.139	18

IW15: Email Headers Details

Email From	Email To	Subject	Count
xyxfp@yahoo.com	p.toledo.t@gmail.com	p.toledo.t VIAGRA ♦ Official Discount ID64063	33
xyxfp@yahoo.com	p.toledo.bwl@gmail.com	p.toledo.bwl VIAGRA ♦ Official Discount ID64063	31
xyxfp@yahoo.com	p.toland@gmail.com	p.toland VIAGRA ♦ Official Discount ID64063	28
xyxfp@yahoo.com	p.tolbert_sa@mail2patty.com	p.tolbert_sa VIAGRA ♦ Official Discount ID64063	2
summer99@coolgoose.com	kobayashi123@startribune.com	my hot picture	90
summer99@coolgoose.com	kobayashi123@celanese.com	my hot picture	89
summer99@coolgoose.com	kobayashi123@aditi.com	my hot picture	40
summer99@coolgoose.com	kobayashi123@blackboard.com	my hot picture	40
summer99@coolgoose.com	kobayashi123@syntegra.com	my hot picture	39
summer99@coolgoose.com	kobayashi1118@orihime.ne.jp	my hot picture	38

Export: Raw Formatted

1 2 3 4 5 ...6 »

Data exfiltration Detection

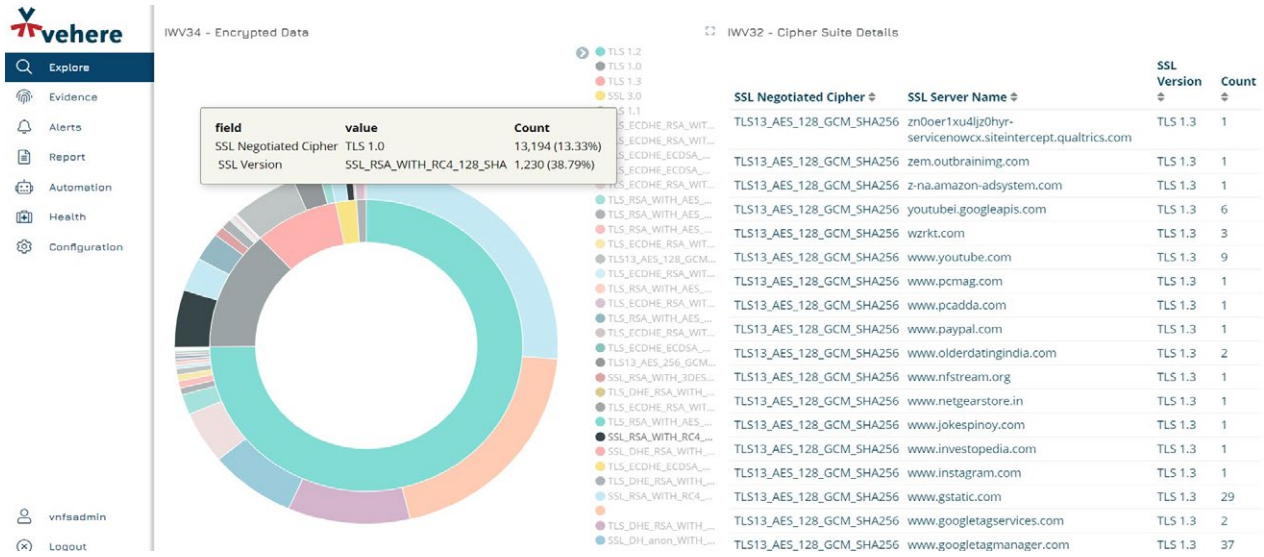
- **Sensitive Personal Information** – This is to extract any information from within the content that indicates exchange or leakage of sensitive information such as a location in mobile app data or, credit card data to an IP Address outside of the geographic location being monitored.
- **Data Exfiltration** – Theft of data to foreign shores using communication channels that should not generally be carrying such information. This capability is a mix of behaviour-based rules and Advanced Machine Learning algorithms.

Lateral Movement and Attack Detection

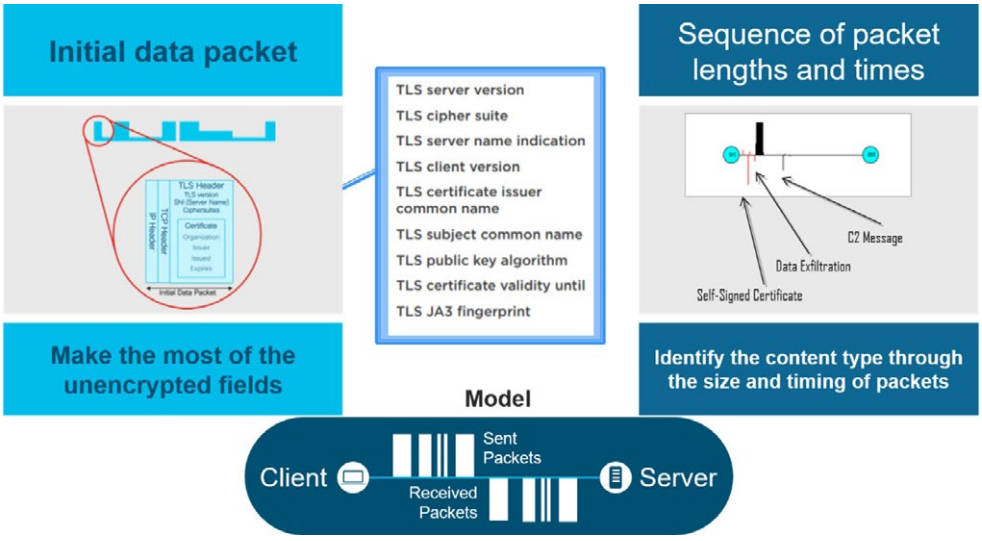
- **Reconnaissance** – Reconnaissance is the first step in any cyber Criminals activity wherein the attackers scout for targets to compromise. Using behavioural indicators, the solution can detect reconnaissance attempts.
- **Lateral movement detection via Link analysis** – Link analysis is a popular network analysis technique that is used to identify and visualize relationships (links) between different objects. PacketWorker Link Analysis has advanced statistical modelling for data mining. It helps the security analyst quickly drill down on the devices that has communicated with the infected machine and are likely compromised.

Encrypted Traffic Analysis

- **Mathematical Modelling**: Analyze almost any type of encrypted communication using mathematical modelling and heuristics.
- **Cryptographic compliance:** Cipher suite analysis helps to know whether more secure versions of TLS like (TLS 1.3 or TLS 1.2) are in use or not. Many ciphers are prone to replay attacks and also attacks have been reported against MD5 and SHA. So through this we can also get to know whether weak or strong ciphers are in use.

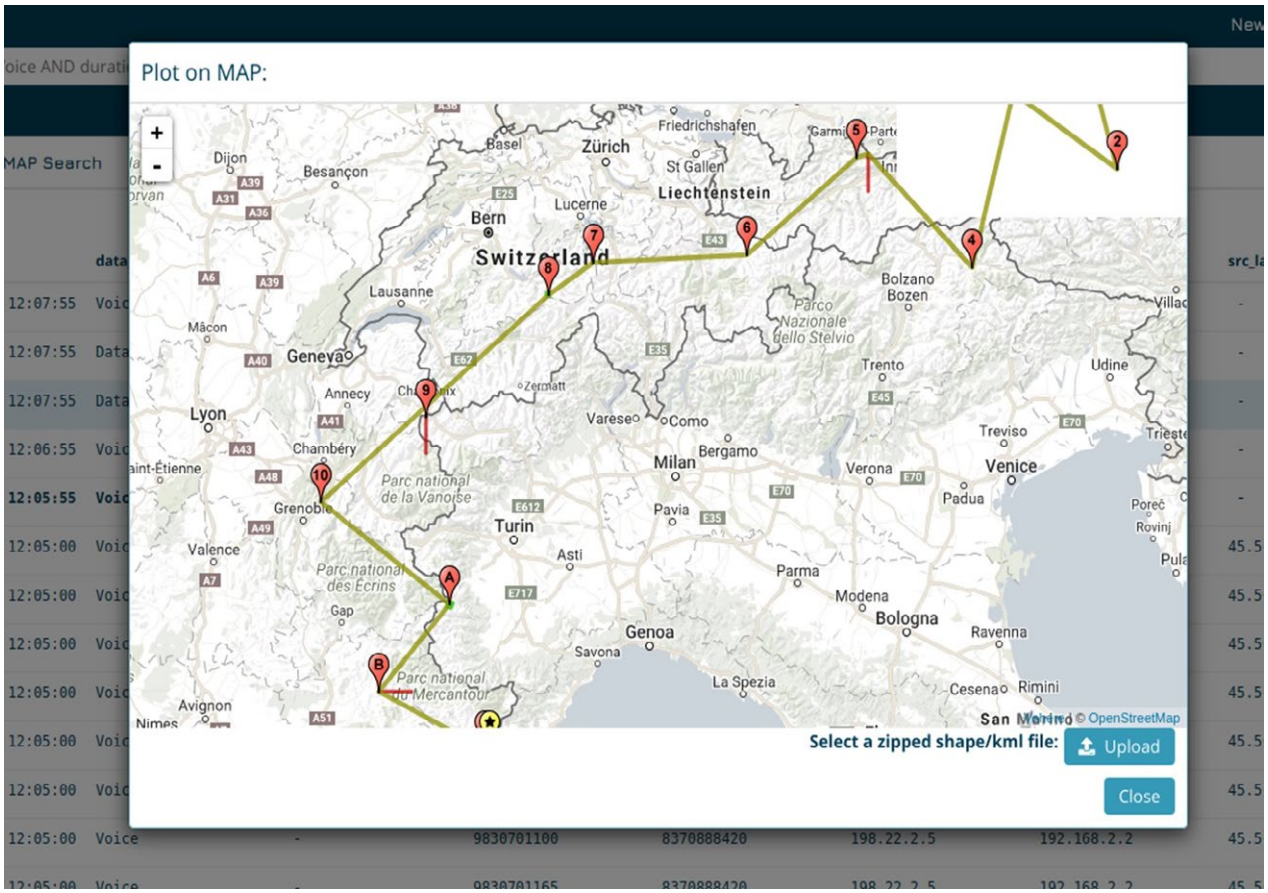


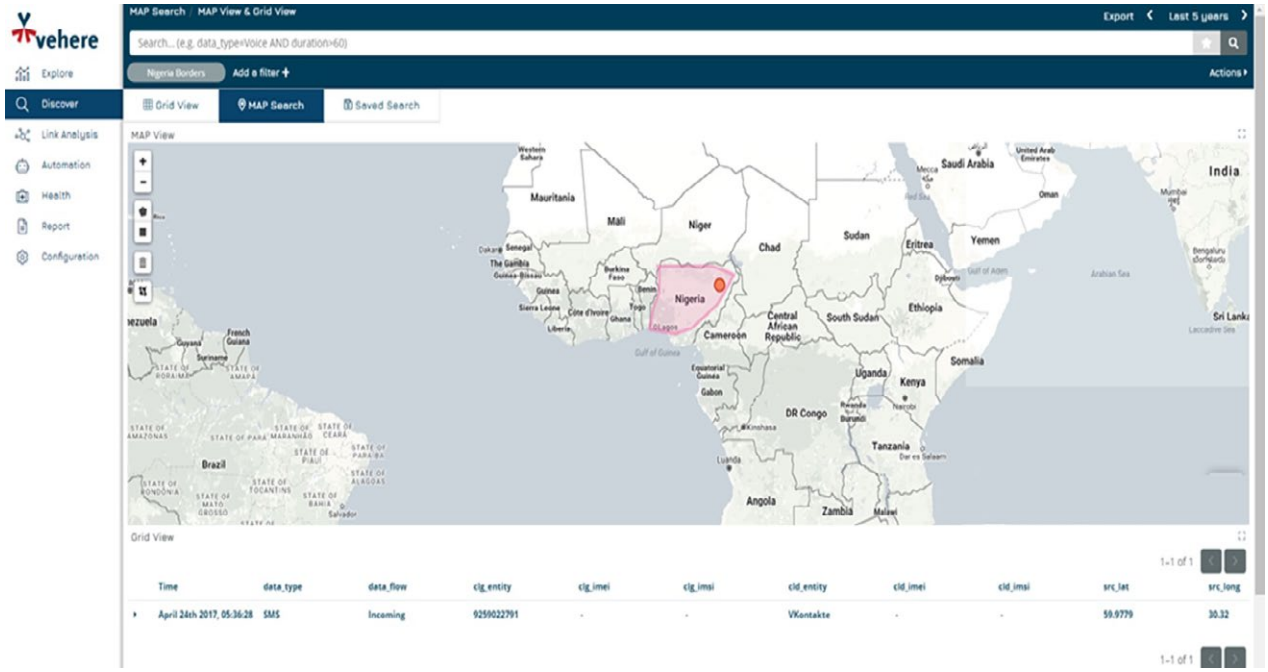
- **Detect malware in encrypted traffic:** It is possible to detect malware within encrypted traffic using packet lengths, arrival times and durations as they tend to be inherently different for malware than benign traffic.



Geo-fencing

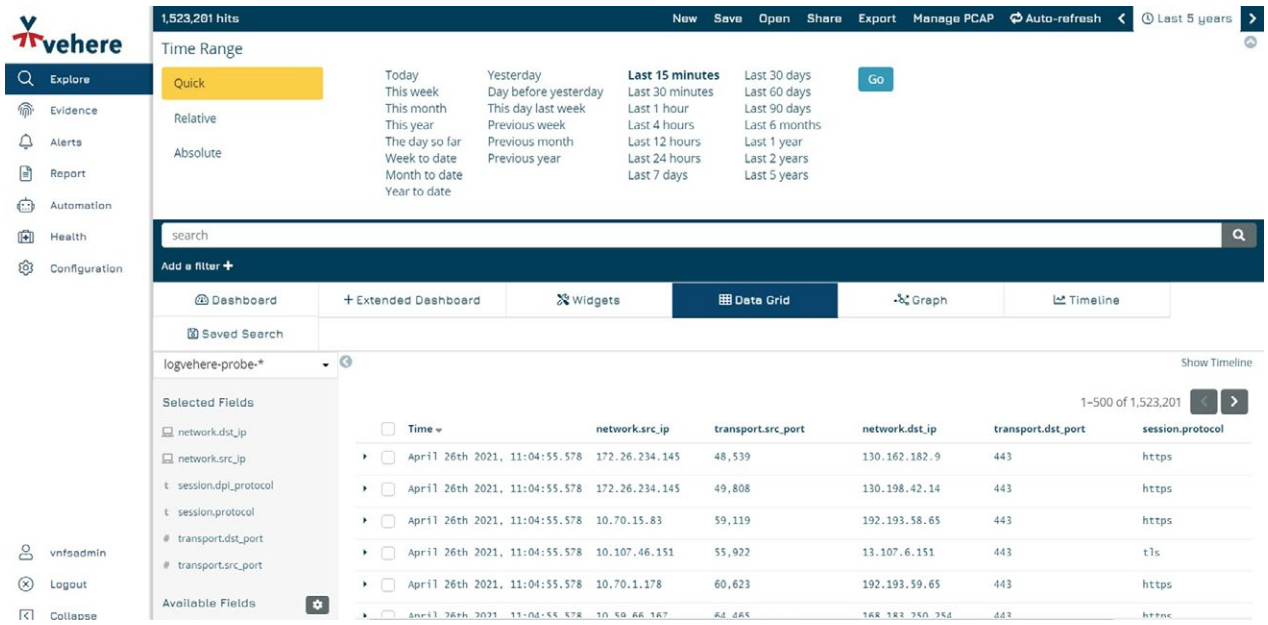
- Location visualization and detailed location based data analysis including geo-fencing capability
- Advanced GIS Search and Geo-fencing for data mining and alerts
- Geo-fencing allows users to create virtual fences using the location services (GPS) on the map. Geo-fencing enables analysts to track Subjects in or out of the defined perimeter.





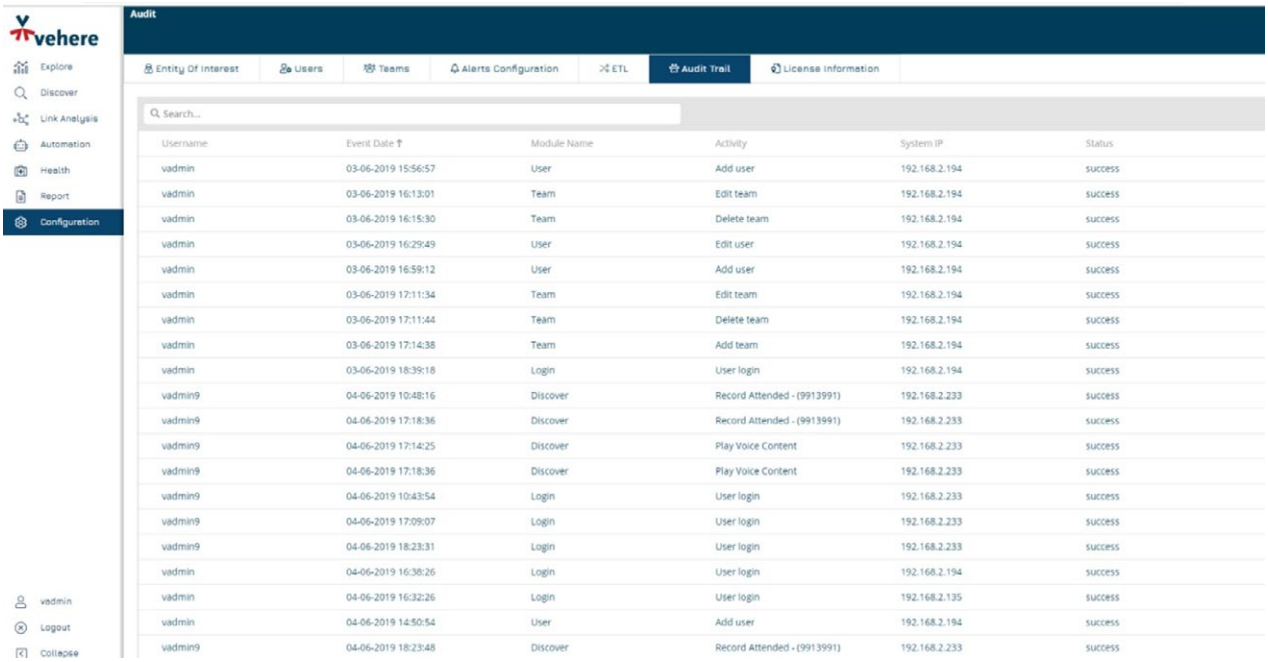
Time travel for Forensics

- Preserves **metadata and full packet captures** (Raw as well as content) for durations spanning several months/ years for forensics analyses as and when required.
- **Timeline Analysis –** When you need to widen or narrow down your window of investigation keeping the presented information same so as to assess change or impact as time moved on. That's the kind of analysis Timeline or Time-Travel allows an analyst to do. This is a fundamental requirement from an incident analysis point of view.



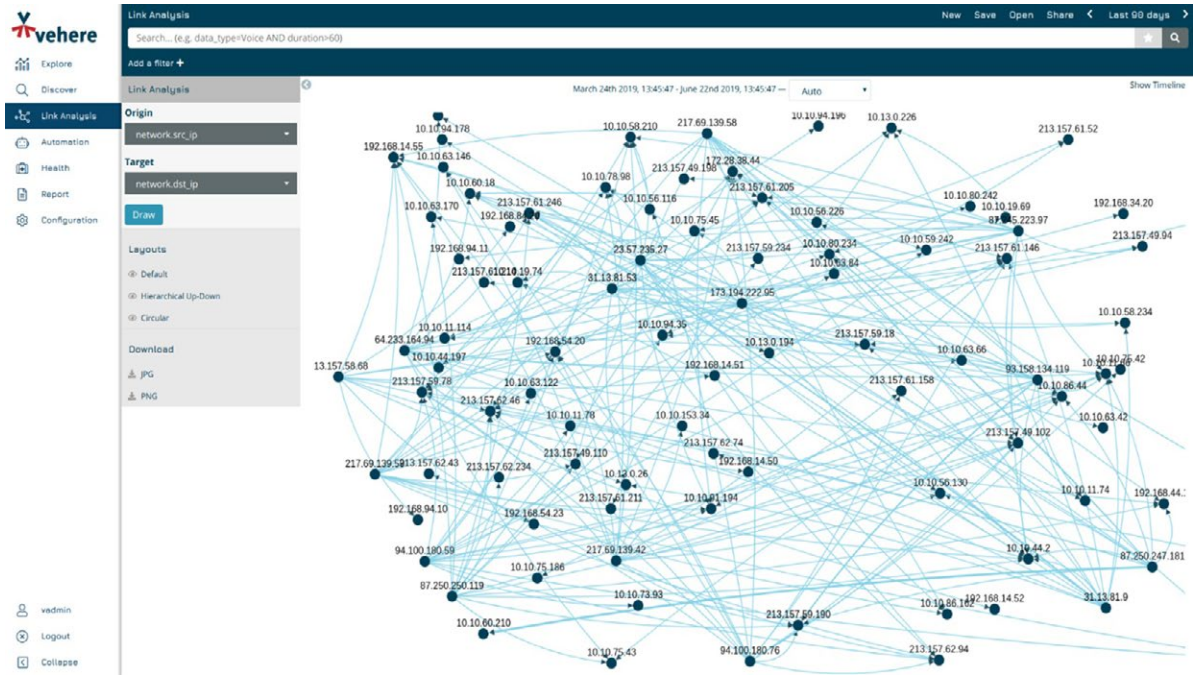
Role Based Access Control (RBAC) and Audit Trail

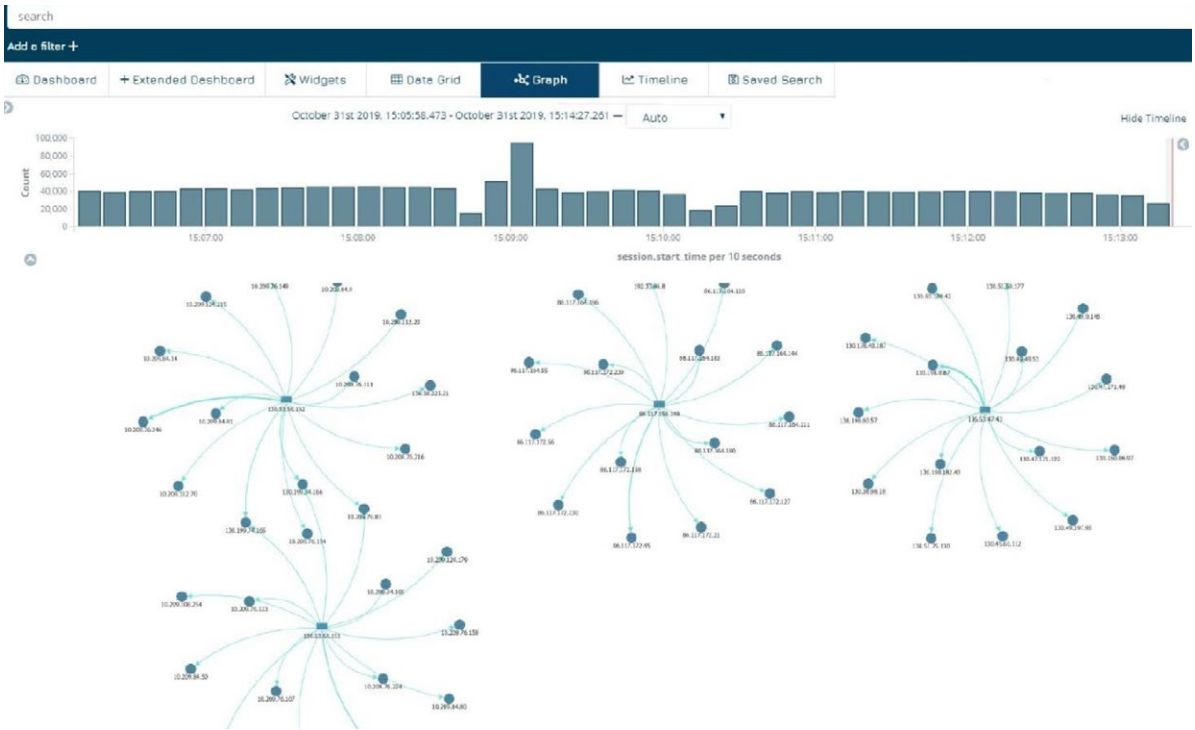
- **RBAC –** Role based access control so that only authorized users can access the data
- **Audit Trail –** The system provides security-relevant chronological records for documentary evidence of the sequence of activities that have affected at any time a specific operation, procedure, or event.



Data Mining Using Link Analysis

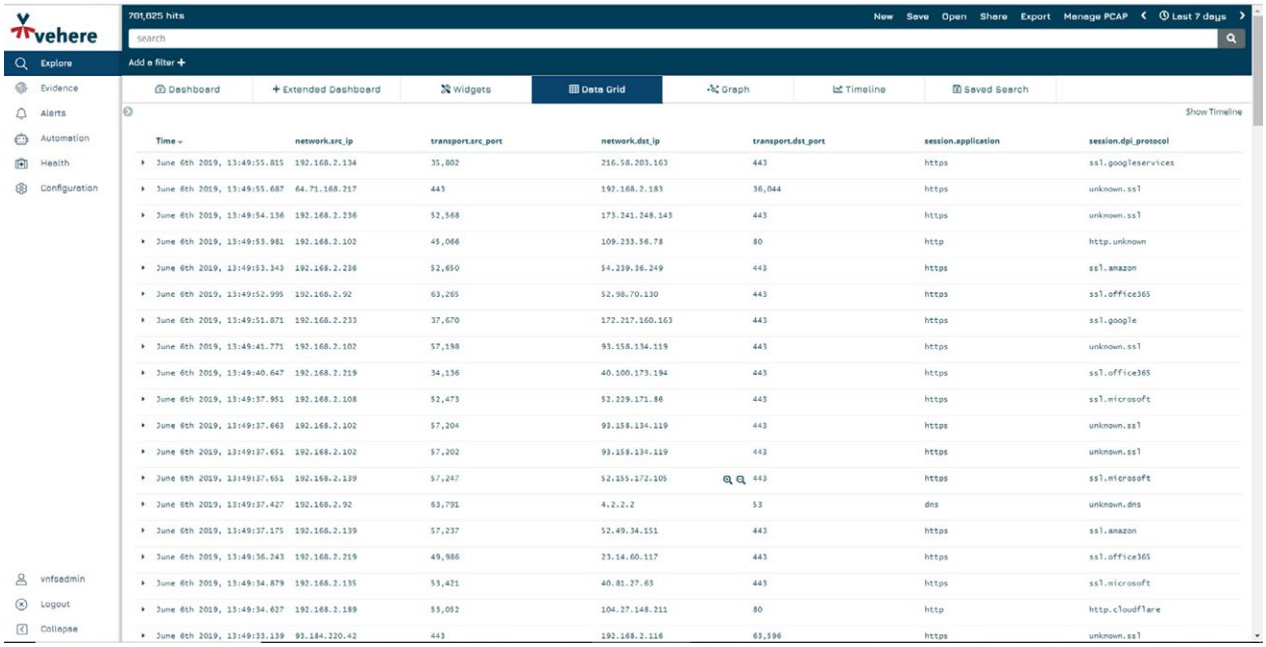
- **Link analysis** is a popular network analysis technique that is used to identify and visualize relationships (links) between different objects. PacketWorker Link Analysis has advanced statistical modelling for data mining.





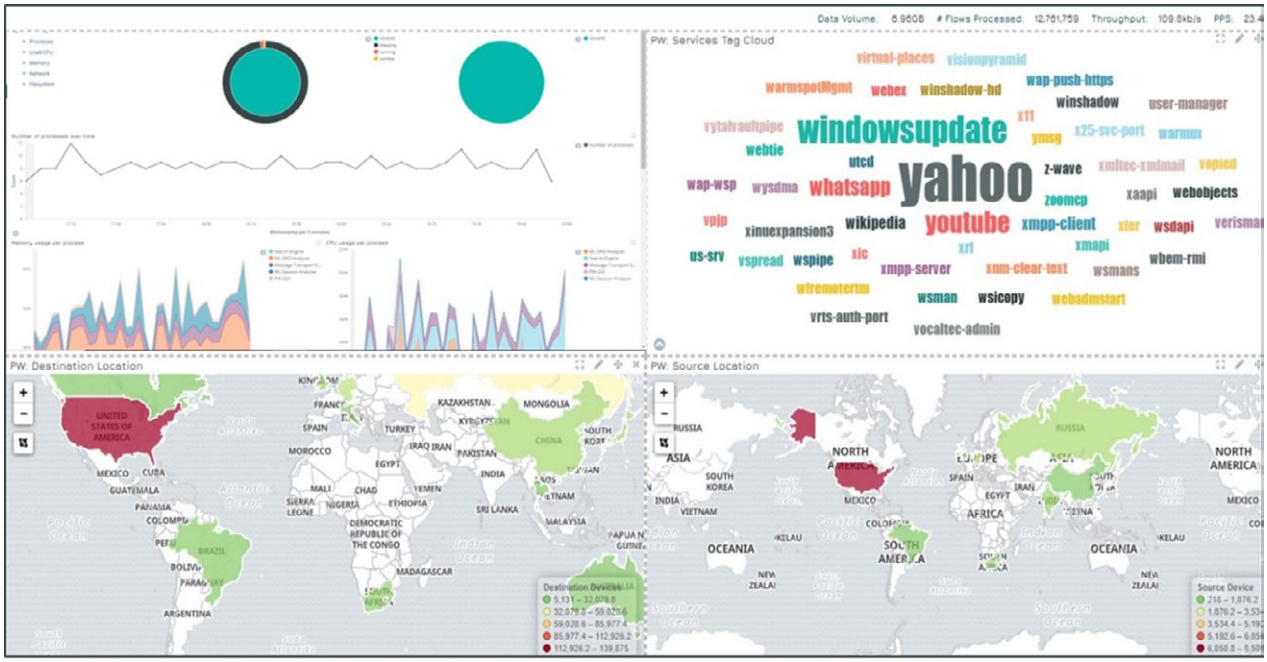
Advanced Free Search Data Mining

- The system allows for free search across all fields e.g If IP<18985 and minimum>=45895 and protocol=SMB and Max_duration>=82



Intuitive Dashboard and Reporting

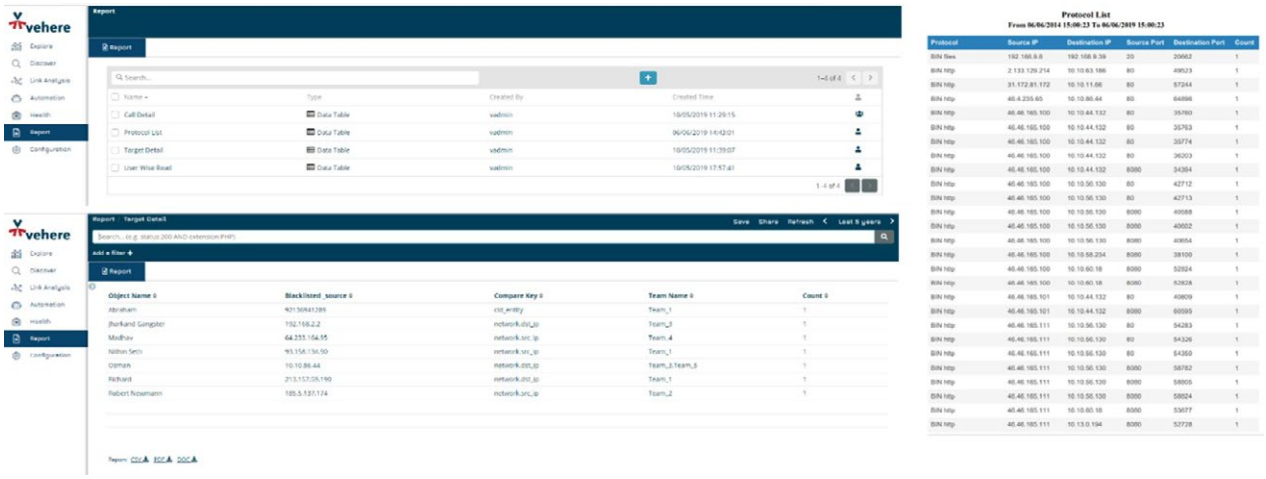
- **Intuitive Dashboard** – Provides real-time view of the current status using intuitive Dashboard. It can be tailored and with the Drill-Down functionality it is very easy get an overview from top to bottom. With a few clicks, you will get to the detailed level which will make it easier to analyze the situation.



Fusion Data Dashboard
(multiple source of data)

System allows to quickly create customized dashboard for analytics

- Advance Reporting – Built-in, in-depth interactivity and customization allows business users to dynamically reshape pre-designed reports for changing business needs with zero training. Ad hoc reporting further empowers business users with direct access to underlying data assets in a governed and secure environment.



Why Network Detection and Response for Power Sector?

Network Detection and Response (NDR) is a burgeoning field of cybersecurity that would enable Power Sector security and network teams to monitor network traffic for malicious actors and suspicious behaviour, and react and respond to the detection of cyber threats to the network. The rise of NDR systems reflects the growing number of system wide attacks by criminal actors ranging from hackers to nation-states.

How did Network Detection and Response evolve?

Monitoring network traffic is not a new practice. In the beginning, network metadata was captured to analyse network performance characteristics. Is our network running okay? But as data volumes soared, many organizations were unable to harness network activity, leaving it as an untapped resource for cyber defense.

Eventually, computing power caught up, giving companies network traffic visibility and behavioural analysis detection methods for computer security – technology first called network traffic analysis (NTA). And while NTA remains a fixture in enterprise security operations centres (SOCs), the market category has evolved and broadened to network detection and response. Organizations increasingly value the response capabilities in NDR solutions to address threats detected by network traffic analysis tools, which focus mainly on detection-only threats and mostly around basic variations of known threats.

Today, increasingly sophisticated behavioural analytics; machine learning; and artificial intelligence (AI) of cloud, virtual, and on-premise networks form the backbone of NDR solutions. By harnessing these technologies, NDR vendors have enabled organizations to improve detection capabilities, determine the confidence and risk level of a threat, and increasingly automate tasks manual tasks performed by analysts such as the acquisition of relevant third-party contextual telemetry information and the application of standardized investigative playbooks to further prioritize threats by risk, thereby enabling them to focus strategically on triage and rapid response. By analysing network behaviour using machine learning models, advanced NDR tools can detect sophisticated evasion methods or “known unknown” cyber threats to brand new zero-day threats or “unknown unknowns.”

How does Network Detection and Response work?

Here’s a quick look at common tools and techniques used by Network Detection and Response solutions:

Machine learning

Machine learning leverages machine computing power to analyse large sets of data in order to make more accurate predictions. With NDR solutions, machine learning models can detect "unknown unknown" threats to your network using behavioural analytics. Machine learning algorithms can see cyber threats coming around the corner (e.g., ports suddenly being used that have never been used before), in turn enabling more rapid triage and mitigation. Machine learning models are also used to continually reweigh prioritization of potential threats based on real-world outcomes.

Deep learning

Deep learning is a powerful form of machine learning that uses artificial neural networks to enhance NDR capabilities. At Vehere, we use deep learning after customizing its use to the NDR applications that are well-suited to the training data requirements and interpretability challenges of deep learning models.

Statistical analysis

Statistical analysis is a useful behavioural technique that is sometimes marketed as "AI" by a handful of NDR providers. These can range from simple outlier analysis (e.g., which URL has not been seen in this group of devices) to basic Bayesian analysis of network traffic pattern to other statistical methods. Commonly there is an element of sample to determine a baseline that is then used to identify which activity deviates from normal traffic usage, allowing SOCs to model normal network traffic and highlight suspicious traffic that falls outside the normal range.

Heuristics

Heuristic analysis detects threats by analysing data for suspicious properties. In NDR solutions, heuristics extend the power of signature-based detection methods to look beyond known threats and spot suspicious characteristics found in unknown threats and modified versions of existing threats. Some network sandbox vendors position analysis of file-based malwares as a variation of network behavioural analysis.

Threat Intelligence Feeds

Threat intelligence feeds are data streams containing information on previously identified cyber threats. Threat intelligence, if timely and actionable, can assist NDR solutions in identifying known threats or providing additional contextualization for prioritization of a detected network anomaly by risk. The limitation of threat intel feeds is the need to actively procure, manage, and curate threat intel so that the information is relevant and timely to the enterprise, which can be beyond the scope of all but the most security mature enterprises.

Signatures

Signature-based detection methods use a unique indicator of compromise (IOC) identifier about a known threat to identify that threat in the future. Signatures were effective a generation ago, but the process of using unique identifiers to guard against known threats has become increasingly ineffective in a world where custom malware, malware toolkits, and non-malware based attacks such as credential replay are the norm. Furthermore, nearly three quarters of all network traffic today is encrypted, part of an upward trend that's rendering signature-based tools ineffective by preventing the content inspection required to match certain categories of IOCs.