
CYBER
SECURITY.

TEAM MEMBERS:

ADI MEGHANA JYOTHI

ADARI PADMA SRI

MORTHA SUDHEER

DOGGA NAGAMANIKNTA

INTRODUCTION:

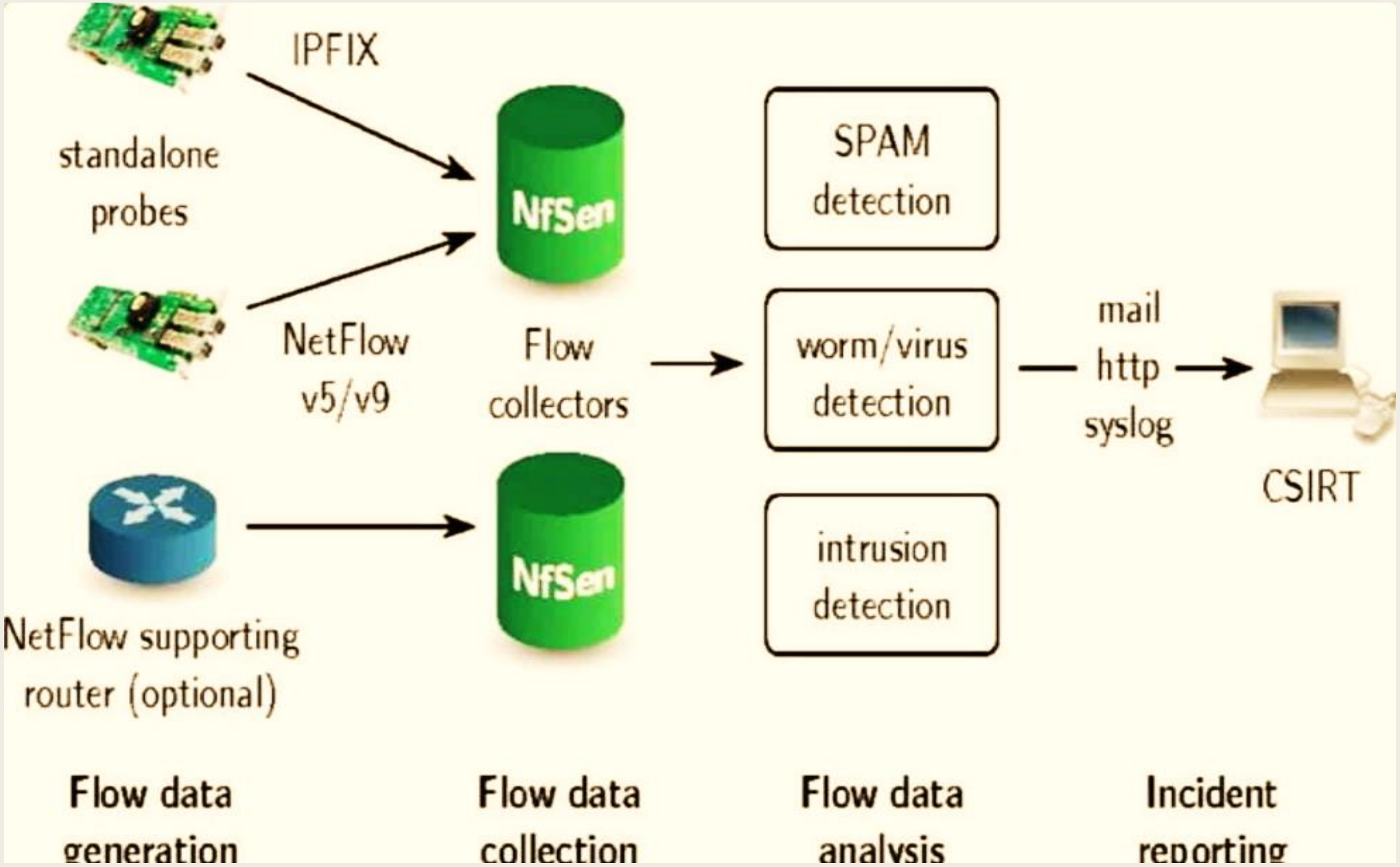
- Network traffic analysis have been the most spoken topic nowadays.
- Network traffic analysis techniques allow the traffic at a particular points on a network to be recorded displayed in useful form and analysed.
- Traffic can be monitored at the network boundary on specific segments at a particular interfaces.
- Network traffic analysis can easily be detected using various network analyzers.

WHAT IS CYBER SECURITY:

- Computer security cyber security or information technology security is the protection of a computer system and networks from information disclosure theft of or damage to their hardware software or electronic data as well as from the disruption or miss direction of the service they provide.
- Cyber security is the application of technology processes and controls to protect systems network programs devices in data from cyber attacks.
- It AIIMS to reduce the risk of cyber attacks in protect against the unauthorised explosion of system network and technologies
- Cyber security is important because it protects categorizes of data from theft and damage

WHAT IS NETWORK TRAFFIC ANALYSIS ?

- Network traffic analysis is a method of monetary network availability in activity to identify anomalies including security and operation issues.
- Common news cases of network traffic analysis Includes collecting a real time and historical record of what happening on your network detecting malware such as ransomware activity.
- Network traffic analysis is primarily done to get independence in depth inside into what type of traffic network packets or data is flowing through a network


IPFIX
standalone probes
NetFlow v5/v9
NfSen
Flow collectors
SPAM detection
worm/virus detection
intrusion detection
mail
http
syslog
CSIRT
NetFlow supporting router (optional)
NfSen
Flow data generation
Flow data collection
Flow data analysis
Incident reporting

NEED OF NETWORK TRAFFIC ANALYSIS:

- Gain special knowledge about the network
- Investigate and troubleshoot abnormal behaviour

-Abnormal packets

-Network slow performance

1. Congestion
2. Retransmission

-Unexpected traffic

-Broken application-Load balance issue

- Network forensenics

-Collecting evidence

-incident handling

-tracing attacks

-linking infected host

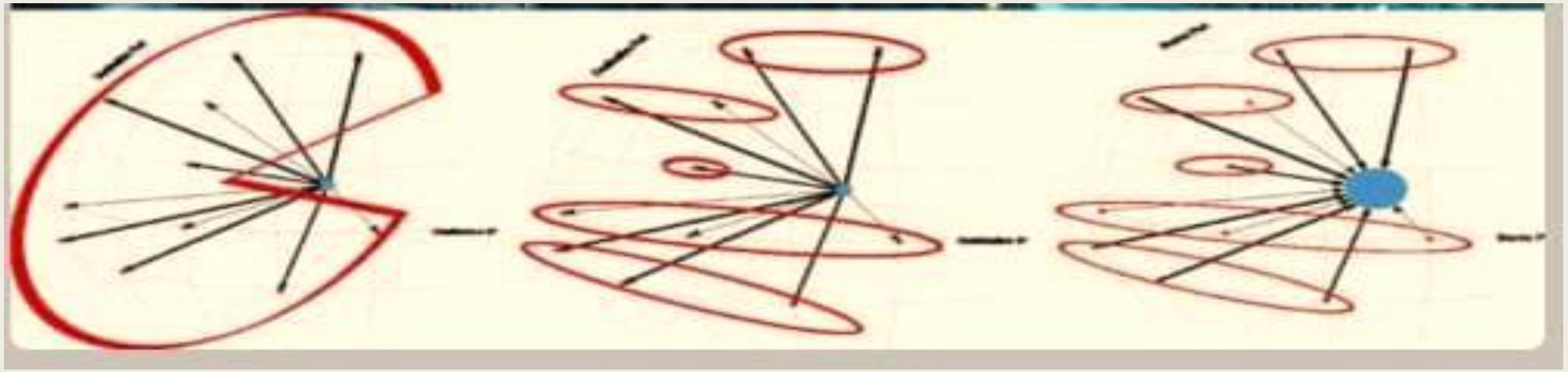
-determining patient zero

- Stealing sensitive information
- Pen testing
- Developing IPS and IDS signatures
- Troubleshoot problems
- Analyse the performance of network sections to identify bottlenecks
- Network instruction detection
- Logging network traffic for forsenic evidence

- Analysing the operation of network application
- Tracing the source of dos attack
- Detecting spyware and compromised hosts possibly a botnet member
- To capture clear text usernames and password and those which are trivially encrypted
- To passively map a network
- To capture other confidential information

HOW TO SOLVE NETWORK TRAFFIC ?

- Identify what applications are protocols are running on the network
- Identify band with hogs down to a user application or device level
- Monitor client to serve network traffic
- Troubleshoot network and application performance issues



FEATURES OF NETWORK TRAFFIC ANALYSIS

- Broad visibility

Whether the network communication in a question are traditional TCP IP style package virtual network traffic crossing from a switch or a traffic from and with cloud were clothes API calls to SAS applications are serverless computing instances network traffic analysis tools have the ability to monitor and analyse a broad variety of communication in real time

- Encrypted traffic analysis

With over 70% of web traffic encrypted organisations need and accessible method for decorating their network traffic without destructing data privacy implications network traffic analysis solutions delivers on this challenge by enabling security professionals to uncover network threats by analysing the payload with out actually peeking into it

- Entity tracking

Network traffic analysis products offers the ability to track and profile all entities on a network including the devices users applications and destinations and more machine learning and analytics then attributes and behaviours and relationships to the named entities provide infinity more value to organisations and static list of IP address

- Detection and response

Because NDA tools attributes behaviours to entities ample context is available for detection and response work flows this means security professionals no longer needs to shift through multiple data source such as DHCP and DNS locks configuration management database and directory service infrastructure in an atom to gain comprehensive visibility instead they can quickly detect anomalies decisively track them down and determine the root use and react accordingly

- Comprehensive baseline

To keep up with everything modern it environments network traffic analysis solutions track behaviours that are unique to an entity or a small number of entities in a comparison to the bulk of entities in an environment the underline data is available immediately at and t a machine learning baselines evolve in real time as behaviour change also with the tracking capabilities NTA baselines are even more comprehensive as they can understand the source and destination entities in addition to traffic patterns for instance what might be normal for a workstation is not normal for the server or IP phone or camera

NETWORK ANALYZERS

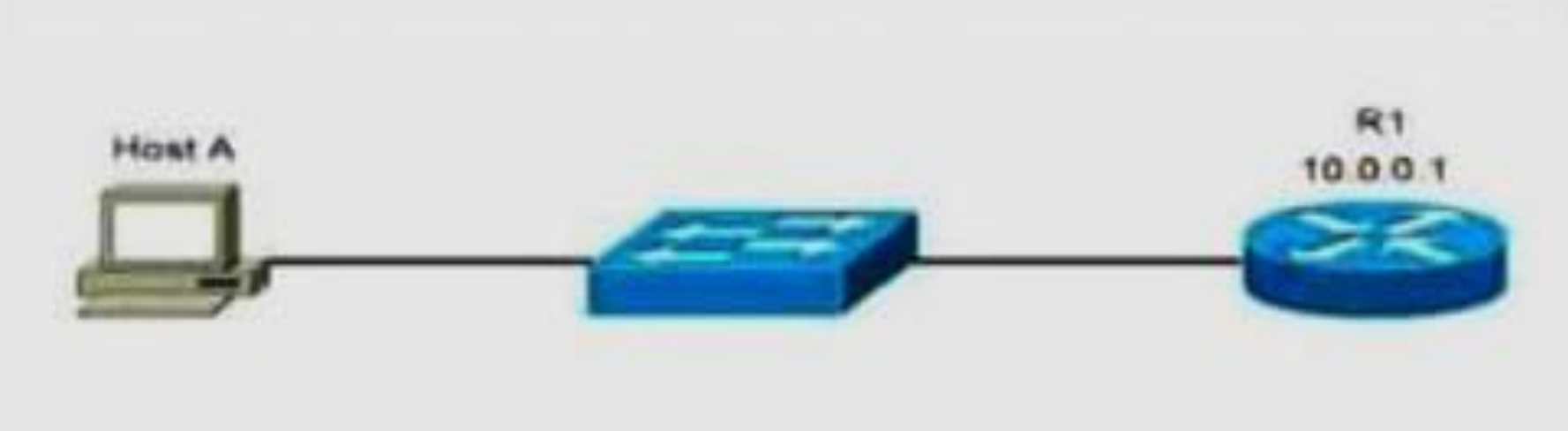
- Wireshark
- NMAP cli and gui
- Network associates sniffer
- TCP dump based basic command line utility Unix
- Windows network monitor includes with windows server Oss
- Snort
- Dsniff
- Ettercap

IMPORTANCE OF NETWORK TRAFFIC ANALYSIS

- Keeping a close eye on your network perimeter is always good practice even with strong firewalls in a place mistakes can happen and rogue traffic good get through
- Uses could also leverage methods such as tunneling external anonymizers ,and vpns to get around firewall rules
- A network monitoring solution should be able to detect activity indicator of ransomware attacks via insecure protocols take one a cry for example where attackers at Delhi stand for network with TCP port 445 open and then used a vulnerability in smbv1 to access network file shares

- Remote desktop protocol is another commonly targeted application make sure you blocked any inbound connection attempts on your firewall
- Monitoring traffic inside your firewall allows you to validate rules gain valuable inside and can also be used as a source of network traffic based alerts
- Monitoring traffic inside a firewall allows you to validate rules gain vulnerable inside and can also be used as a source of network traffic based alerts
- CLI strings may reveal login procedures presentation of user predictions commands to display boot or running configuration copying files and more

- Be sure to check your network data for any device running unencrypted management protocol such as
- Telnet
- Hypertext transfer protocol HTTP port 80
- Simple network management protocol SNMP ,port 161/161
- Cisco smart install SMI port 4786




Device Explorer
Current Report
Report:
Auto refresh
Device Interface
Flow Templates
Inbound Results 1 - 10 of 684 (5.20s)

USECASE FOR ANALYZING NETWORK TRAFFIC

- Detection of ransomware activity
- Monitoring data exfiltration/ internet activity
- Monitor access to files on file server or MSSQL database
- Track a users activity on the network through user forensic reporting
- Provide and inventory of what device servers and services are running on the network
- Highlight and identity dude causes of bandwidth peaks on the network
- Provide real time dashboards focusing on network and user activity
- Generate network activity reports for management and auditors for any time period

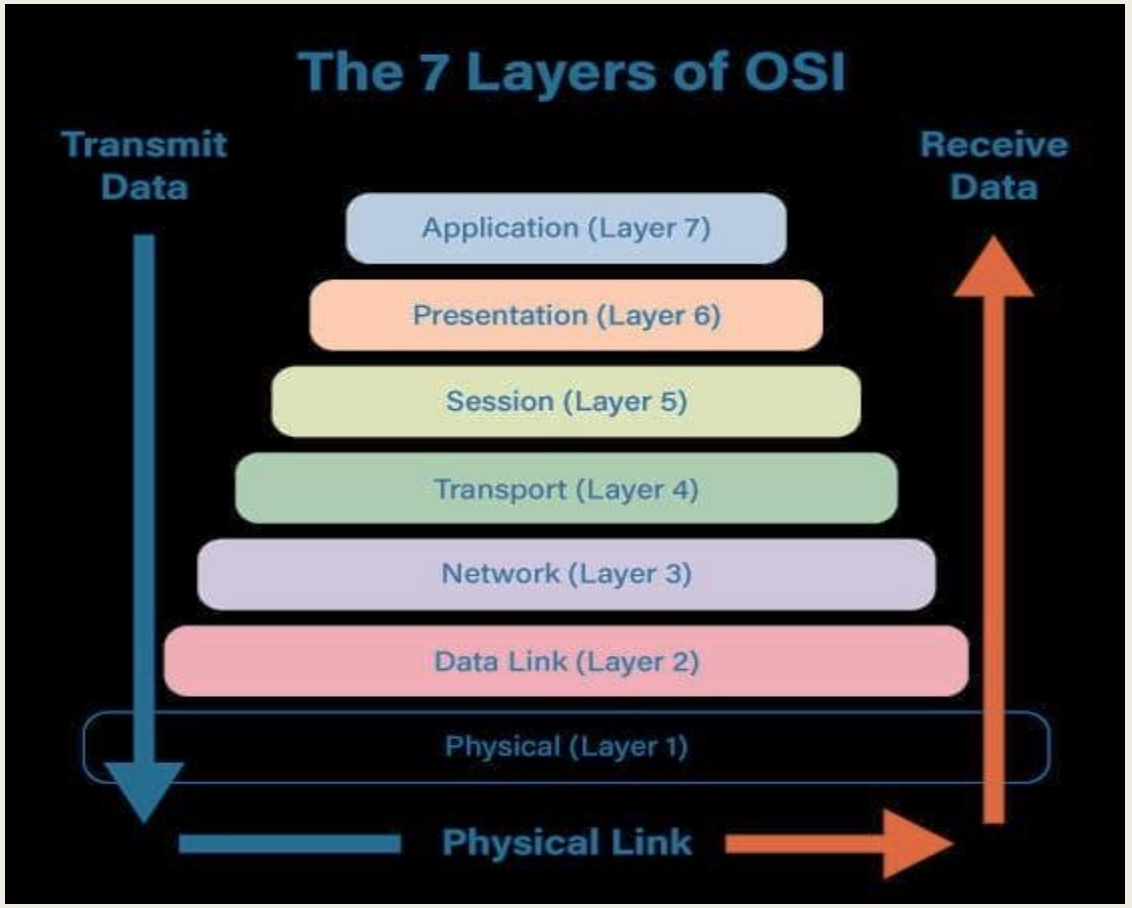
WHAT TO LOOK FOR IN A NETWORK TRAFFIC ANALYSIS

- Not all tools for managing network traffic are same. Generally, they can be broke down into two types: flow based tools and deep packet inspection tools.
- Within they stools you will have options for software agents storing historical data and historical data ,and intrusion detection systems
- When evaluating which solution is right for your organisation considered this five things

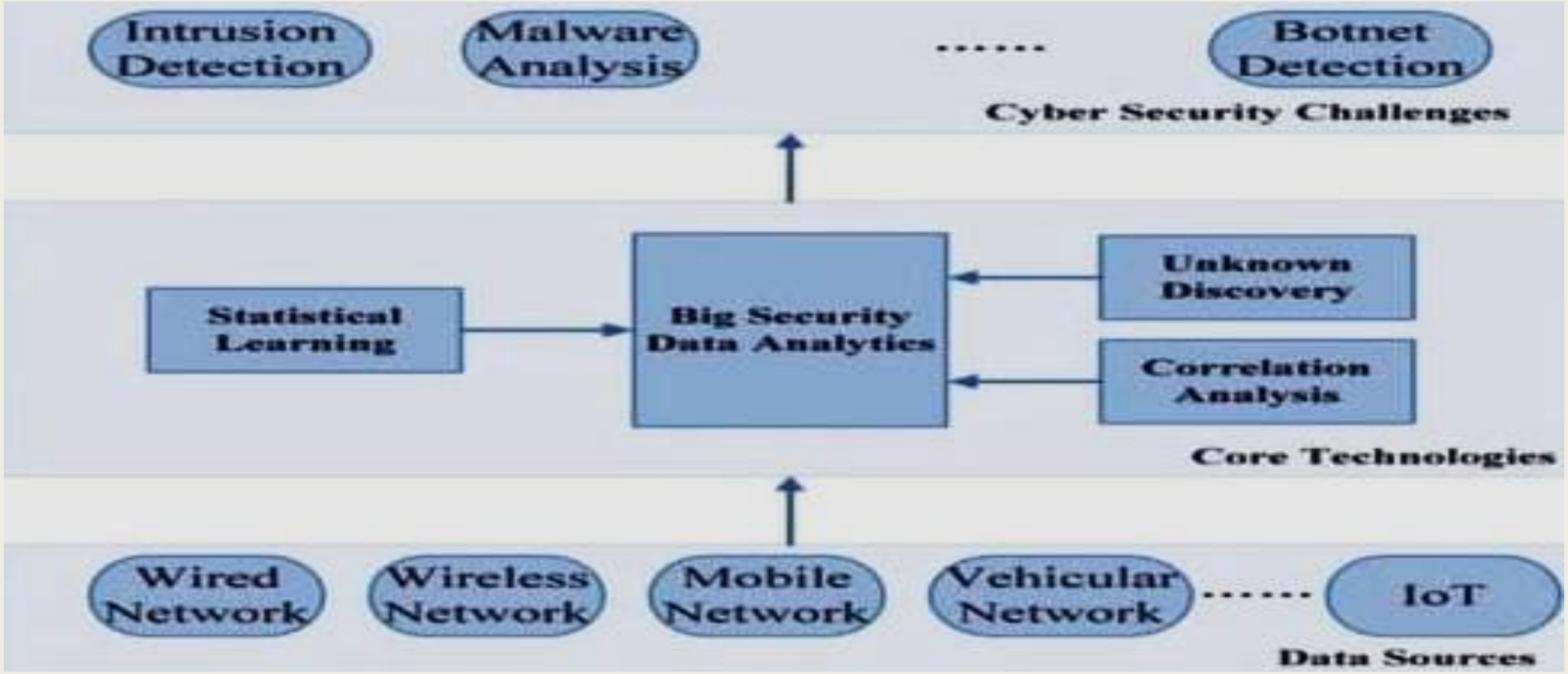
1. Availability of flow-enable devices
2. The data source
3. The points on the network
4. Real time data vs historical data
5. Full packet capture cost and complexity

NETWORK PROTOCOLS

- There are totally 7 layers of Protocols for analysing network traffic



ARCHITECTURE DIAGRAM



CONCLUSION

- Network traffic analysis is an essential way to monitor network availability in activity to identify anomalous maximize performance and keep and eye I out for attacks
- Alongside log aggregation UEBA , and endpoint data network traffic is a core piece of comprehensive visibility and security analysis to discover threats early and extinguish them fast.
- When choosing a NTA solution , consider the current blind spot on your network the data source you need information from and the critical points on the network where they convert for efficient monitoring with NTA added as a layer to the security information and event management solution you will gain visibility into even more of your environment and your users

FUTURE SCOPE

This can be further enhance to

- Fault management
- Alerts and threshold
- Windows even log monitoring
- Traffic management
- Network security
- Network scheduling