

NETWORK TRAFFIC ANALYSIS WITH CYBER SECURITY



CONTENTS

- INTRODUCTION
- WHAT IS CYBER SECURITY?
- WHAT IS NETWORK TRAFFIC ANALYSIS?
- NEED OF NETWORK ANALYSIS
- HOW TO SOLVE NETWORK TRAFFIC?
- FEATURES OF NETWORK TRAFFIC ANALYSIS
- NETWORK ANALYZERS
- IMPORTANCE OF NETWORK TRAFFIC ANALYSIS
- USE CASES FOR ANALYSING NETWORK TRAFFIC
- WHAT TO LOOK FOR IN A NETWORK TRAFFIC ANALYSIS
- NETWORK PROTOCOLS
- ARCHITECTURE DIAGRAM
- CONCLUSION

INTRODUCTION

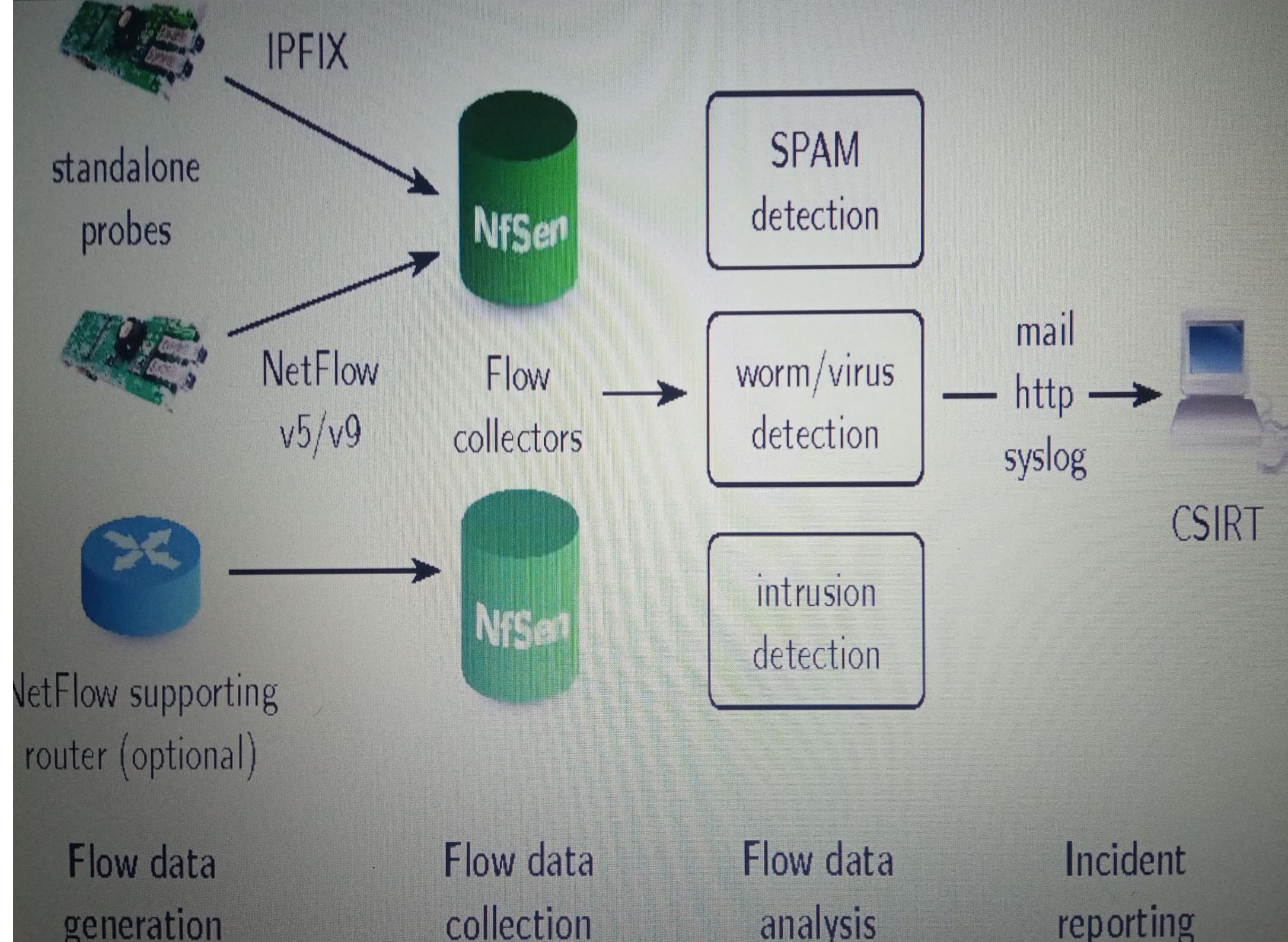
- Network traffic analysis have been the most spoken topic nowadays.
- Network traffic analysis techniques allow the traffic at particular points on a network to be recorded displayed in useful form and analyzed.
- Traffic can be monitored at the network boundary on specific segments at particular interfaces.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

WHAT IS CYBER SECURITY?

- Computer security, cybersecurity or information technology security is the protection of computer systems and networks from information disclosure, theft of or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide.
- **Cyber security** is the application of technologies, processes and controls to protect systems, networks, programs, devices and data from **cyber attacks**.
- It aims to reduce the risk of **cyber attacks** and protect against the unauthorised exploitation of systems, networks and technologies.
- **Cybersecurity** is important because it protects all categories of data from theft and damage.

WHAT IS NETWORK TRAFFIC ANALYSIS?

- Network traffic analysis (NTA) is a method of monitoring network availability and activity to identify anomalies, including security and operational issues.
- Common use cases for NTA include: Collecting a real-time and historical record of what's happening on your network. Detecting malware such as ransomware activity.
- Network traffic analysis is primarily done to get in-depth insight into what type of traffic/network packets or data is flowing through a network.



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 applications
 - Load balancer issues

- Network forensics
 - Collecting evidence
 - Incident Handling
 - Tracing attacks
 - Linking infected hosts
 - Determining patient zero
- Stealing Sensitive information
- Pen-testing
- Developing IPS/IDS signatures
- Troubleshoot problems
- Analyse the performance of network sections to identify bottlenecks

- Network intrusion detection
- Logging network traffic for forensic evidence
- Analysing the operation of network applications
- Tracing the source of DoS attack
- Detecting spyware and compromised hosts possibly a botnet member
- To capture clear-text usernames and passwords and those which are trivially encrypted
- To passively map a network
- To passively fingerprint the OS of network hosts
- To capture other confidential information

FEATURES OF NETWORK TRAFFIC ANALYSIS

- **Broad Visibility**
 - Whether the network communications in question are traditional TCP/IP style packets, virtual network traffic crossing from a vSwitch, traffic from and within cloud workloads, API calls to SaaS applications, or serverless computing instances, NTA tools have the ability to monitor and analyze a broad variety of communications in real-time.
- **Encrypted Traffic Analysis**

With over 70 percent of web traffic encrypted, organizations need an accessible method for decrypting their network traffic without disrupting data privacy implications. NTA solutions deliver on this challenge by enabling security professionals to uncover network threats by analyzing the full payload without actually peeking into it.

NETWORK ANALYZERS

- Wireshark
- NMAP cli and gui
- Network Associates Sniffer
- TCP Dump based basic command line utility (UNIX)
- Windows Network Monitor included with windows server Oss
- Snort
- Dsniff
- Ettercap

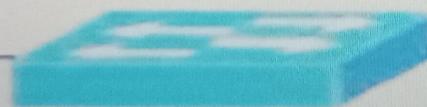
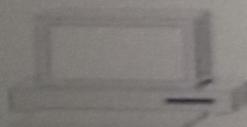
IMPORTANCE OF NETWORK TRAFFIC ANALYSIS

- Keeping a close eye on your network perimeter is always good practice. Even with strong firewalls in place, mistakes can happen and rogue traffic could get through.
- Users 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 indicative of ransomware attacks via insecure protocols. Take WannaCry, for example, where attackers actively scanned for networks with TCP port 445 open, and then used a vulnerability in SMBv1 to access network file shares.

- Remote Desktop Protocol (RDP) is another commonly targeted application. Make sure you block any inbound connection attempts on your firewall.
- Monitoring traffic inside your firewalls allows you to validate rules, gain valuable insight, and can also be used as a source of network traffic-based alerts.
- Monitoring traffic inside your firewalls allows you to validate rules, gain valuable insight, and can also be used as a source of network traffic-based alerts.

- CLI strings may reveal login procedures, presentation of user credentials, commands to display boot or running configuration, copying files, and more.
- Be sure to check your network data for any devices running unencrypted management protocols, such as:
 - Telnet
 - Hypertext Transport Protocol (HTTP, port 80)
 - Simple Network Management Protocol (SNMP, ports 161/162)
 - Cisco Smart Install (SMI port 4786)

Host A



R1
10.0.0.1



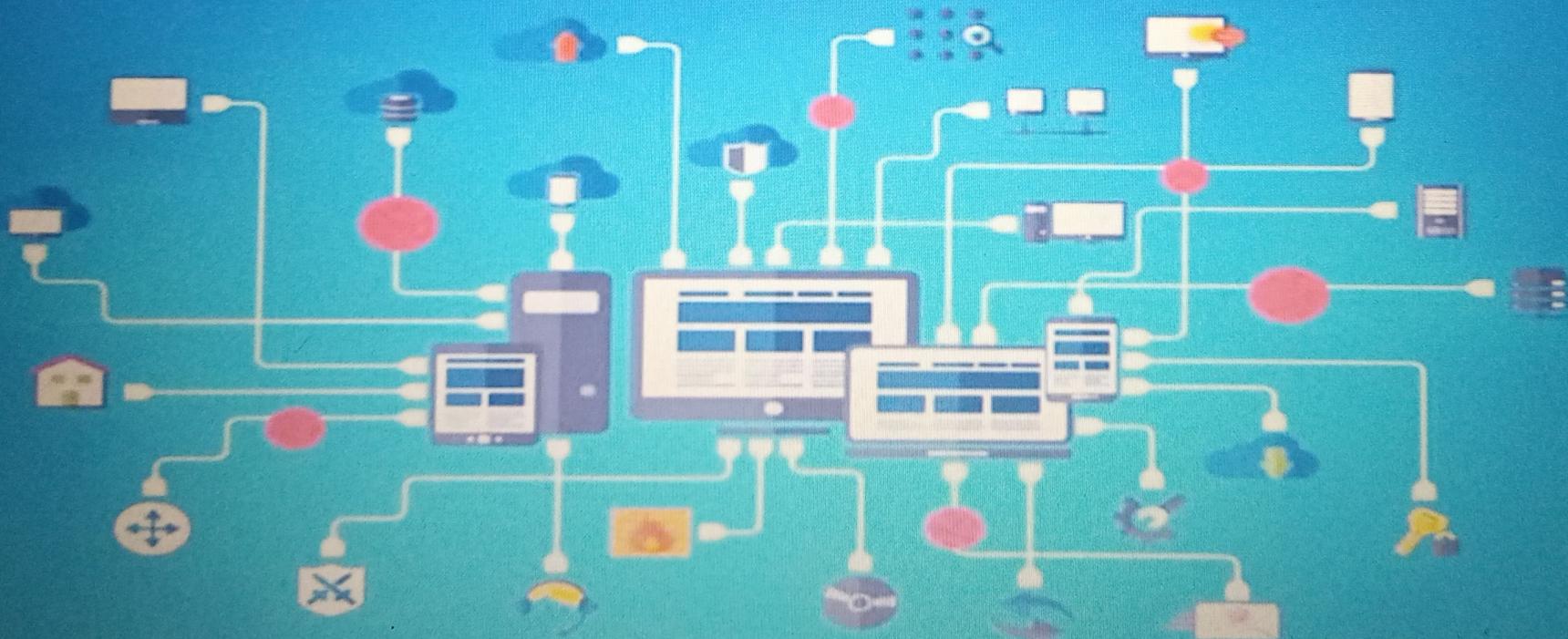
USECASES FOR ANALYZING NETWORK TRAFFIC

- Detection of ransomware activity
- Monitoring data exfiltration/internet activity
- Monitor access to files on file servers or MSSQL databases
- Track a user's activity on the network, through User Forensics reporting
- Provide an inventory of what devices, servers and services are running on the network
- Highlight and identify root cause 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

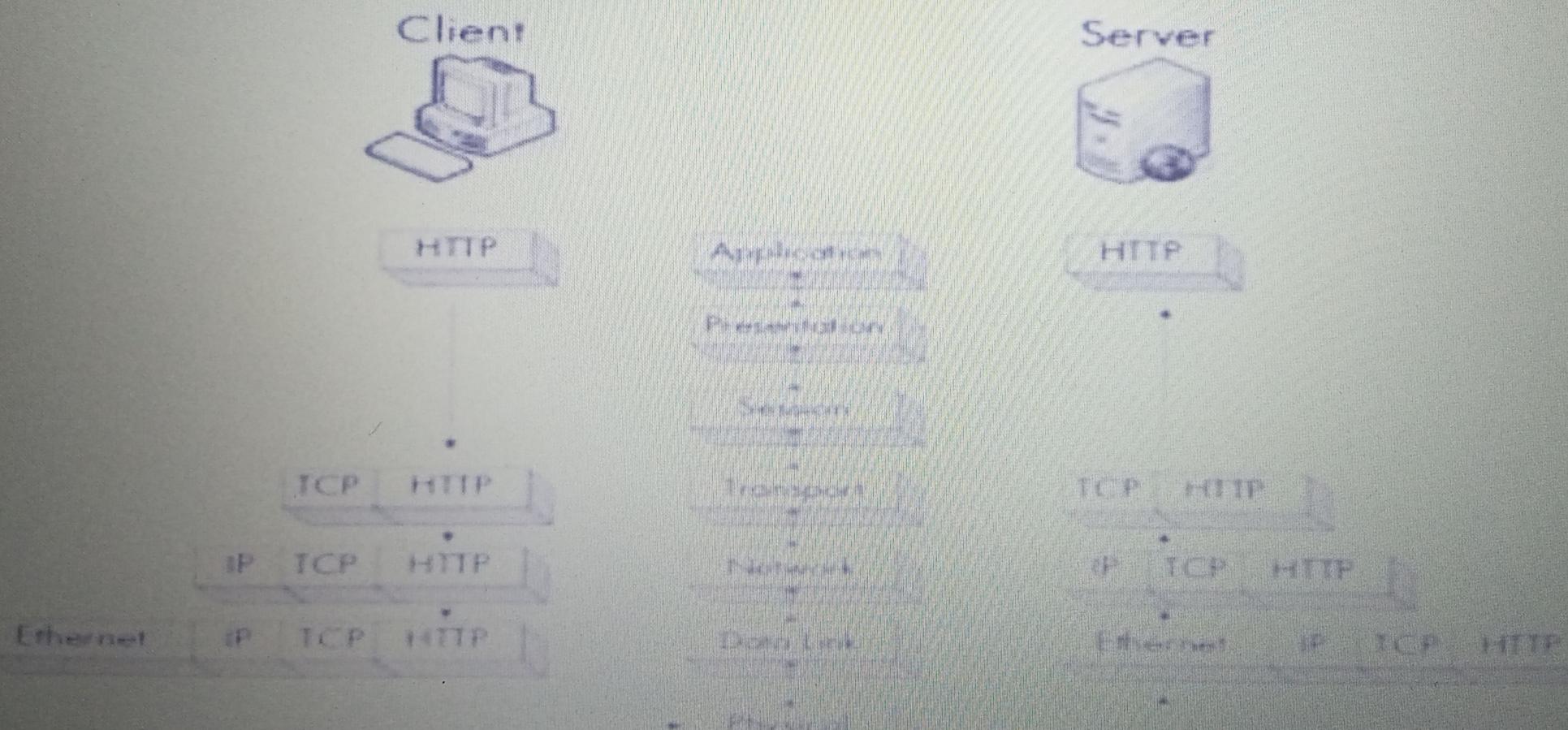
- Not all tools for monitoring network traffic are the same. Generally, they can be broken down into two types: flow-based tools and deep packet inspection (DPI) tools.
- Within these tools you'll have options for software agents, storing historical data, and intrusion detection systems.
- When evaluating which solution is right for your organization, consider these five things:

1. Availability of flow-enabled 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

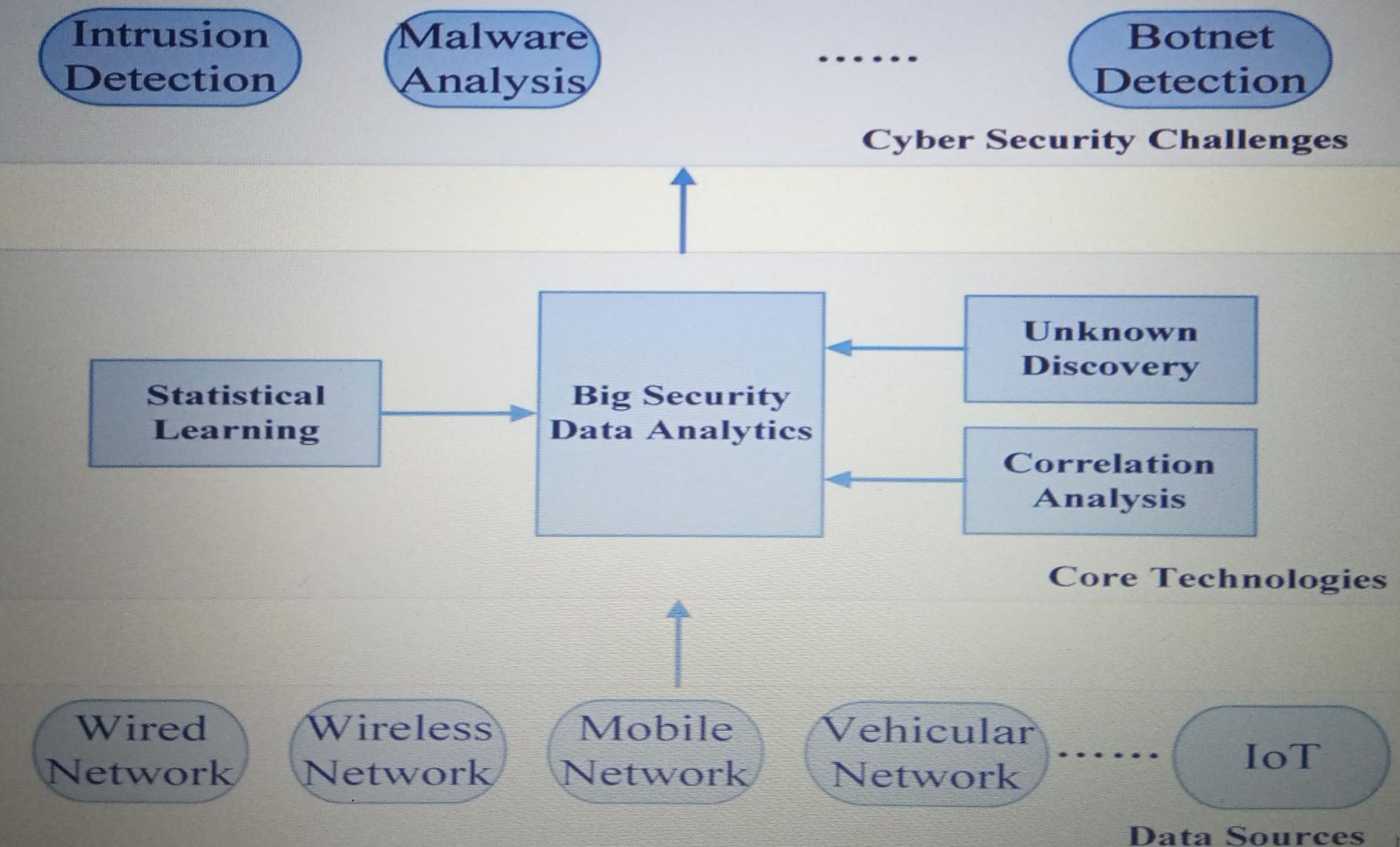


NETWORK PROTOCOLS

- There are totally 7 layers of protocols for analyzing network traffic



ARCHITECTURE DIAGRAM



CONCLUSION

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

FUTURE SCOPE

- This can be further enhanced to
 - Fault management
 - Alerts and Threshold
 - Windows event log monitoring
 - Traffic management
 - Network Security
 - Network scheduling