NETWORK TRAFFIC ANALYSIS WITH CYBER SECURITY

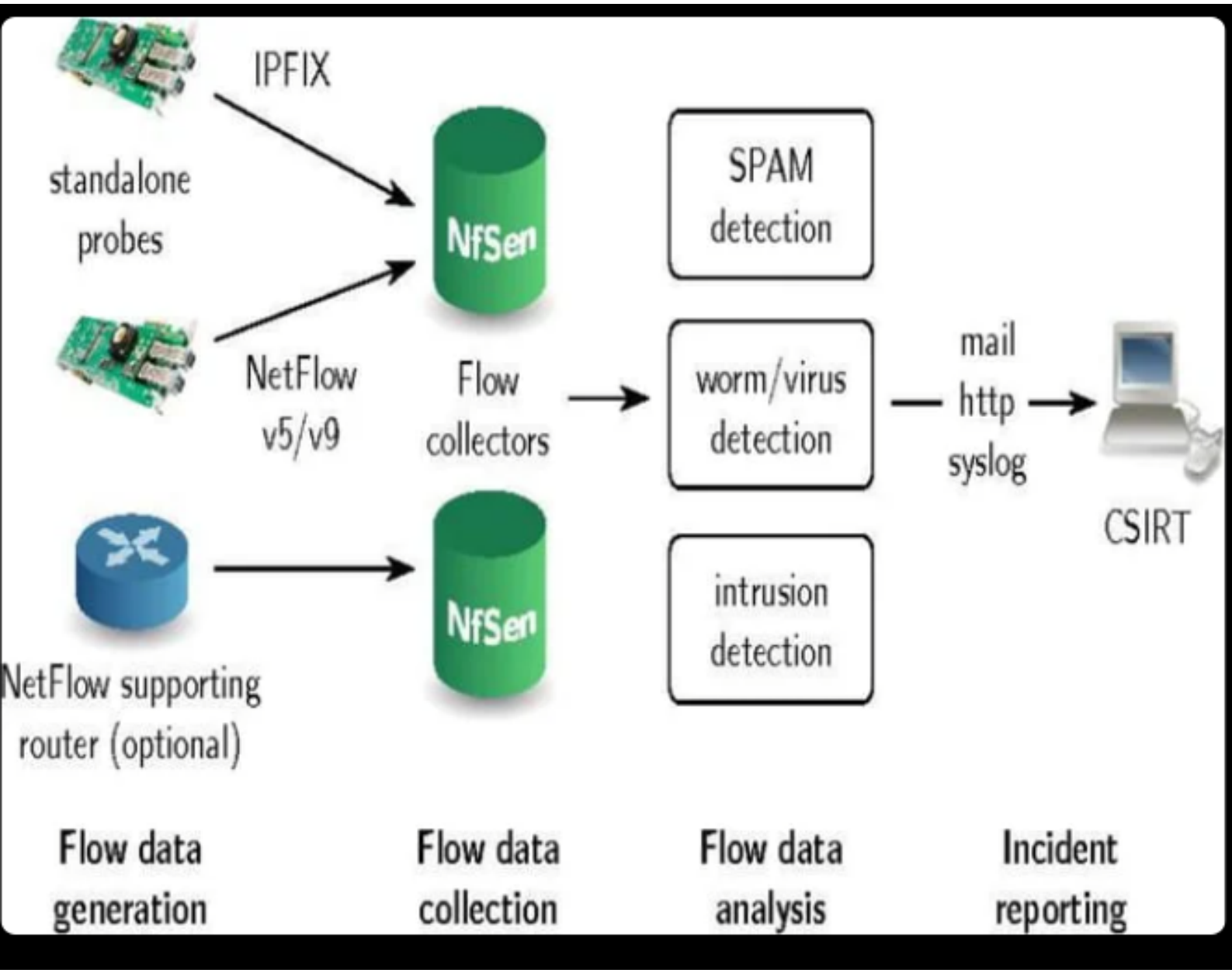
PRESENTED BY
JONNA ANKITHA

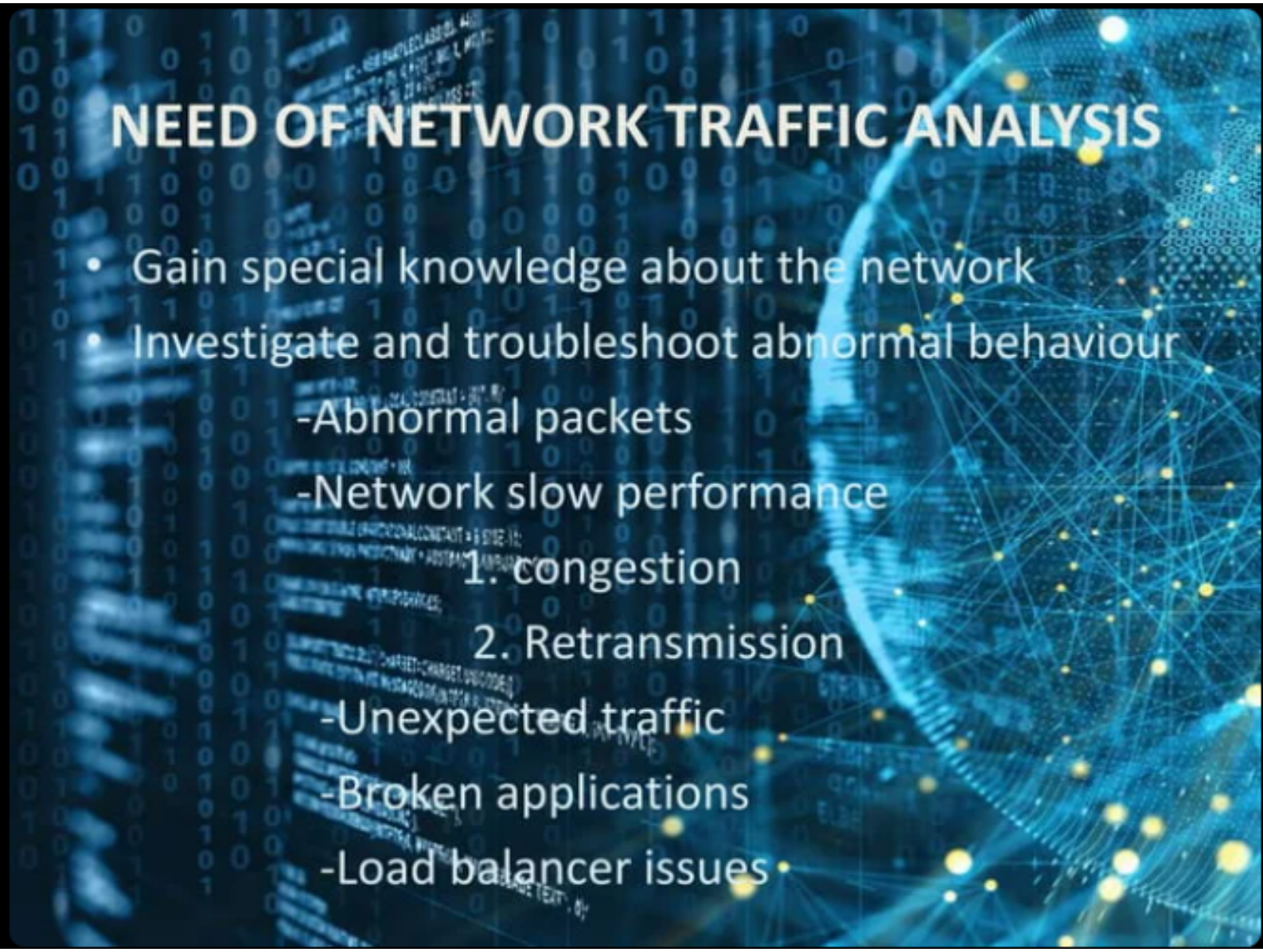
CONTENTS

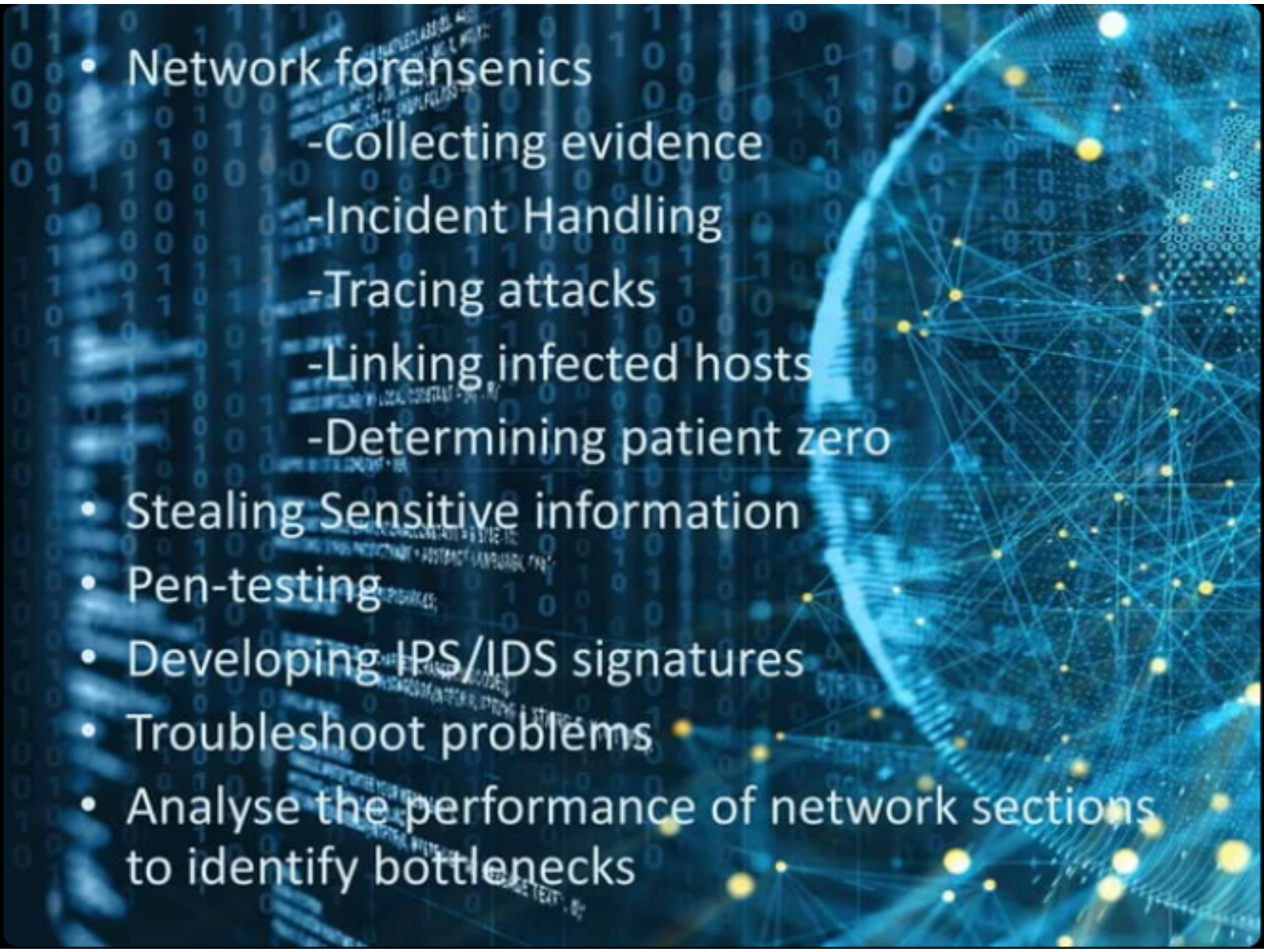

WHAT IS CYBER SECURITY?
•Computer security, cybersecurity or information technology security is the protection of computer systems and networks from information disclosure, theft of or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services 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.

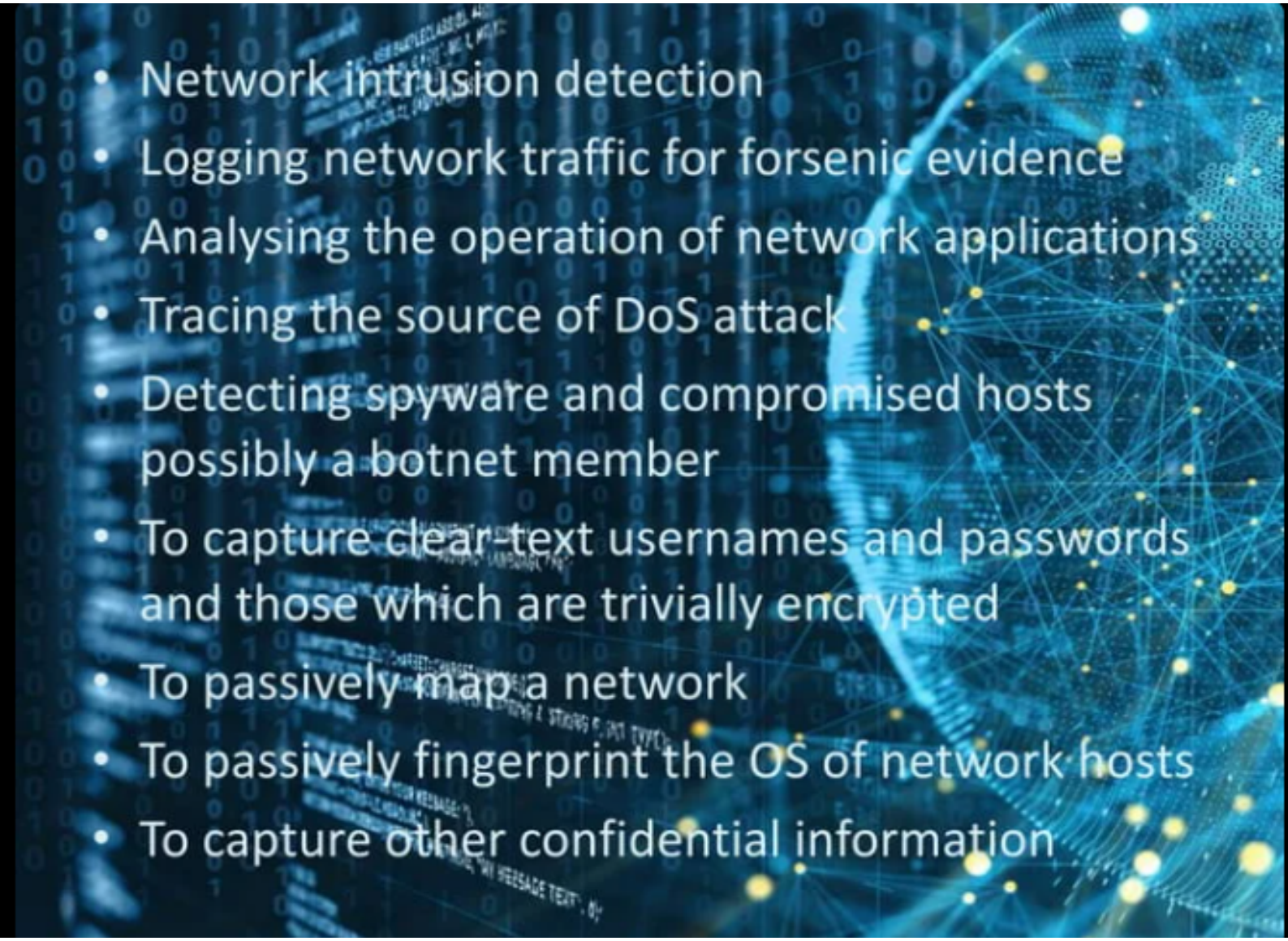
WHAT IS NETWORK TRAFFIC ANALYSIS?

- **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


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

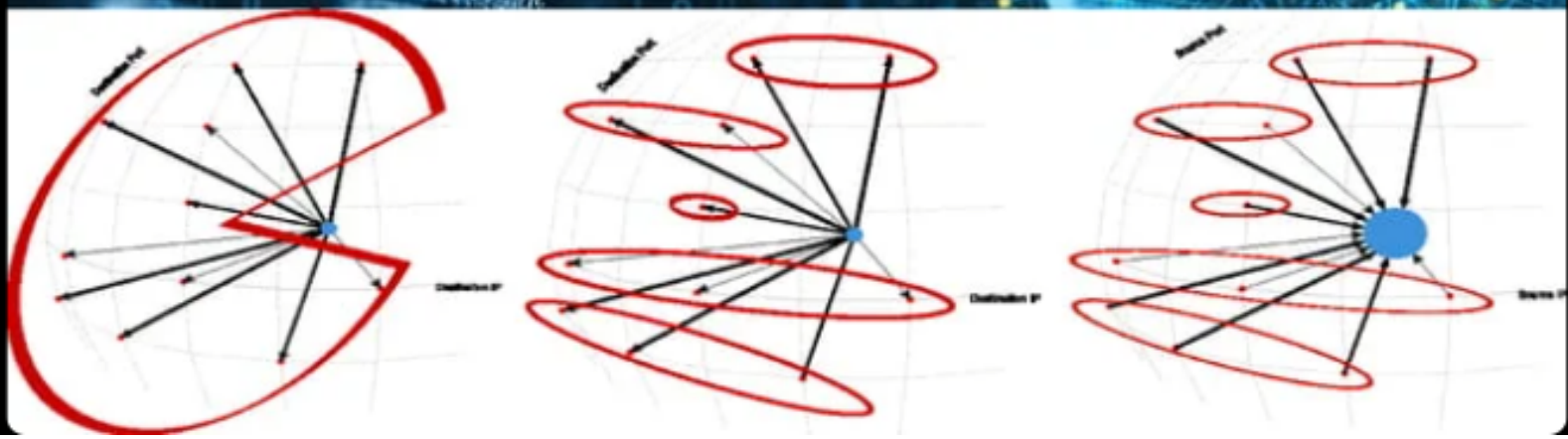

NEED OF NETWORK TRAFFIC ANALYSIS
• Gain special knowledge about the network
• Investigate and troubleshoot abnormal behaviour
-Abnormal packets
-Network slow performance
1. congestion
2. Retransmission
-Unexpected traffic
-Broken applications
-Load balancer issues


• Network forensenics
-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 forsenic 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

HOW TO SOLVE NETWORK TRAFFIC?

- Identify what applications/protocols are running on the network
- Identify bandwidth hogs down to a user, application or device level
- Monitor client to server network traffic
- Troubleshoot network & application performance issues



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**

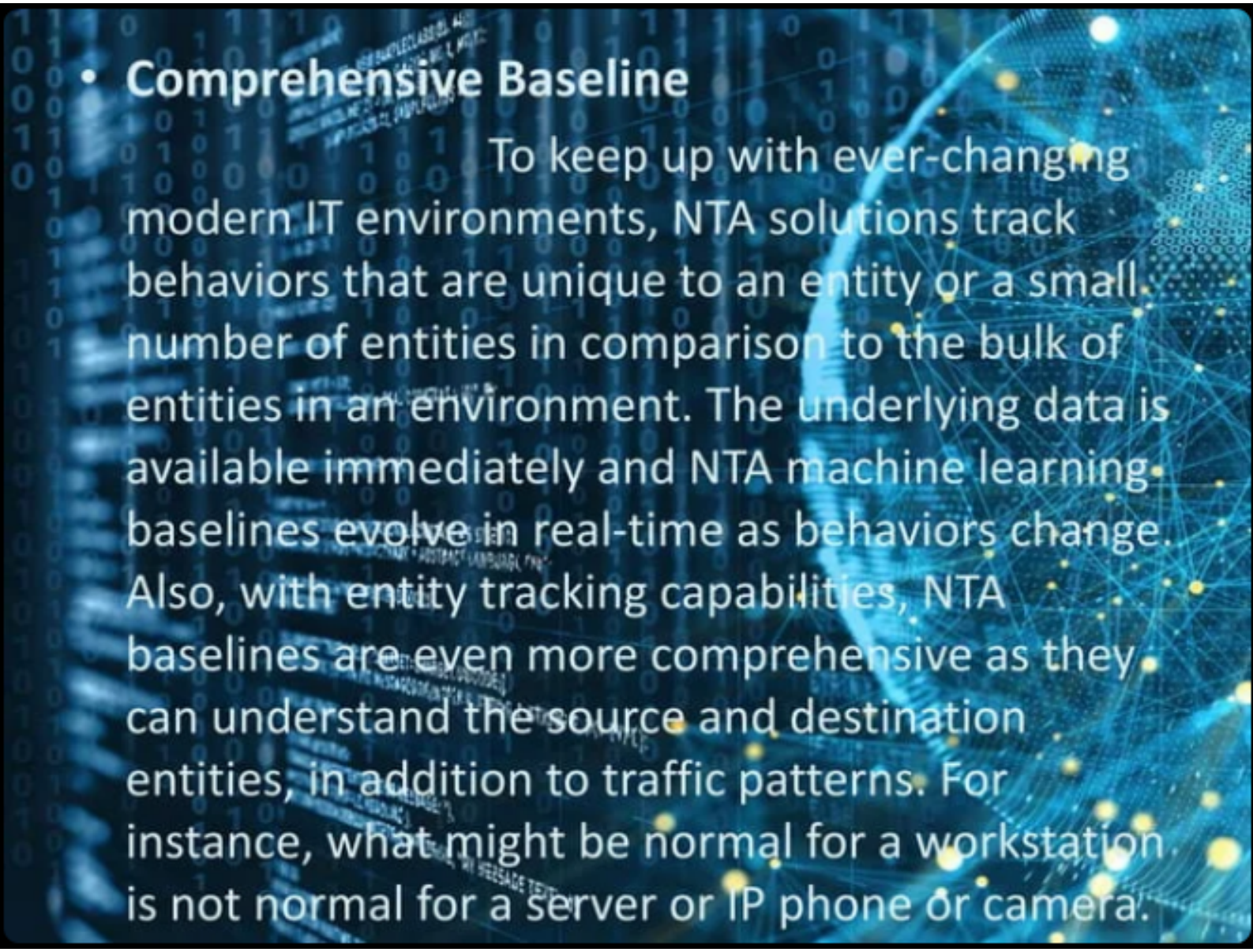
With over 70 percent of web traffic encrypted, organizations need an accessible method for decrypting their network traffic without disrupting data privacy implications. NTA solutions deliver on this challenge by enabling security professionals to uncover network threats by analyzing the full payload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

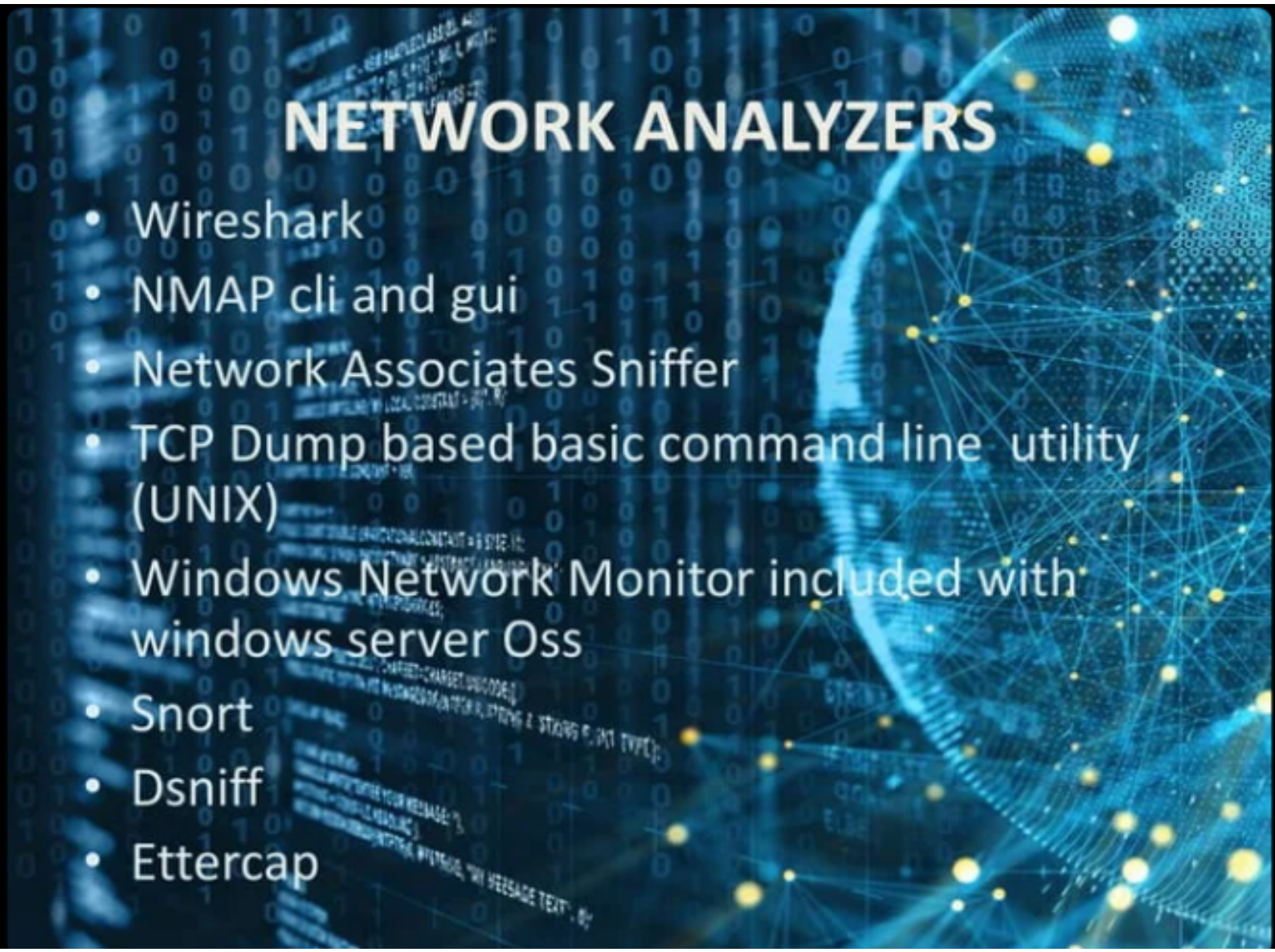
- **Entity Tracking**

  NTA products offer the ability to track and profile all entities on a network, including the devices, users, applications, destinations, and more. Machine learning and analytics then attribute the behaviors and relationships to the named entities, providing infinitely more value to organizations than a static list of IP addresses.

- **Detection and Response**

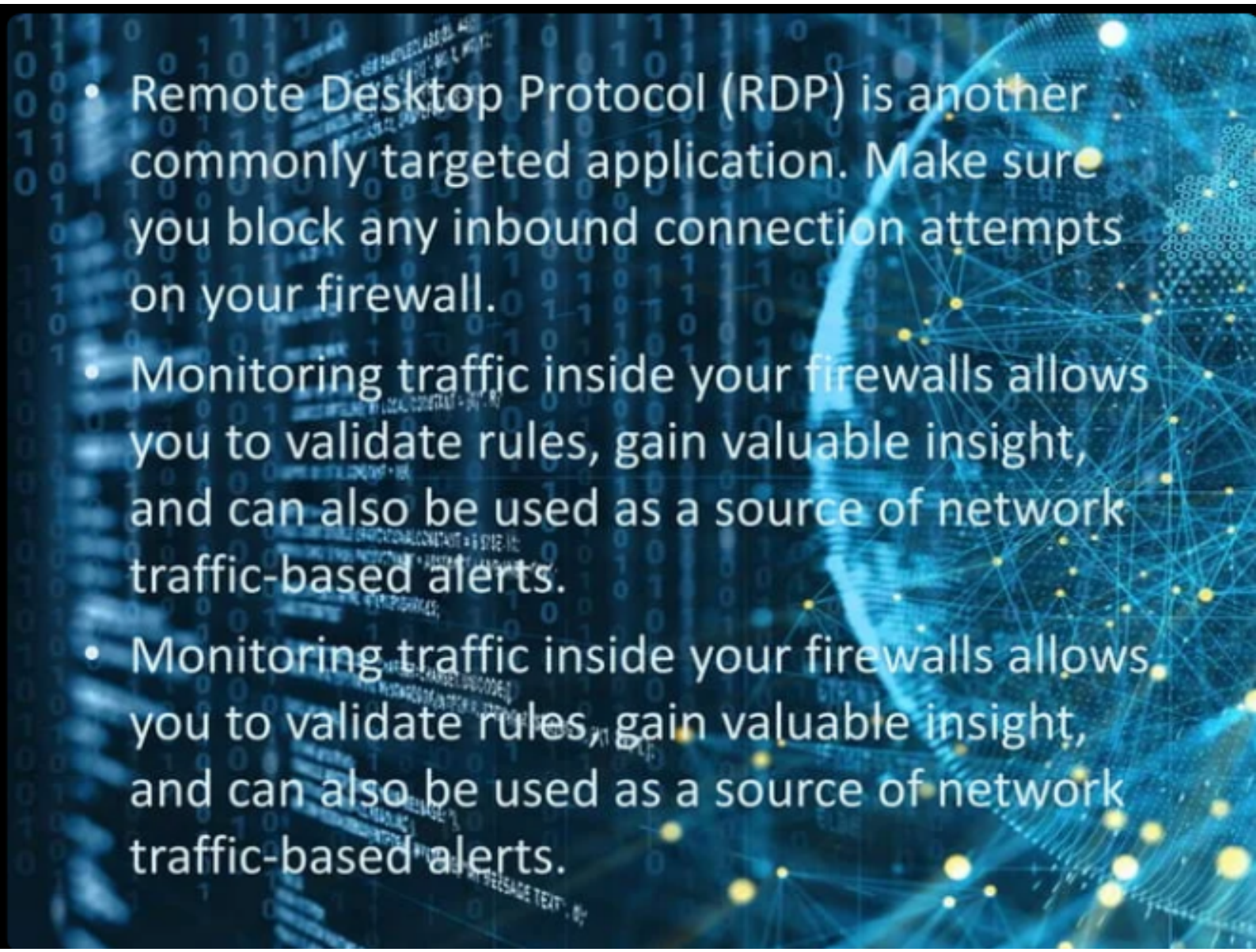
  Because NTA tools attribute behaviors to entities, ample context is available for detection and response workflows. This means security professionals no longer need to sift through multiple data sources such as DHCP and DNS logs, configuration management databases and directory service infrastructure in an attempt to gain comprehensive visibility. Instead, they can quickly detect anomalies, decisively track them down, determine the root cause and react accordingly.


• Comprehensive Baseline
To keep up with ever-changing modern IT environments, NTA solutions track behaviors that are unique to an entity or a small number of entities in comparison to the bulk of entities in an environment. The underlying data is available immediately and NTA machine learning baselines evolve in real-time as behaviors change. Also, with entity 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 a 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 included with windows server Oss
• Snort
• Dsniff
• Ettercap

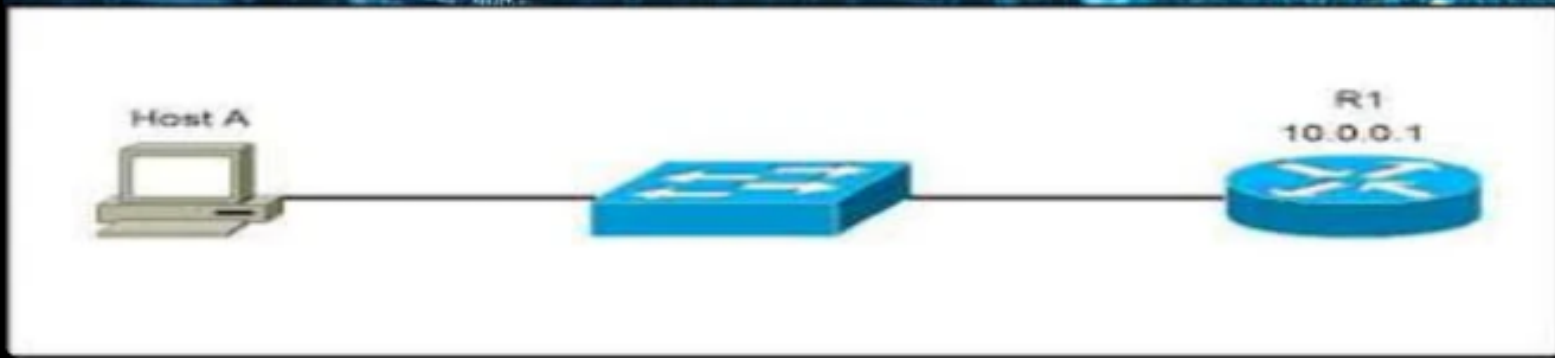
IMPORTANCE OF NETWORK TRAFFIC ANALYSIS

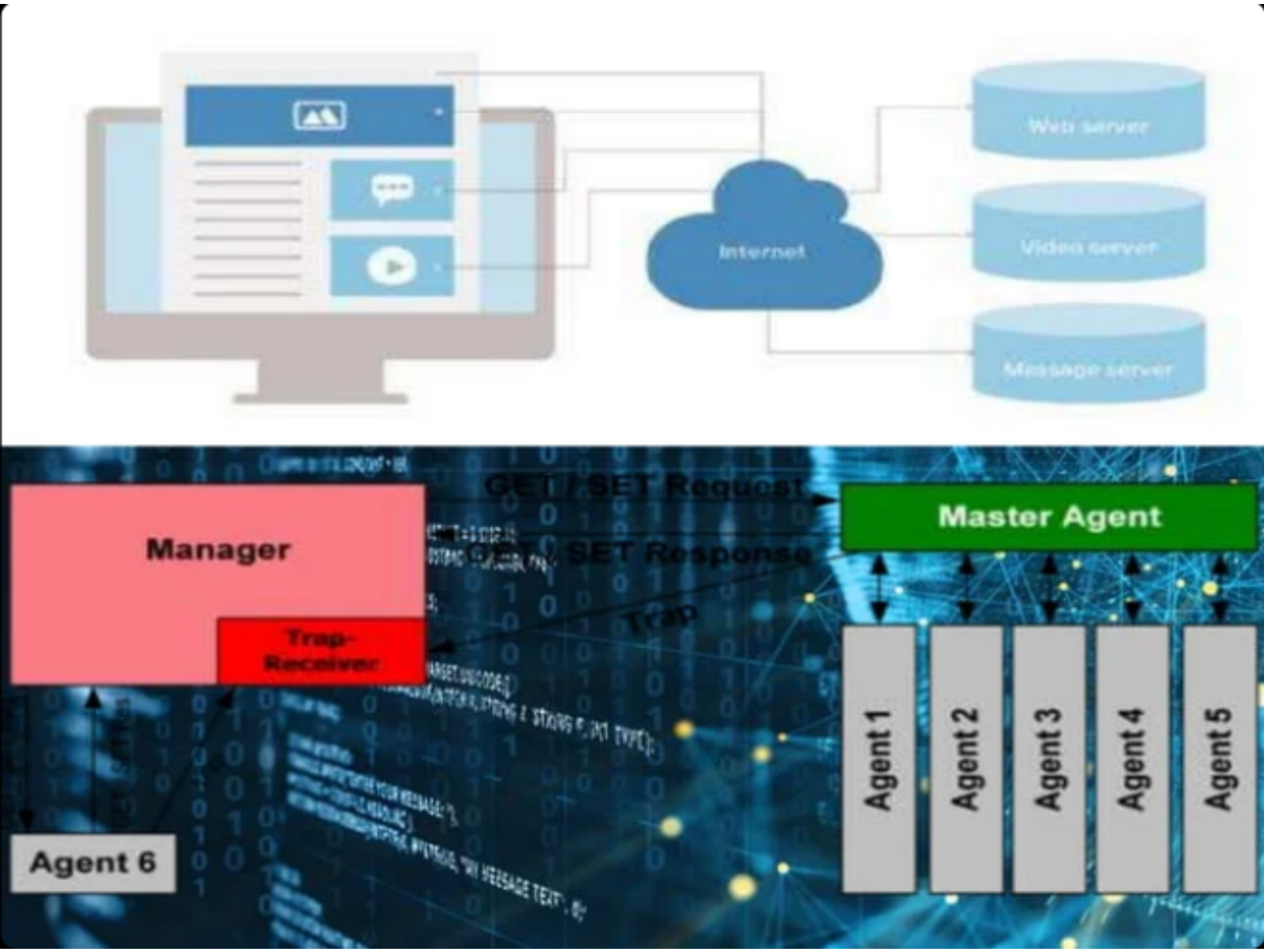
- Keeping a close eye on your network perimeter is always good practice. Even with strong firewalls in place, mistakes can happen and rogue traffic could get through.
- Users could also leverage methods such as tunneling, external anonymizers, and VPNs to get around firewall rules.
- A network monitoring 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.

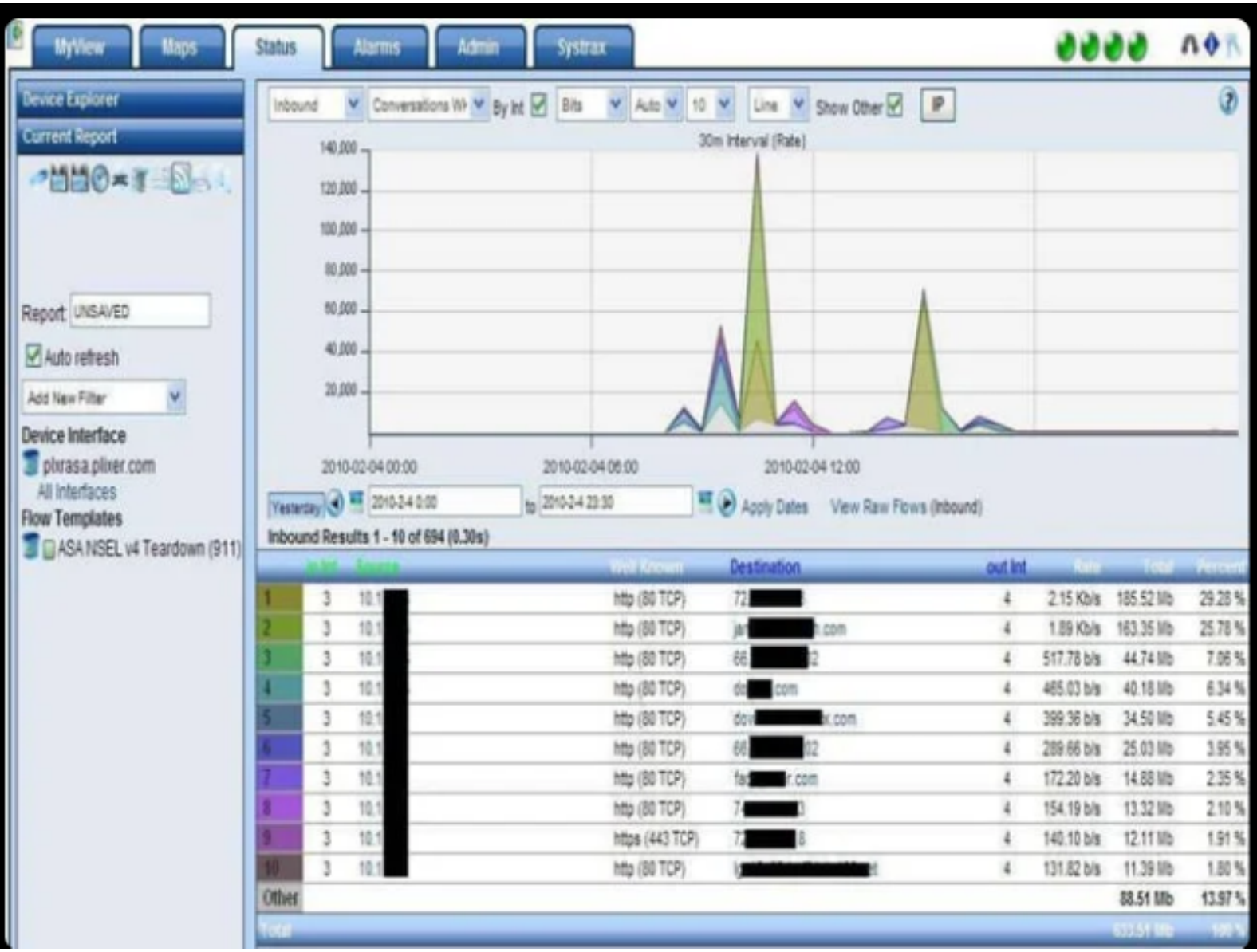


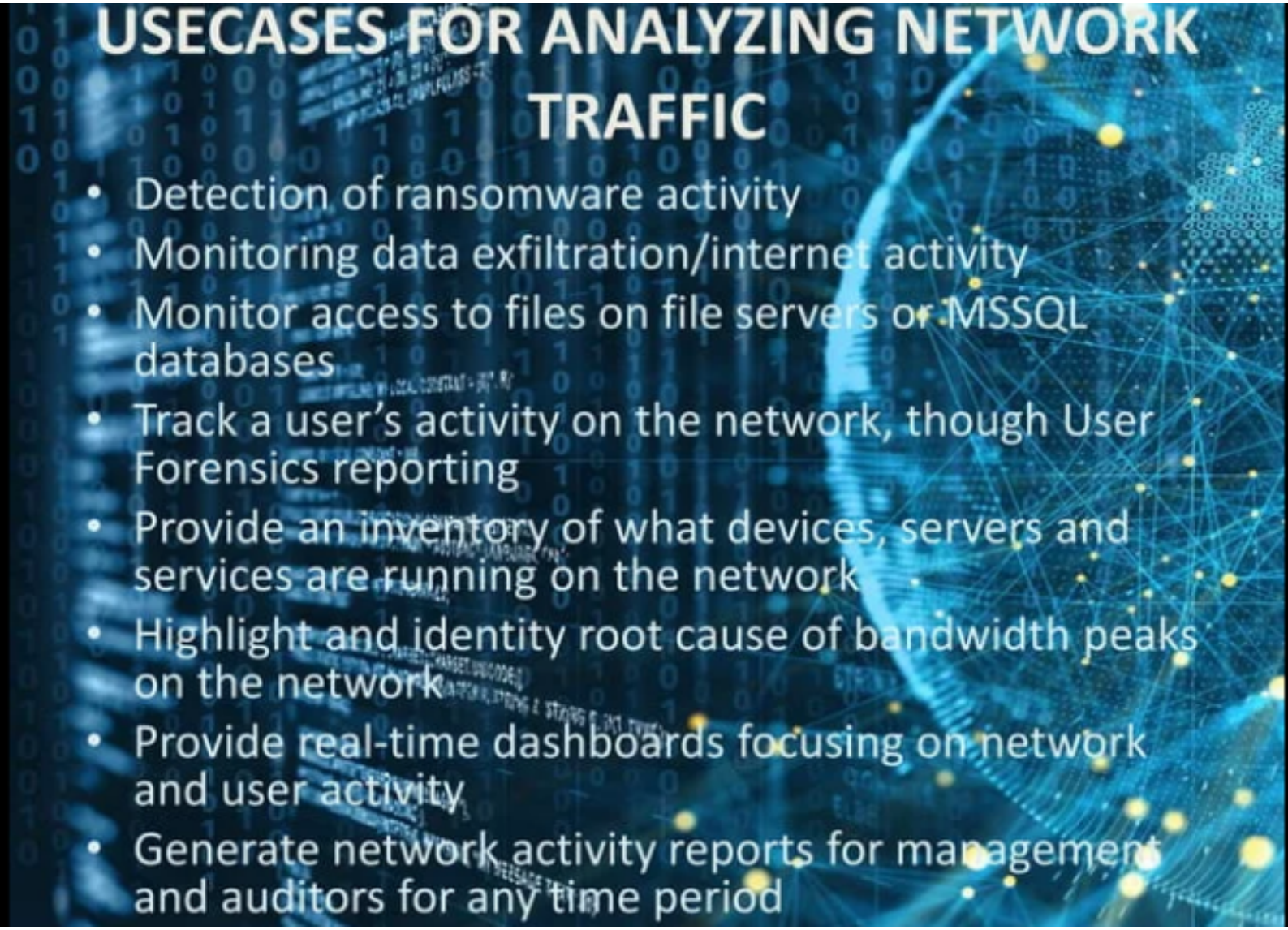
• Monitoring traffic inside your firewalls allows you to validate rules, gain valuable insight, and can also be used as a source of network traffic-based alerts.

- 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)




Web server
Video server
Message server
Internet
GET / SET Request
GET / SET Response
Trap
Manager
Trap-Receiver
Master Agent
Agent 1
Agent 2
Agent 3
Agent 4
Agent 5
Agent 6


MyView
Maps
Status
Alarms
Admin
Systrax
Device Explorer
Current Report
Report: UNSAVED
Auto refresh
Add New Filter
Device Interface
plxrasa.plixer.com
All Interfaces
Flow Templates
ASA NSEL v4 Teardown (911)
Inbound
Conversations W
By Int
Bits
Auto
10
Line
Show Other
IP
30m Interval (Rate)
140,000
120,000
100,000
80,000
60,000
40,000
20,000
2010-02-04 00:00
2010-02-04 06:00
2010-02-04 12:00
Yesterday
2010-2-4 0:00
to
2010-2-4 23:30
Apply Dates
View Raw Flows (Inbound)
Inbound Results 1 - 10 of 694 (0.30s)
Destination
out Int
Rate
Total
Percent
1 3 10.1 http (80 TCP) 72 4 2.15 Kb/s 185.52 Mb 29.28 %
2 3 10.1 http (80 TCP) ja .com 4 1.89 Kb/s 163.35 Mb 25.78 %
3 3 10.1 http (80 TCP) 66 2 4 517.78 b/s 44.74 Mb 7.06 %
4 3 10.1 http (80 TCP) do .com 4 465.03 b/s 40.18 Mb 6.34 %
5 3 10.1 http (80 TCP) dov .com 4 399.36 b/s 34.50 Mb 5.45 %
6 3 10.1 http (80 TCP) 66 02 4 289.66 b/s 25.03 Mb 3.95 %
7 3 10.1 http (80 TCP) fa .com 4 172.20 b/s 14.88 Mb 2.35 %
8 3 10.1 http (80 TCP) 7 3 4 154.19 b/s 13.32 Mb 2.10 %
9 3 10.1 https (443 TCP) 72 8 4 140.10 b/s 12.11 Mb 1.91 %
10 3 10.1 http (80 TCP) 4 131.82 b/s 11.39 Mb 1.80 %
Other 88.51 Mb 13.97 %
Total


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, though User Forensics reporting
• Provide an inventory of what devices, servers and services are running on the network
• Highlight and identity 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

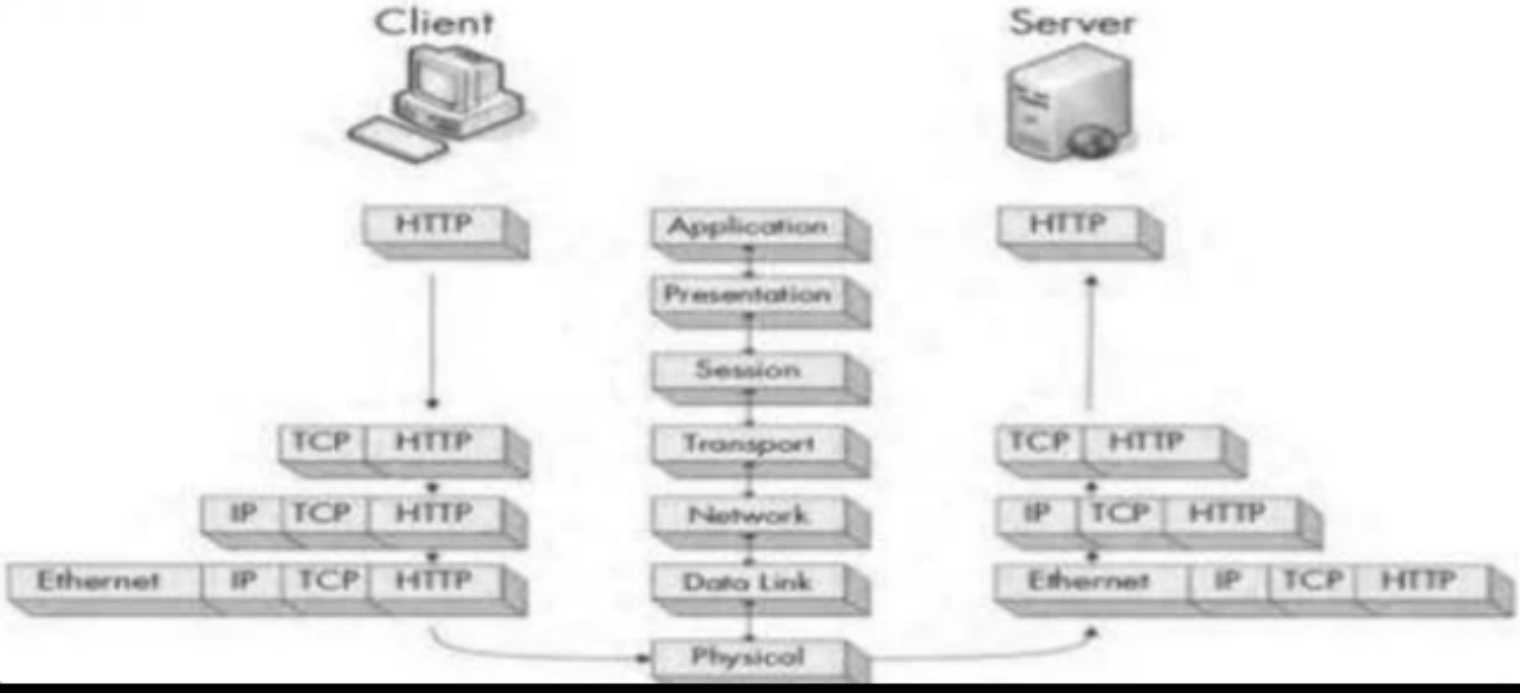
WHAT TO LOOK FOR IN A NETWORK TRAFFIC ANALYSIS

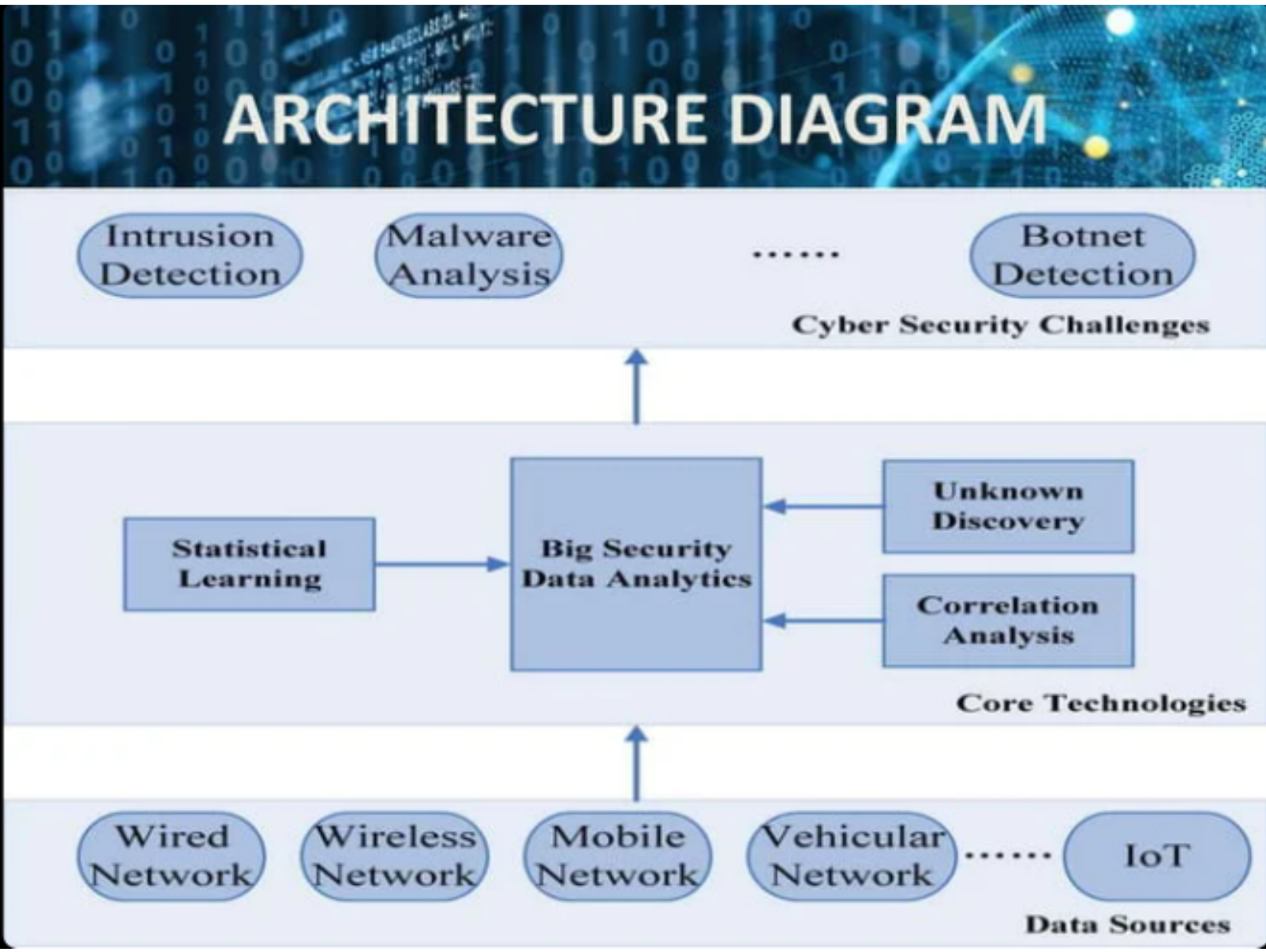
- Not all tools for monitoring network traffic are the same. Generally, they can be broken down into two types: flow-based tools and deep packet inspection (DPI) tools.
- Within these tools you'll have options for software agents, storing historical data, and intrusion detection systems.
- When evaluating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

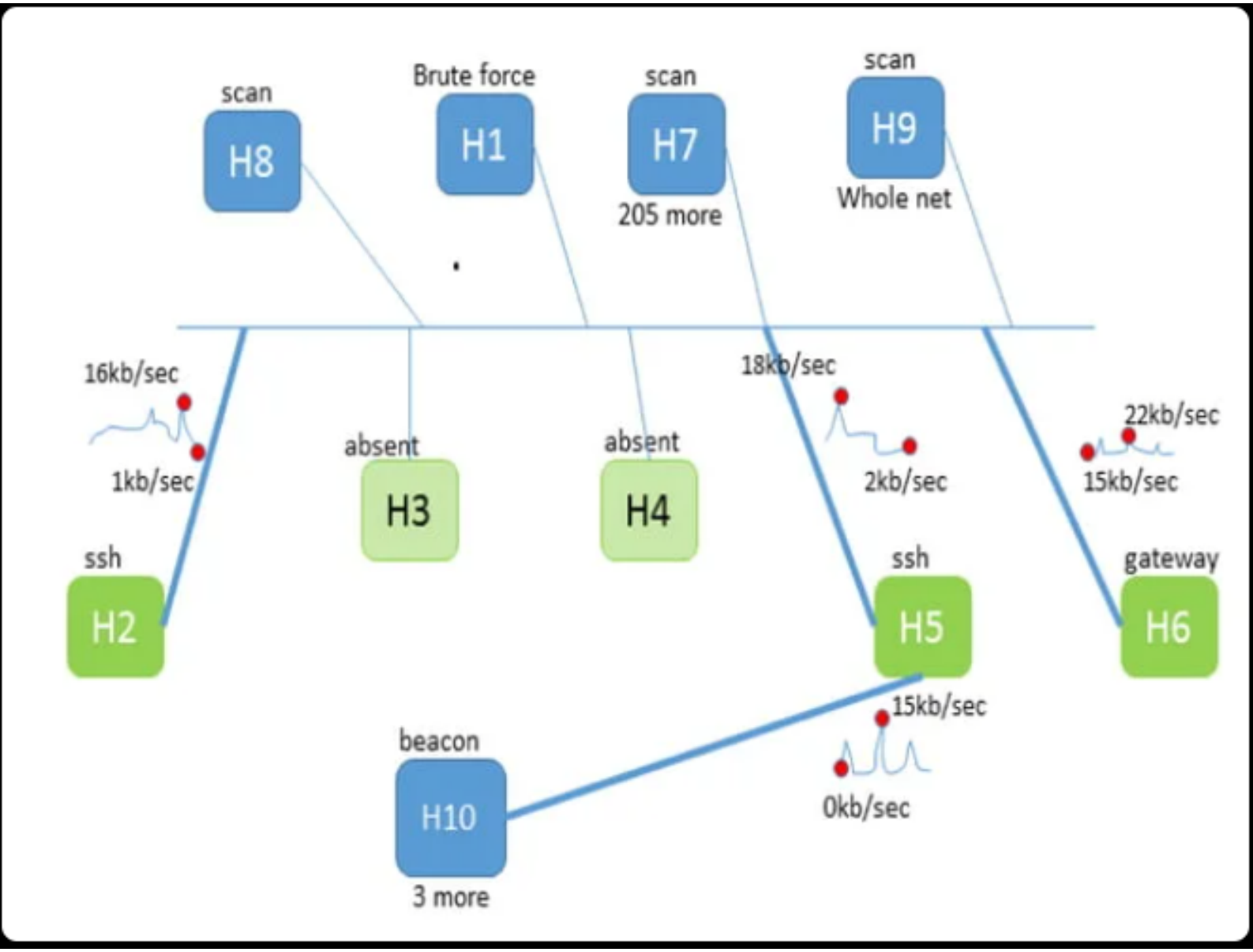
1. Availability of flow-enabled devices
2. The data source
3. The points on the network
4. Real-time data vs. historical data
5. Full packet capture, cost and complexity

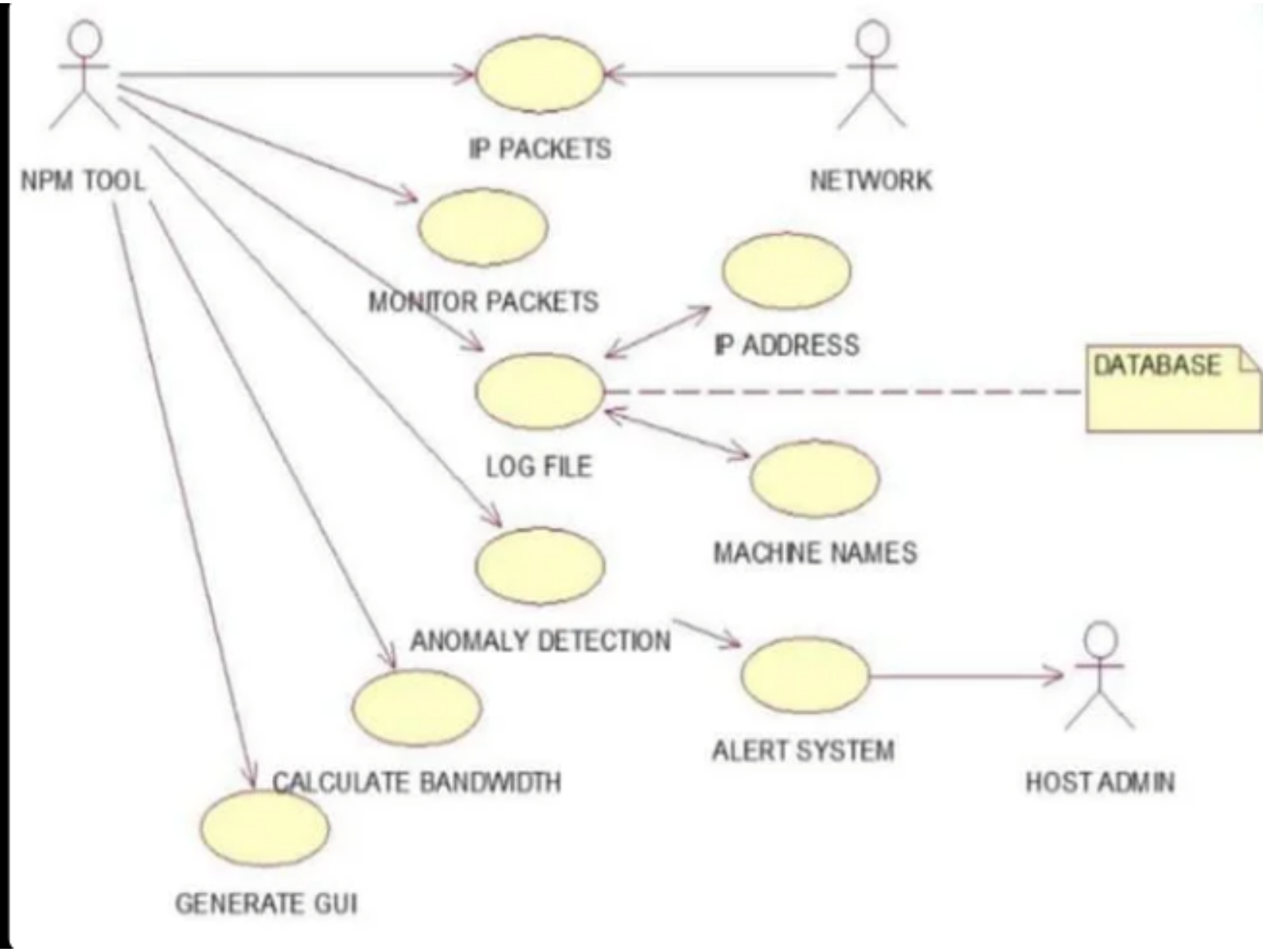
NETWORK PROTOCOLS

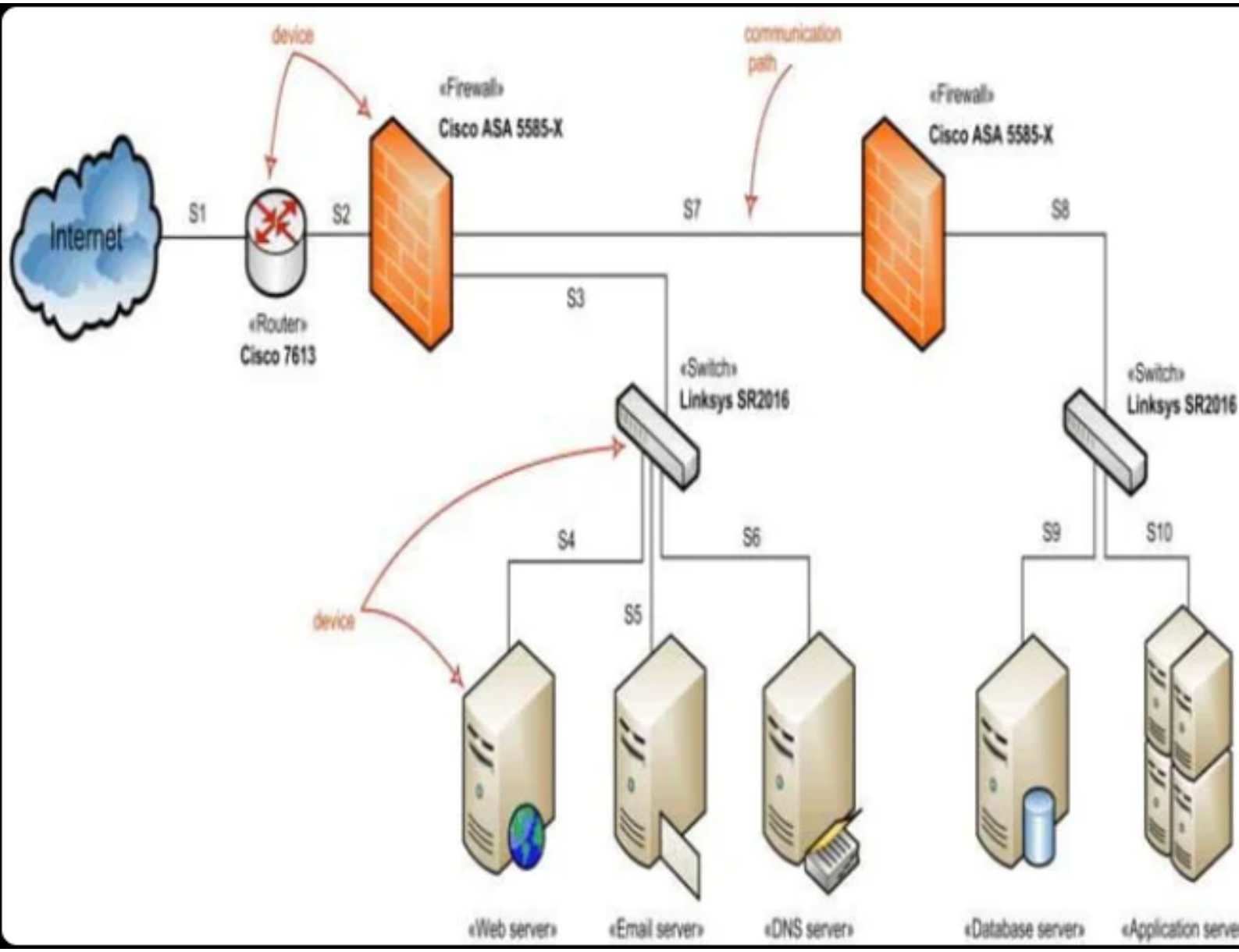
- There are totally 7 layers of protocols for analyzing network traffic

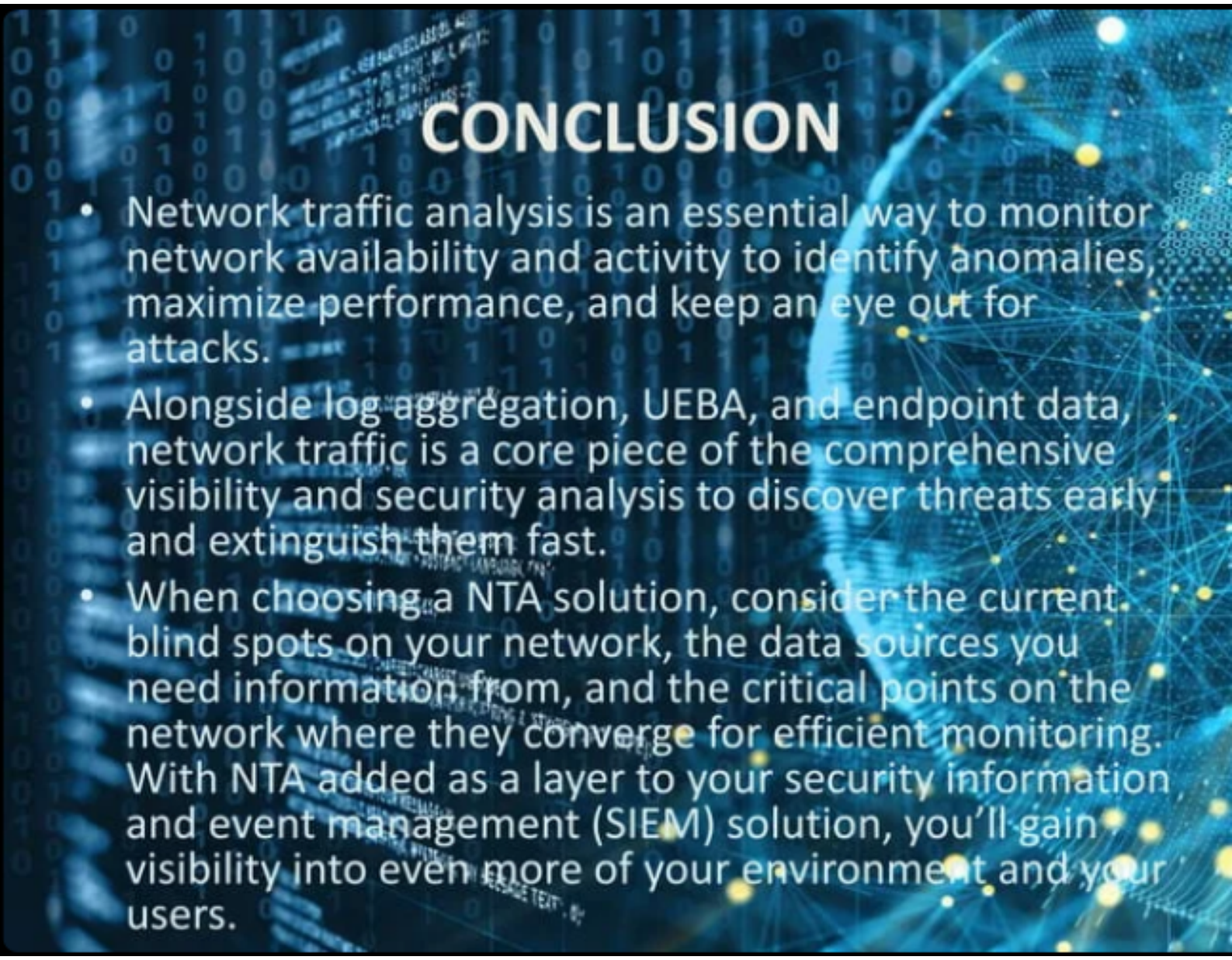



ARCHITECTURE DIAGRAM
Intrusion Detection
Malware Analysis
.....
Botnet Detection
Cyber Security Challenges
Statistical Learning
Big Security Data Analytics
Unknown Discovery
Correlation Analysis
Core Technologies
Wired Network
Wireless Network
Mobile Network
Vehicular Network
.....
IoT
Data Sources


scan
H8
Brute force
H1
scan
H7
205 more
scan
H9
Whole net
16kb/sec
1kb/sec
absent
H3
absent
H4
18kb/sec
2kb/sec
22kb/sec
15kb/sec
ssh
H2
ssh
H5
gateway
H6
15kb/sec
0kb/sec
beacon
H10
3 more


NPM TOOL
IP PACKETS
NETWORK
MONITOR PACKETS
IP ADDRESS
DATABASE
LOG FILE
MACHINE NAMES
ANOMALY DETECTION
ALERT SYSTEM
HOST ADMIN
CALCULATE BANDWIDTH
GENERATE GUI


device
communication path
«Firewall»
Cisco ASA 5585-X
«Firewall»
Cisco ASA 5585-X
Internet
S1
S2
S7
S8
S3
«Router»
Cisco 7613
«Switch»
Linksys SR2016
«Switch»
Linksys SR2016
S4
S6
S9
S10
S5
device
«Web server»
«Email server»
«DNS server»
«Database server»
«Application server»


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.