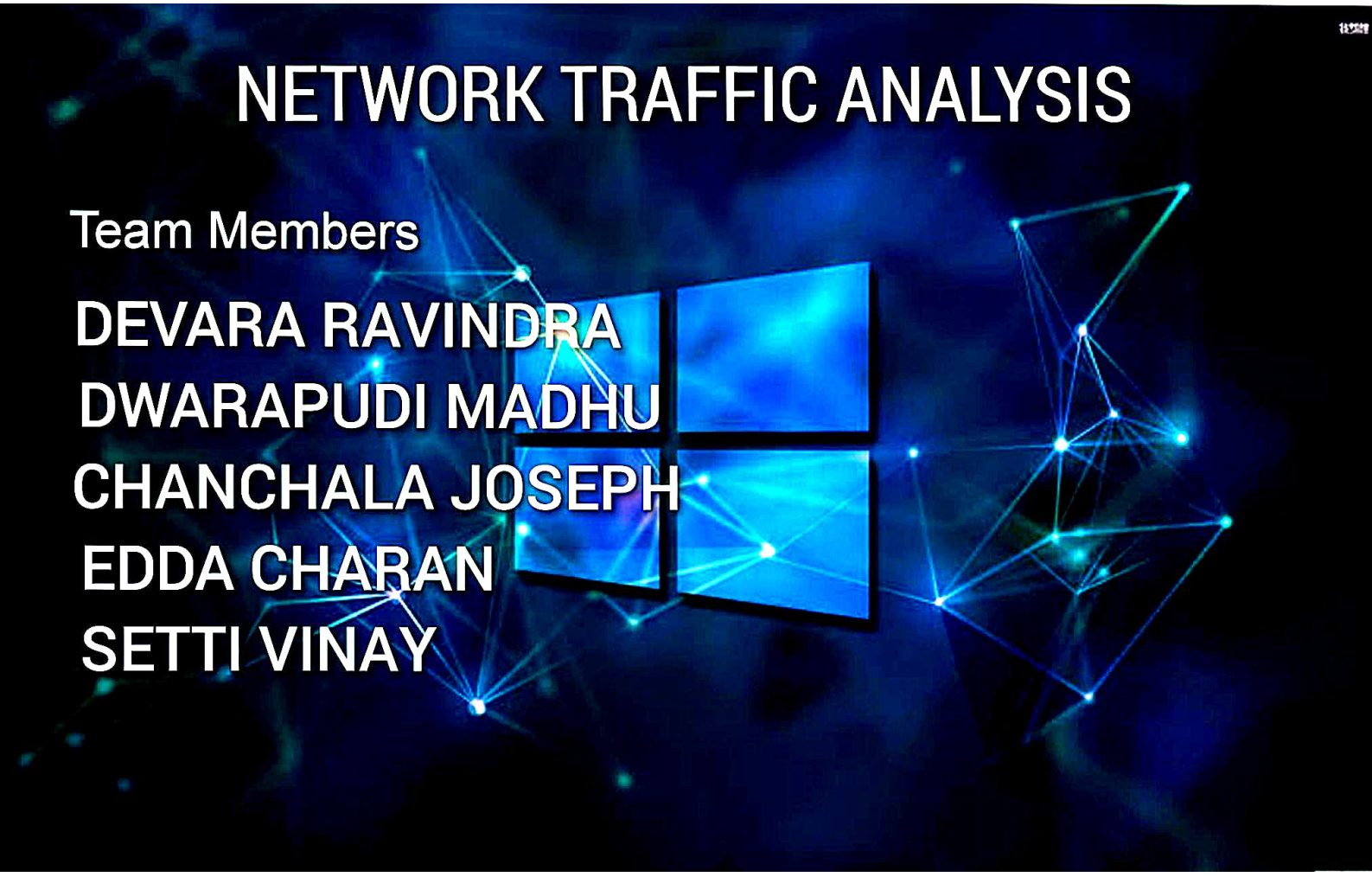
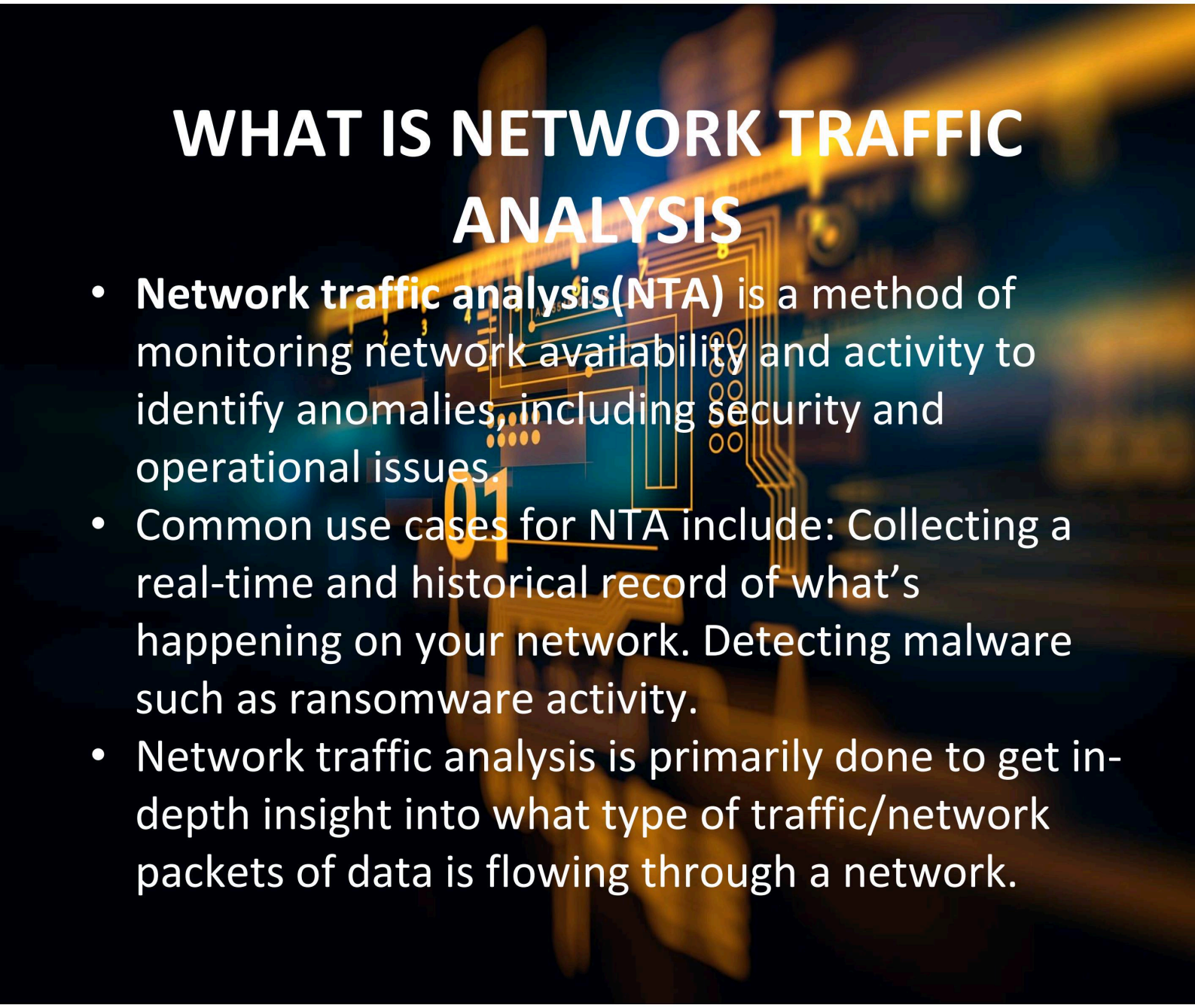

NETWORK TRAFFIC ANALYSIS
Team Members
DEVARA RAVINDRA
DWARAPUDI MADHU
CHANCHALA JOSEPH
EDDA CHARAN
SETTI VINAY

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 unauthorized 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 of data is flowing through a network.

EMAIL FOOTPRINT ANALYSIS

- Email tracking is used to monitor the delivery of emails to an intended recipient.
- Attackers track emails to gather information about a target recipient in order to perform social engineering and other attacks.
- Get recipient's system IP address
- Geolocation of the recipient
- When the email was received and read
- Whether or not the recipient visited any links sent to them
- Get recipient's browser and operating system information
- Time spent on reading the emails

DNS INFORMATION GATHERING

- **DNS enumeration** is the process of locating all the DNS servers and their corresponding records for an organization.
- A company may have both internal and external DNS servers that can yield information such as usernames, computer names, and IP addresses of potential target systems.
- There are a lot of tools that can be used to gain information for performing DNS enumeration. The examples of tool that can be used for DNS enumeration are NSlookup, DNSstuff, American Registry for Internet Numbers (ARIN), and Whois.

WHOIS INFORMATION GATHERING

- Information in regard to whois gathering and how attackers use the information use the information that is displayed in whois records against unsuspecting organizational members, leaders and employees.
- whois searches allow the general public to search for information based on the grounds of, who web locations are registered to, expiry records, when a domain has been created, name servers and contact information.
- However whois information can also aid attackers in obtaining information to help launch a successful penetration into a network.

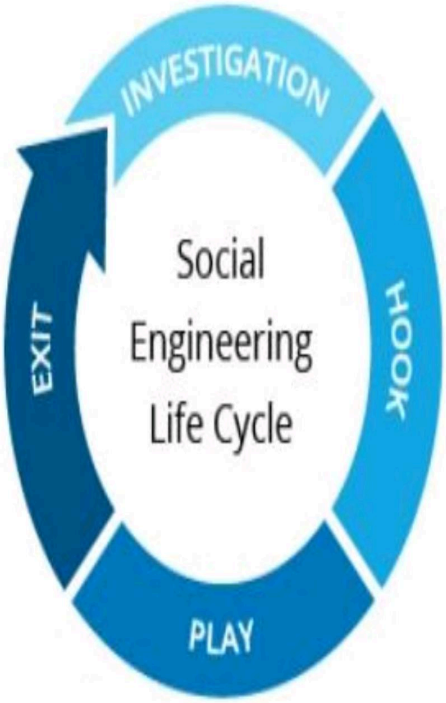
SOCIAL ENGINEERING ATTACKS

- Social engineering is the term used for a broad range of malicious activities accomplished through human interactions. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information.

- Social engineering attacks happen in one or more steps. A perpetrator first investigates the intended victim to gather necessary background information, such as potential points of entry and weak security protocols, needed to proceed with the attack. Then, the attacker moves to gain the victim's trust and provide stimuli for subsequent actions that break security practices, such as revealing sensitive information or granting access to critical resources.

Preparing the ground for the attack:

- Identifying the victim(s).
- Gathering background information.
- Selecting attack method(s).



Deceiving the victim(s) to gain a foothold:

- Engaging the target.
- Spinning a story.
- Taking control of the interaction.

Obtaining the information over a period of time:

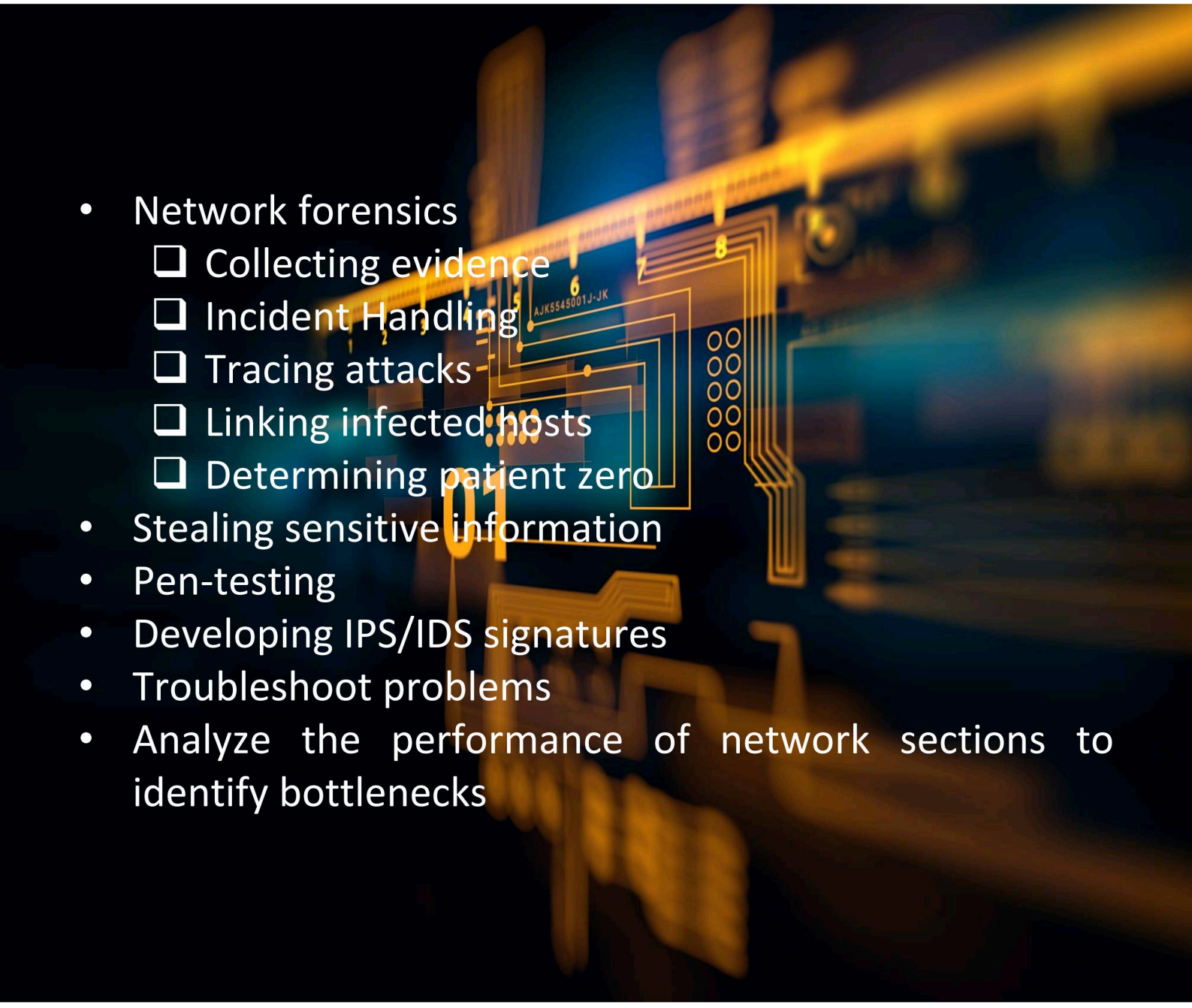
- Expanding foothold.
- Executing the attack.
- Disrupting business or/and siphoning data.

Closing the interaction,
ideally without arousing suspicion:

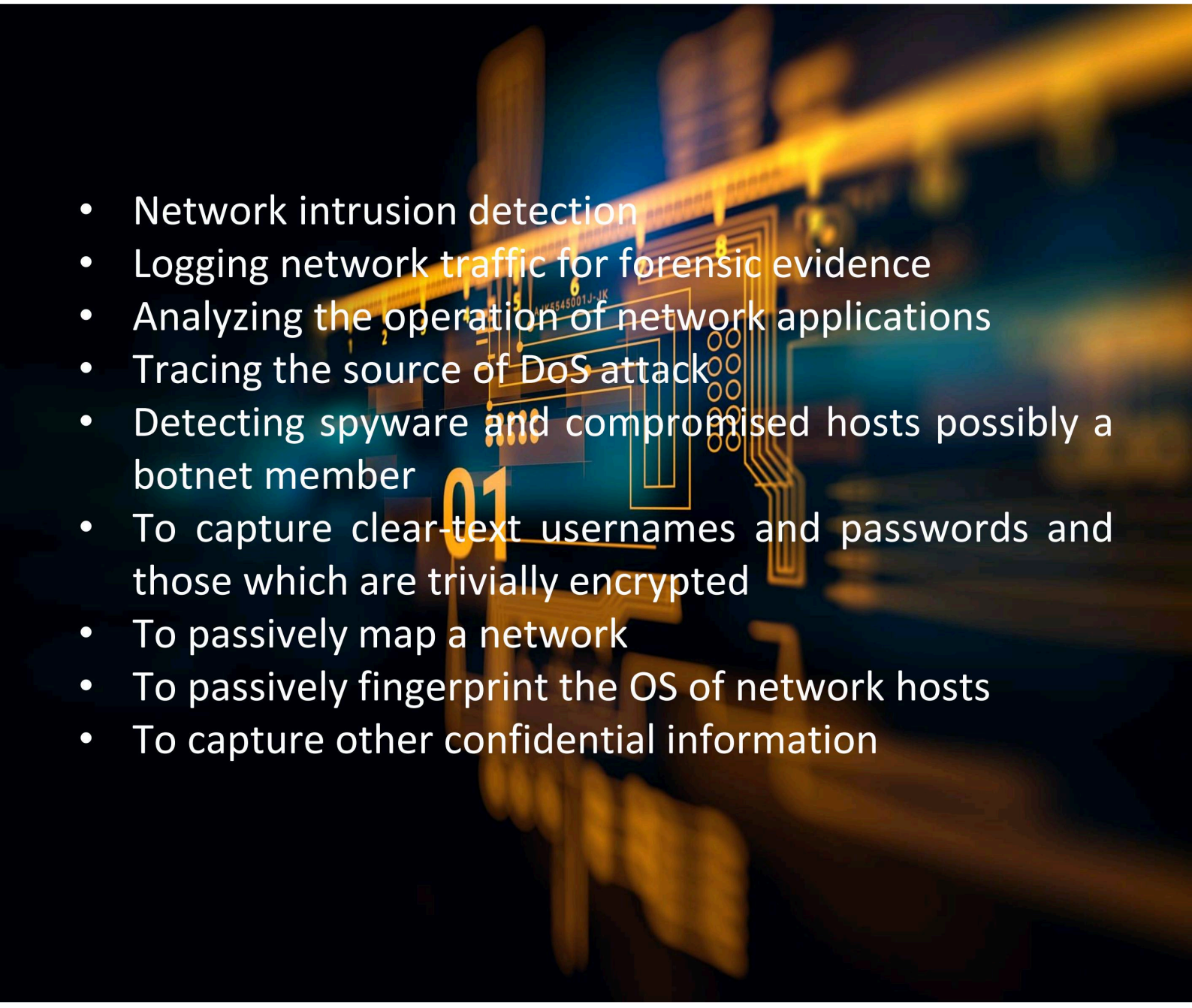
- Removing all traces of malware.
- Covering tracks.
- Bringing the charade to a natural end.

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
- Analyze the performance of network sections to identify bottlenecks



- Network intrusion detection
- Logging network traffic for forensic evidence
- Analyzing 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

TYPES OF VULNERABILITIES

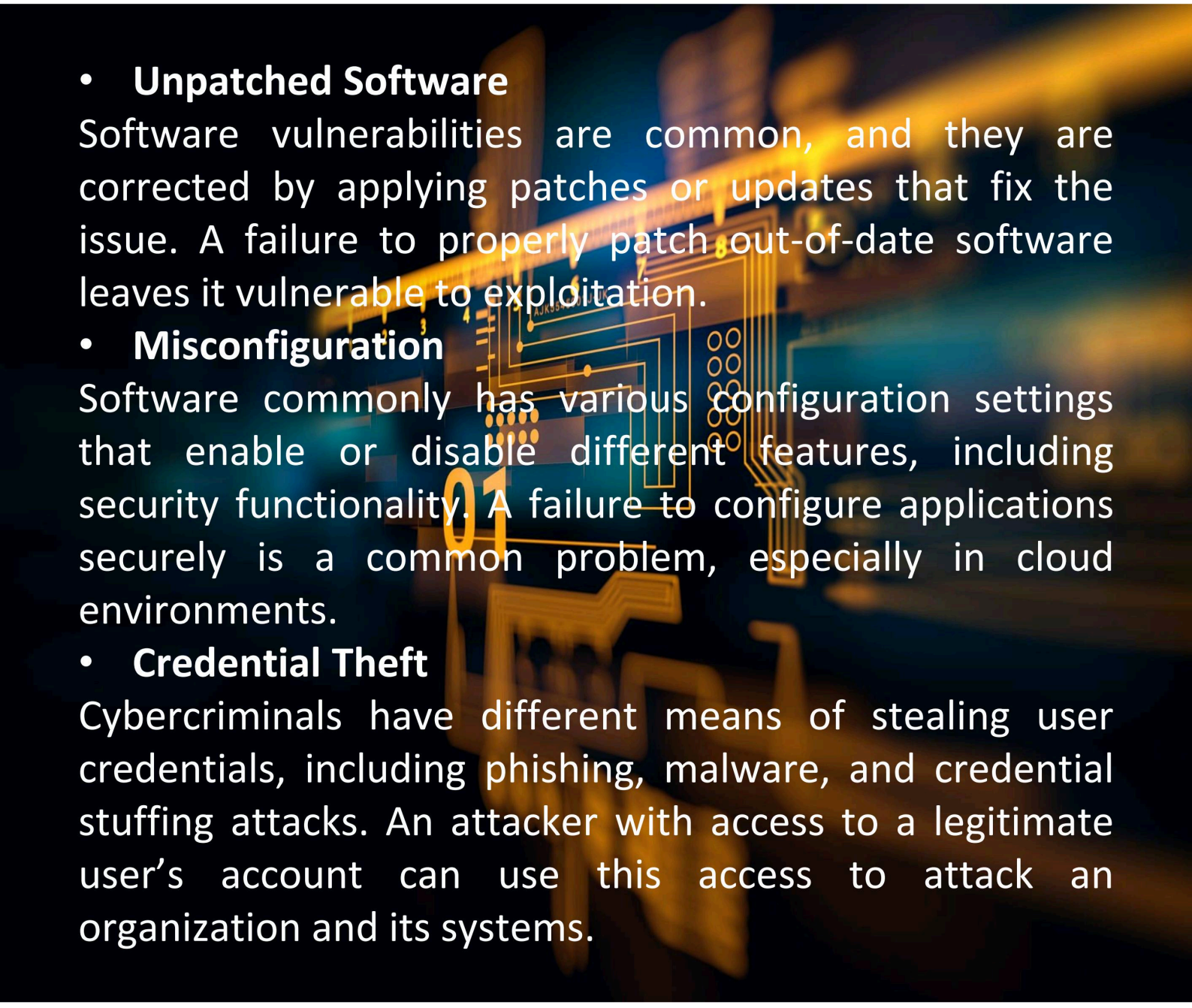
Vulnerabilities come in various forms, but some of the most common types include the following:

- **Zero Day**

A zero-day vulnerability is one that was discovered by cybercriminals and exploited before a patch was available. Zero-day vulnerabilities like Log4j are often the most famous and damaging vulnerabilities because attackers have the opportunity to exploit them before they can be fixed.

- **Poor Data Sanitization**

Many attacks — such as SQL injection and buffer overflows — involve an attacker submitting invalid data to an application. A failure to properly validate data before processing leaves these applications vulnerable to attack.



- **Unpatched Software**

Software vulnerabilities are common, and they are corrected by applying patches or updates that fix the issue. A failure to properly patch out-of-date software leaves it vulnerable to exploitation.

- **Misconfiguration**

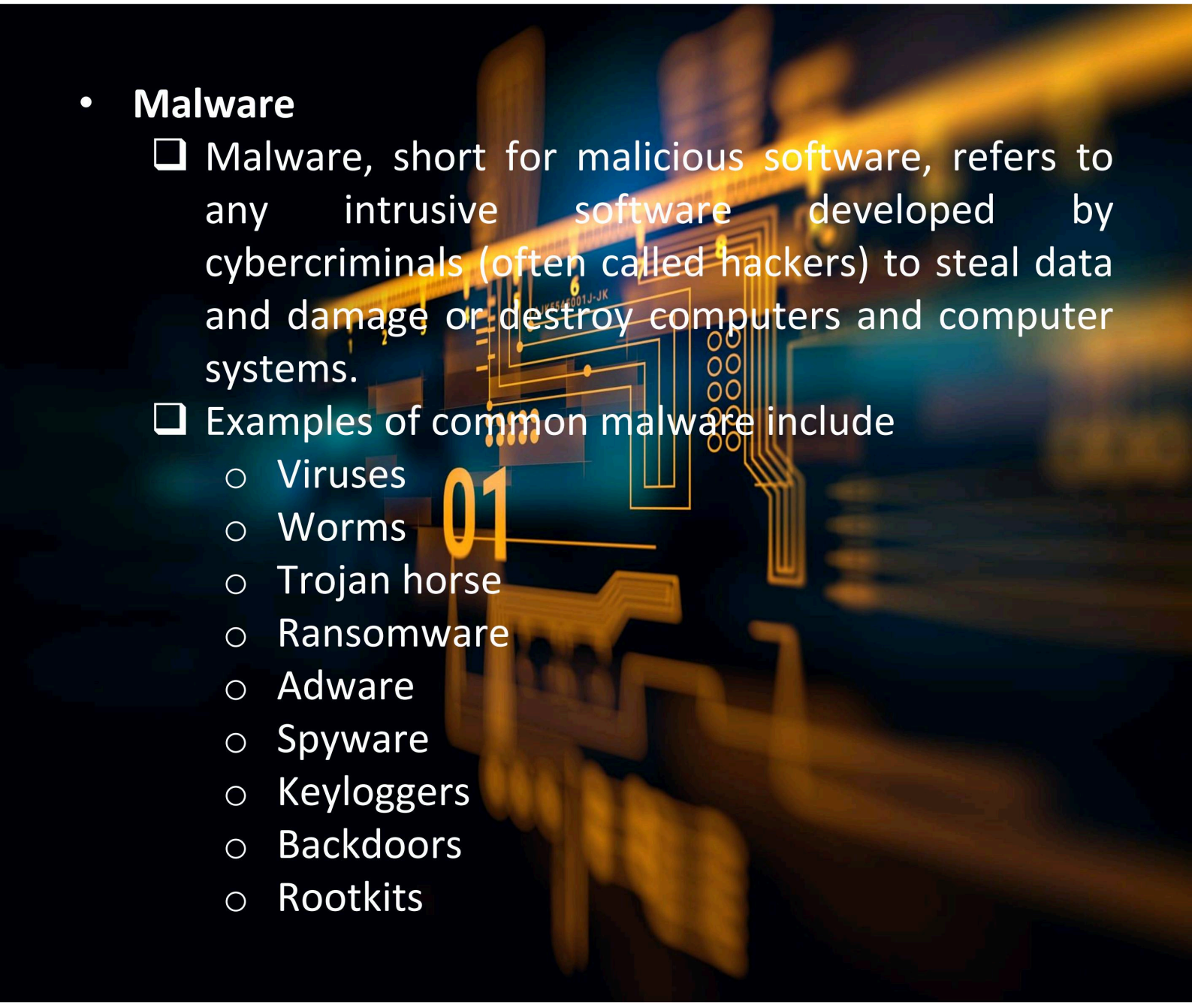
Software commonly has various configuration settings that enable or disable different features, including security functionality. A failure to configure applications securely is a common problem, especially in cloud environments.

- **Credential Theft**

Cybercriminals have different means of stealing user credentials, including phishing, malware, and credential stuffing attacks. An attacker with access to a legitimate user's account can use this access to attack an organization and its systems.

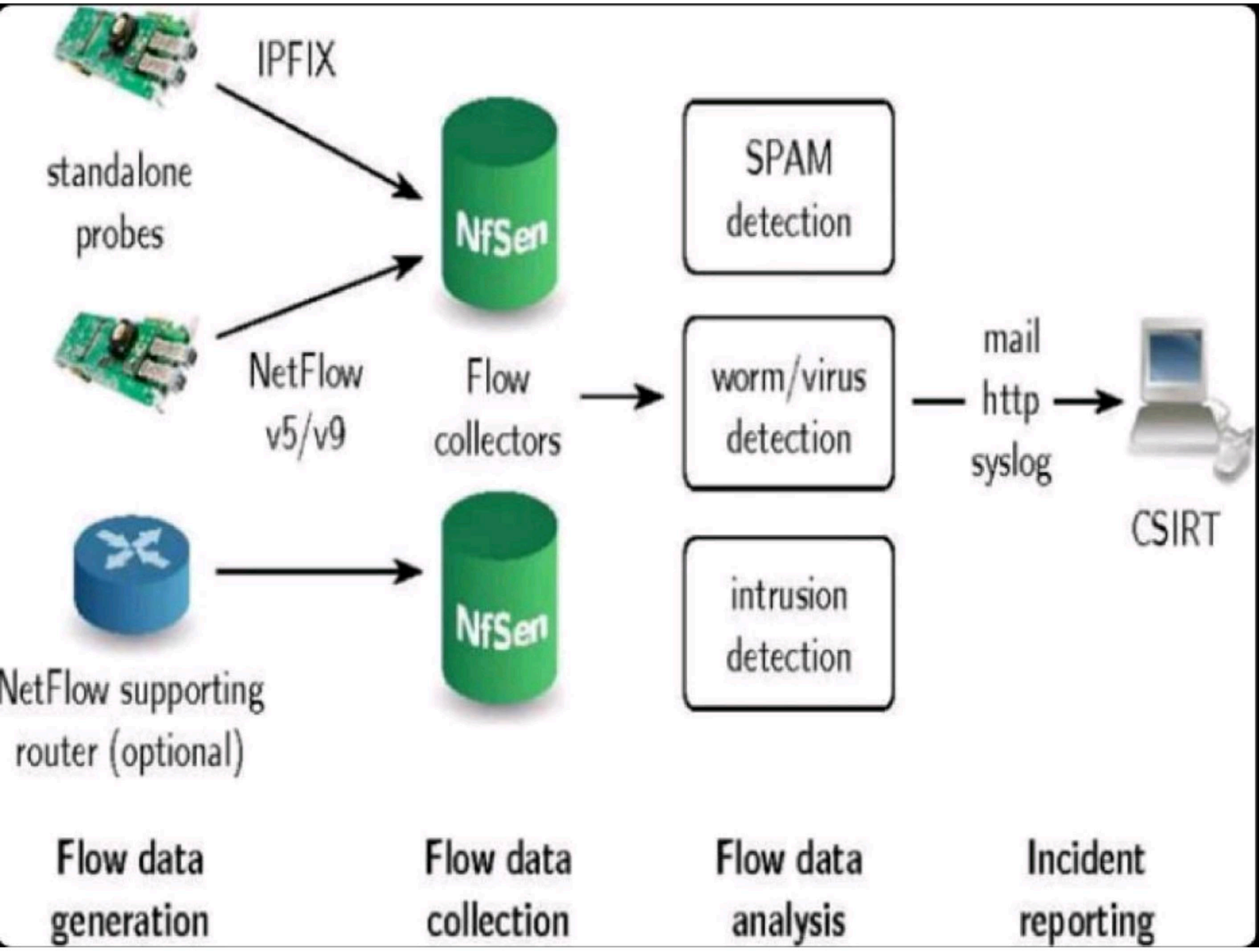
VULNERABILITY PATH AND PARAMETERS

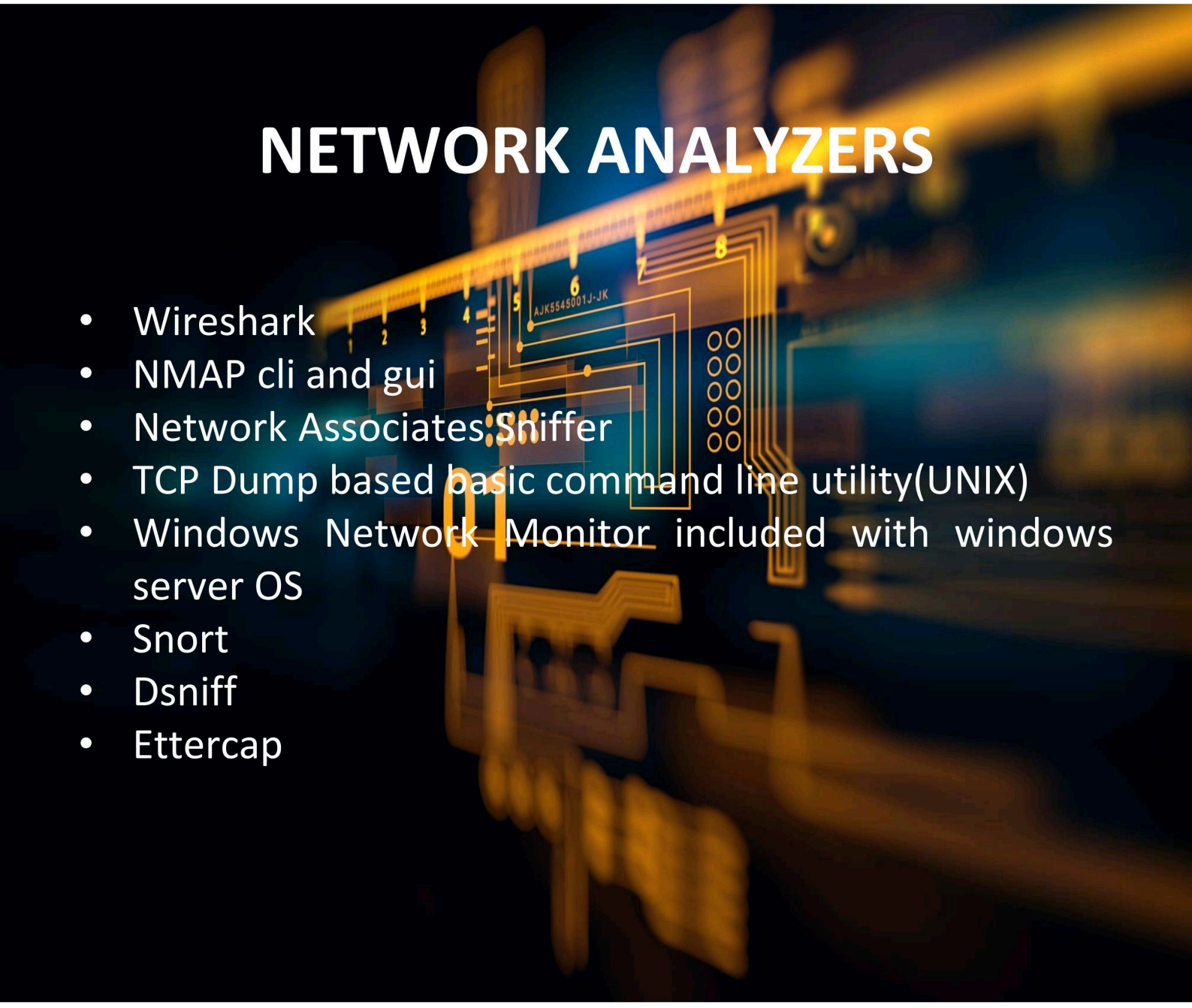
- **Penetration testing**
  - A penetration test (pen test) is an authorized simulated attack performed on a computer system to evaluate its security.
  - Penetration testers use the same tools, techniques, and processes as attackers to find and demonstrate the business impacts of weaknesses in a system.
  - Penetration tests usually simulate a variety of attacks that could threaten a business.
  - They can examine whether a system is robust enough to withstand attacks from authenticated and unauthenticated positions, as well as a range of system roles. With the right scope, a pen test can dive into any aspect of a system.



- **Malware**
  - ❑ Malware, short for malicious software, refers to any intrusive software developed by cybercriminals (often called hackers) to steal data and damage or destroy computers and computer systems.
  - ❑ Examples of common malware include
    - Viruses
    - Worms
    - Trojan horse
    - Ransomware
    - Adware
    - Spyware
    - Keyloggers
    - Backdoors
    - Rootkits

- **Intrusion Detection System**
  - A system called an intrusion detection system (IDS) observes network traffic for malicious transactions and sends immediate alerts when it is observed.
  - It is software that checks a network or system for malicious activities or policy violations. Each illegal activity or violation is often recorded either centrally using a SIEM system or notified to an administration.
  - IDS monitors a network or system for malicious activity and protects a computer network from unauthorized access from users, including perhaps insiders.


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



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 OS
- Snort
- Dsniff
- Ettercap

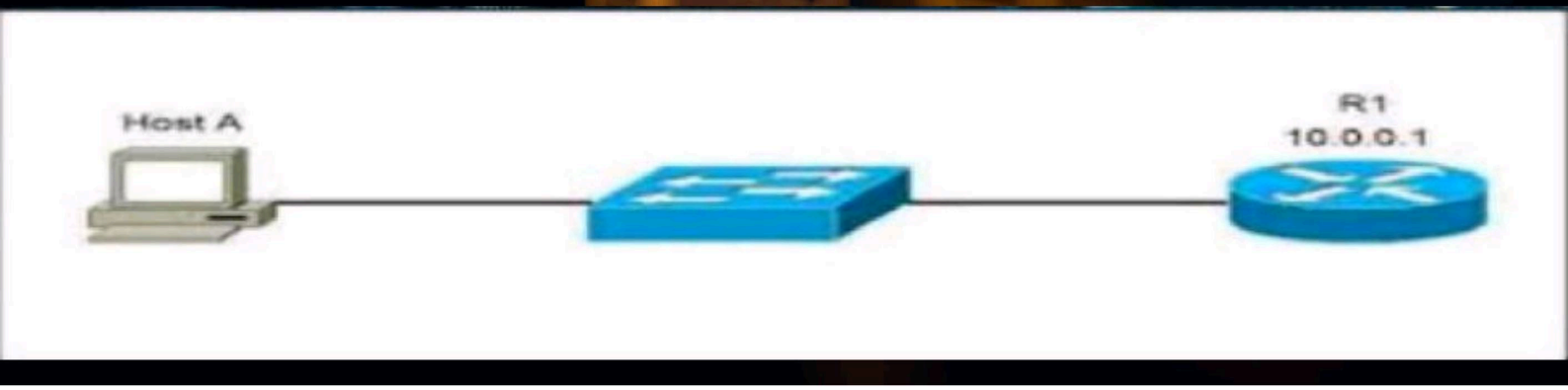
IMPORTANCE OF NETWORK TRAFFIC ANALYSIS

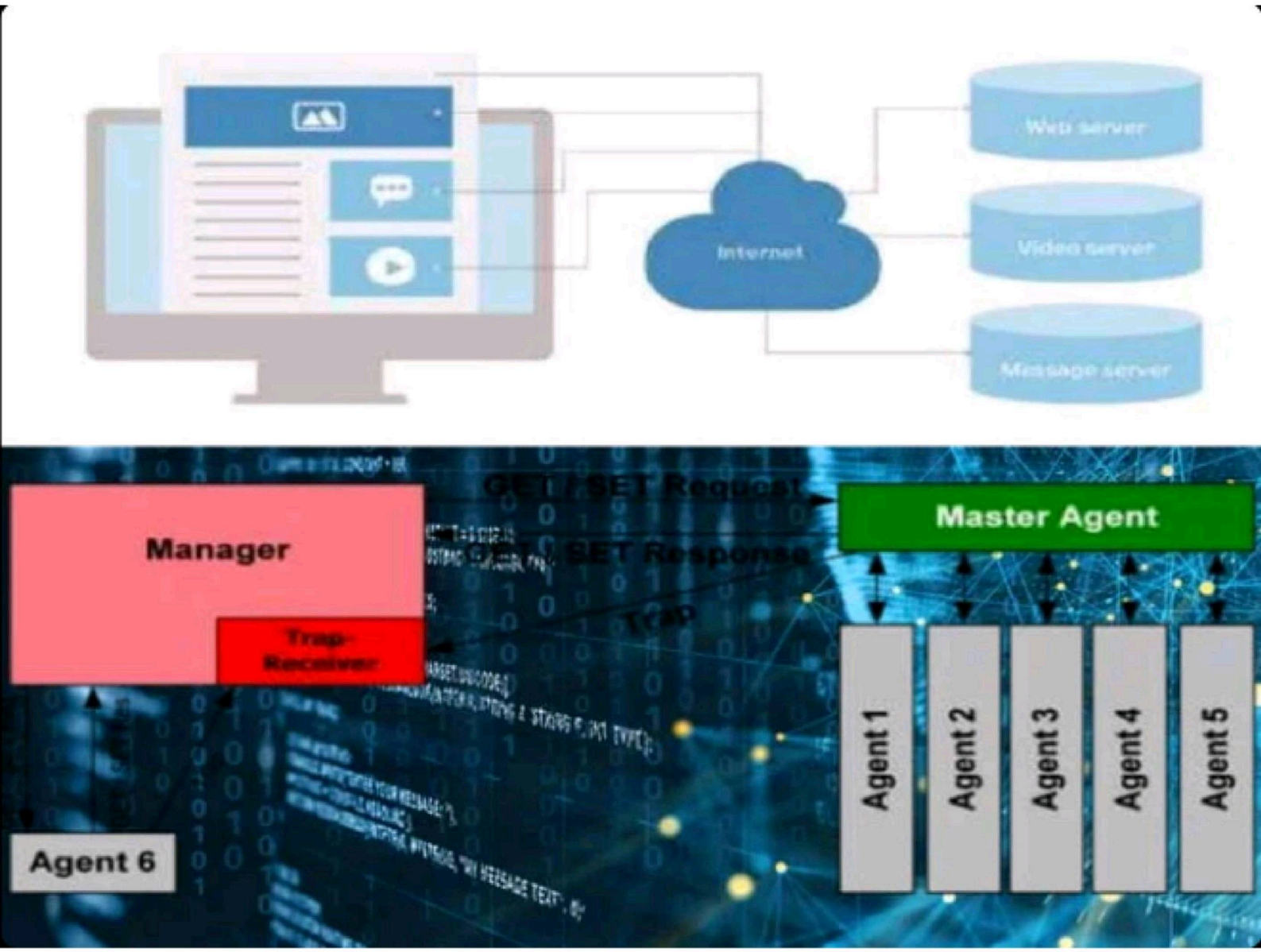
- Keeping a close eye on your network perimeter is always good practise. Even with strong firewalls in place, mistakes can happen and rogue traffic could get through.
- Users could also leverage methods such as tunnelling, external anonymizers, and VPNs to get around firewall rules.
- A network monitoring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

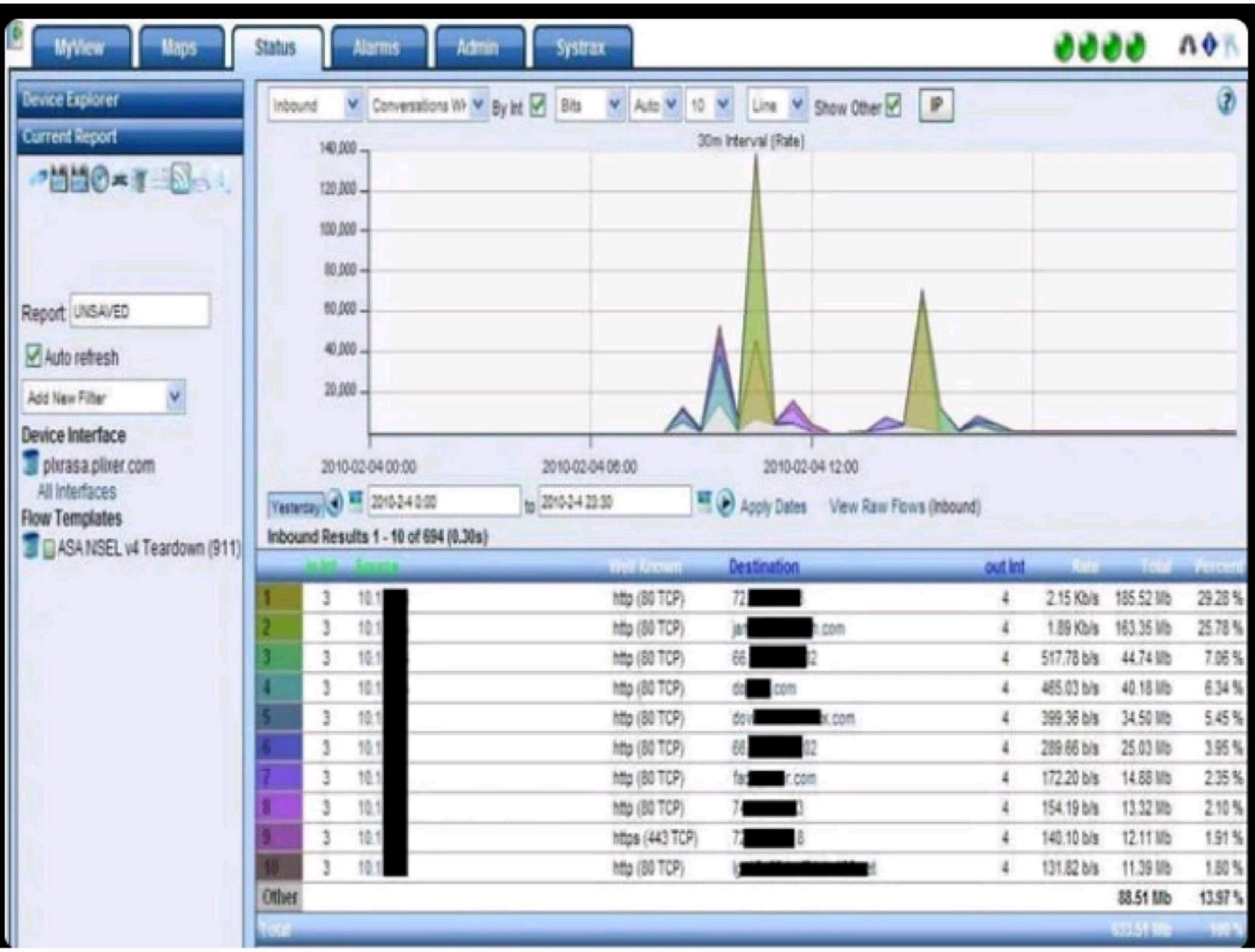
- Remote Desktop Protocol(RDP) is another commonly targeted application. Make sure you block any inbound connection attempts on your firewall.
- Monitoring traffic inside your firewalls allows you to validate rules, gain valuable insight, and can also be used as a source of network traffic-based alerts.

- 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)

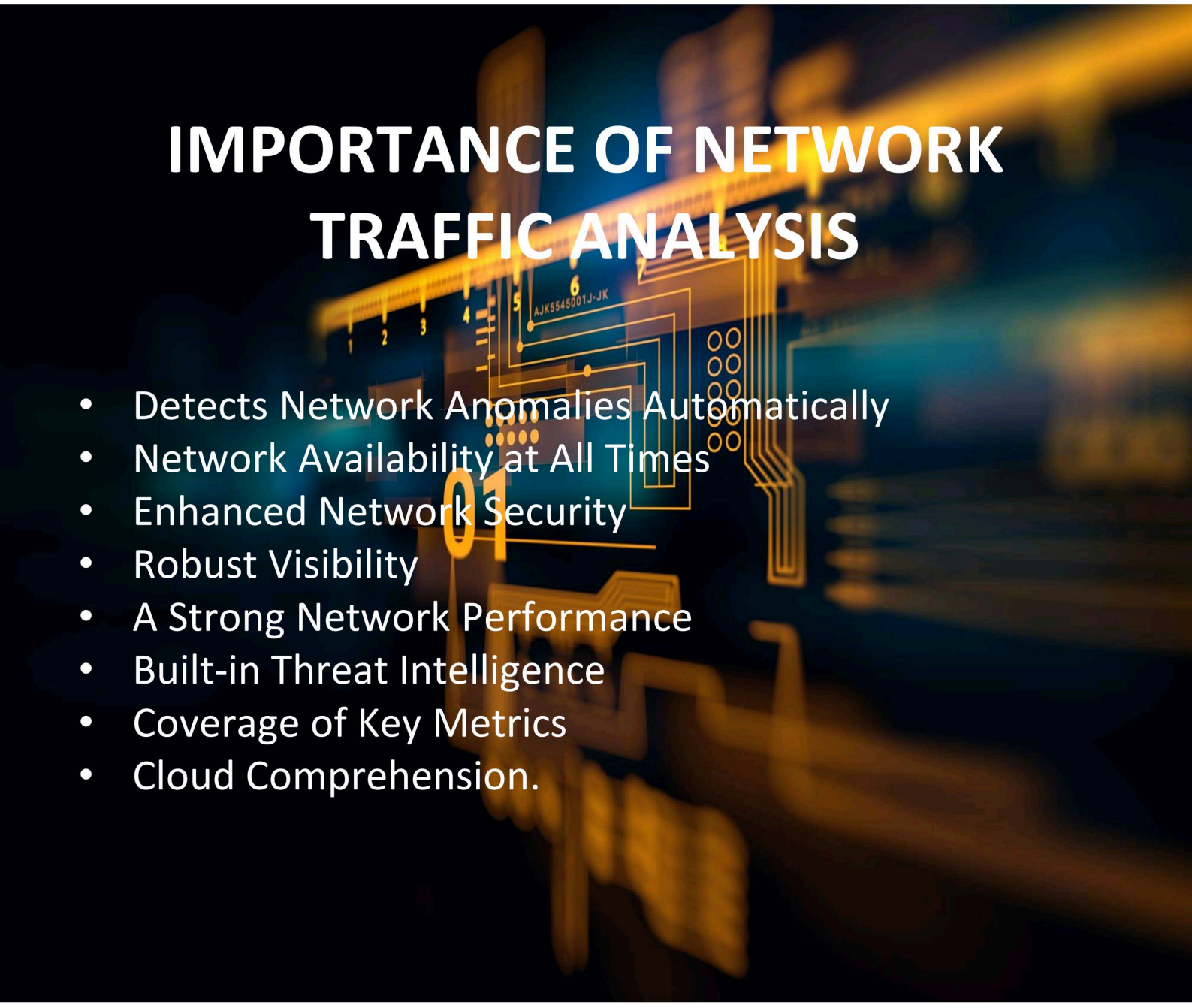



Internet
Web server
Video server
Message server
Manager
Trap-Receiver
GET / SET Request
SET Response
Trap
Master Agent
Agent 1
Agent 2
Agent 3
Agent 4
Agent 5
Agent 6


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
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
to
Apply Dates
View Raw Flows (Inbound)
Inbound Results 1 - 10 of 694 (0.30s)
Destination
out Int
Rate
Total
Percent
http (80 TCP)
https (443 TCP)
2.15 Kb/s
185.52 Mb
29.28 %
1.89 Kb/s
163.35 Mb
25.78 %
517.78 b/s
44.74 Mb
7.06 %
465.03 b/s
40.18 Mb
6.34 %
399.36 b/s
34.50 Mb
5.45 %
289.66 b/s
25.03 Mb
3.95 %
172.20 b/s
14.88 Mb
2.35 %
154.19 b/s
13.32 Mb
2.10 %
140.10 b/s
12.11 Mb
1.91 %
131.82 b/s
11.39 Mb
1.80 %
Other
88.51 Mb
13.97 %

USECASES FOR ANALYSING NETWORK TRAFFIC

- Detection of ransomware activity
- Monitoring data exfiltration/internet activity
- Monitor access to files on file services 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



IMPORTANCE OF NETWORK TRAFFIC ANALYSIS

- Detects Network Anomalies Automatically
- Network Availability at All Times
- Enhanced Network Security
- Robust Visibility
- A Strong Network Performance
- Built-in Threat Intelligence
- Coverage of Key Metrics
- Cloud Comprehension.

NETWORK PROTOCOLS

- Network protocols are a set of rules outlining how connected devices communicate across a network to exchange information easily and safely.
- Protocols serve as a common language for devices to enable communication irrespective of differences in software, hardware, or internal processes.

Types of network protocols

1. **Network Communication Protocols:**
    - Hyper-Text Transfer Protocol (HTTP)
    - Transmission Control Protocol (TCP)
    - Internet Protocol (IP)
    - User Datagram Protocol (UDP)
    - File Transfer Protocol (FTP)

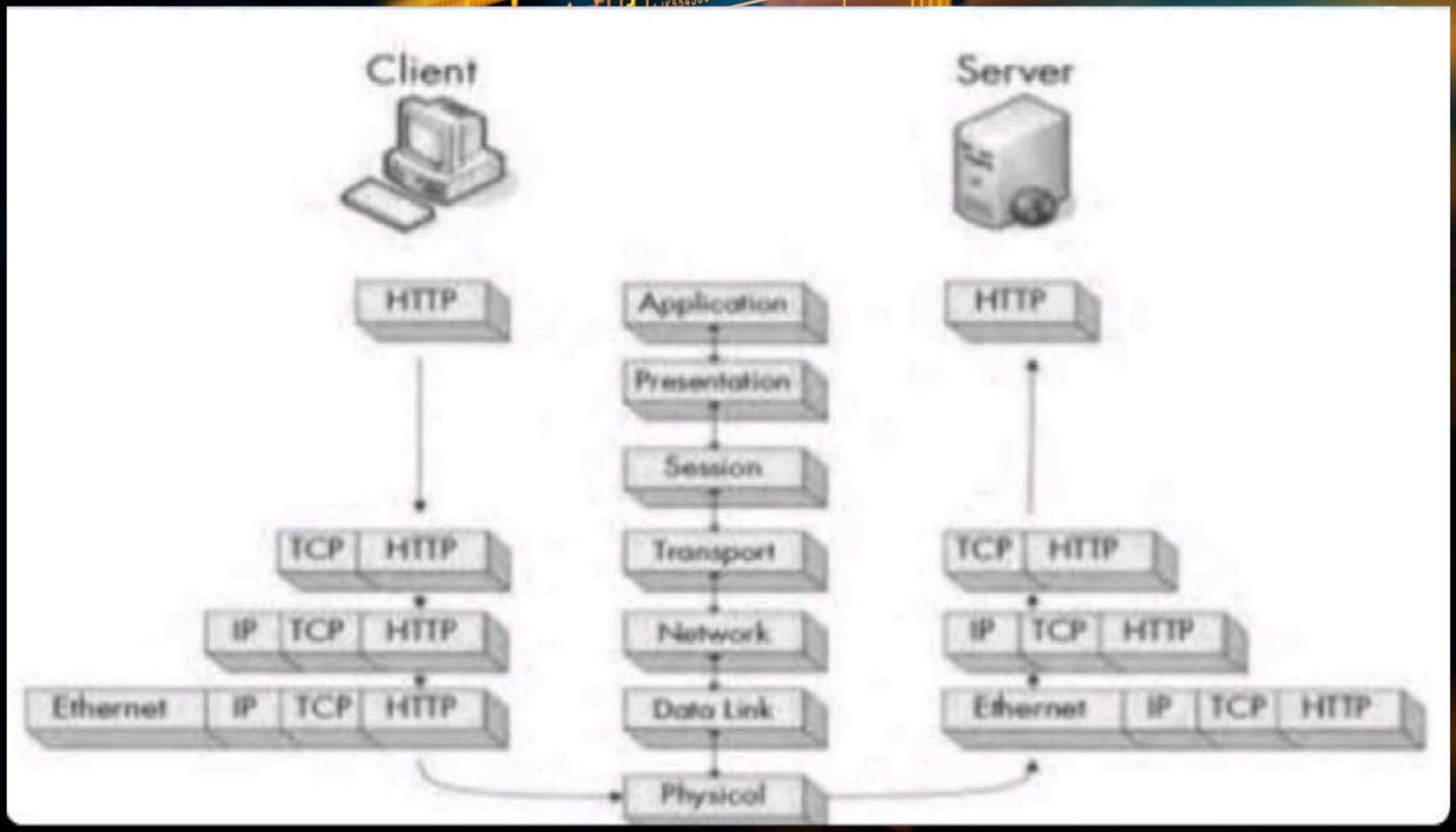
NETWORK PROTOCOLS

2. **Network Security Protocols:**
    - Secure File Transfer Protocol (SFTP)
    - Hyper-Text Transfer Protocol Secure (HTTPS)
    - Secure Socket Layer (SSL)

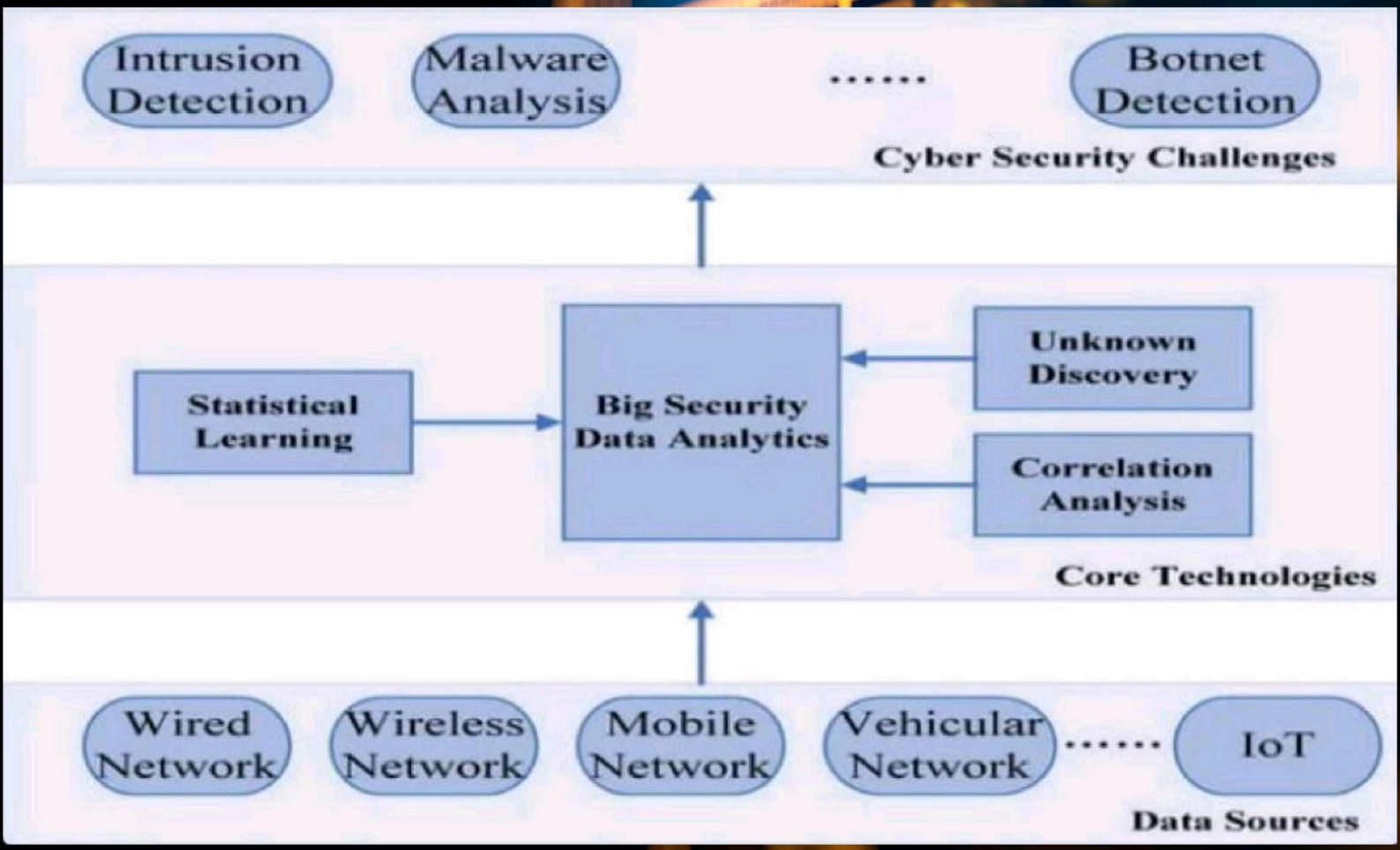
3. **Network Management Protocols**
    - Simple Network Management Protocol (SNMP)
    - Internet Control Message Protocol (ICMP)

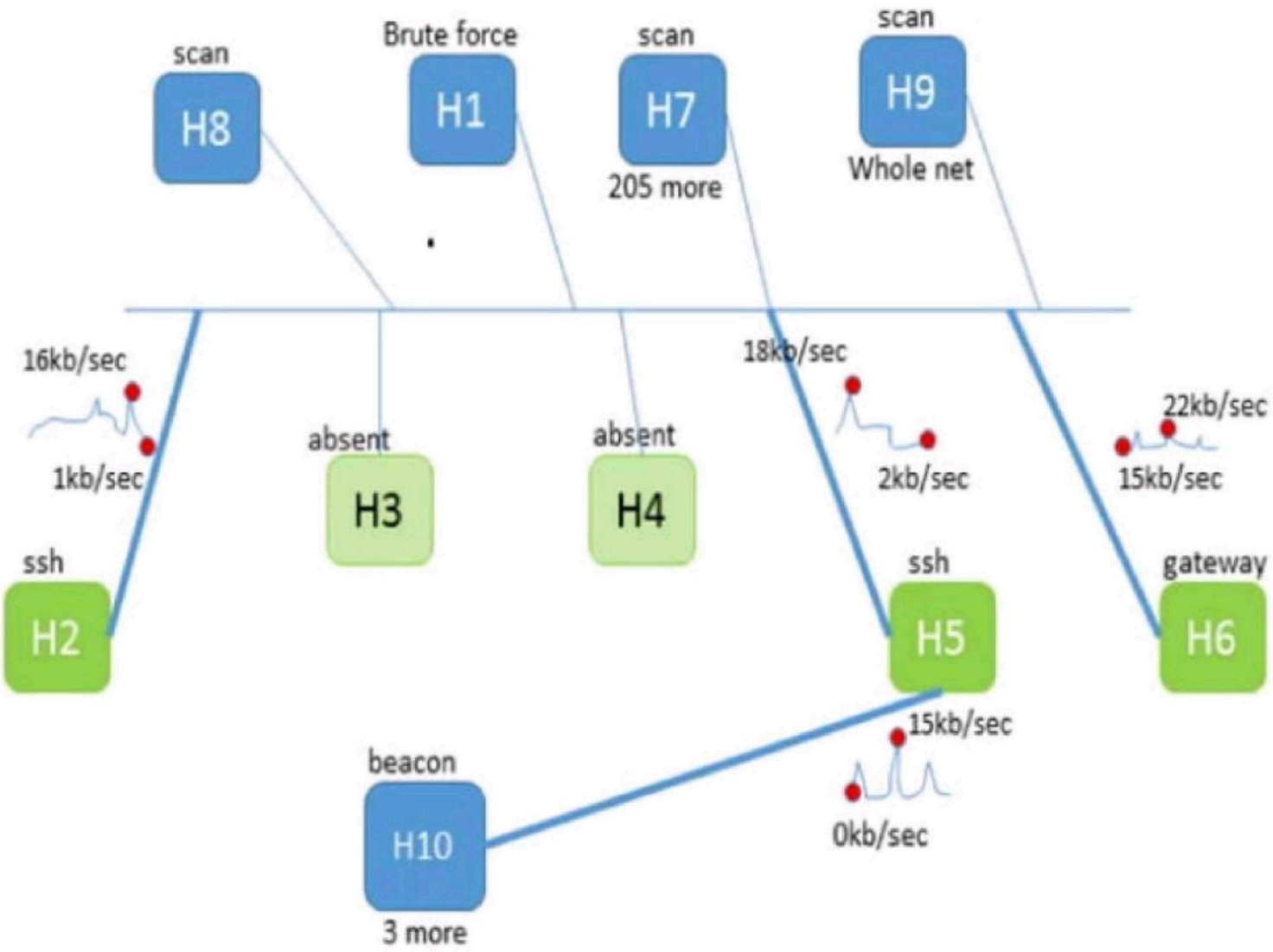
NETWORK PROTOCOLS

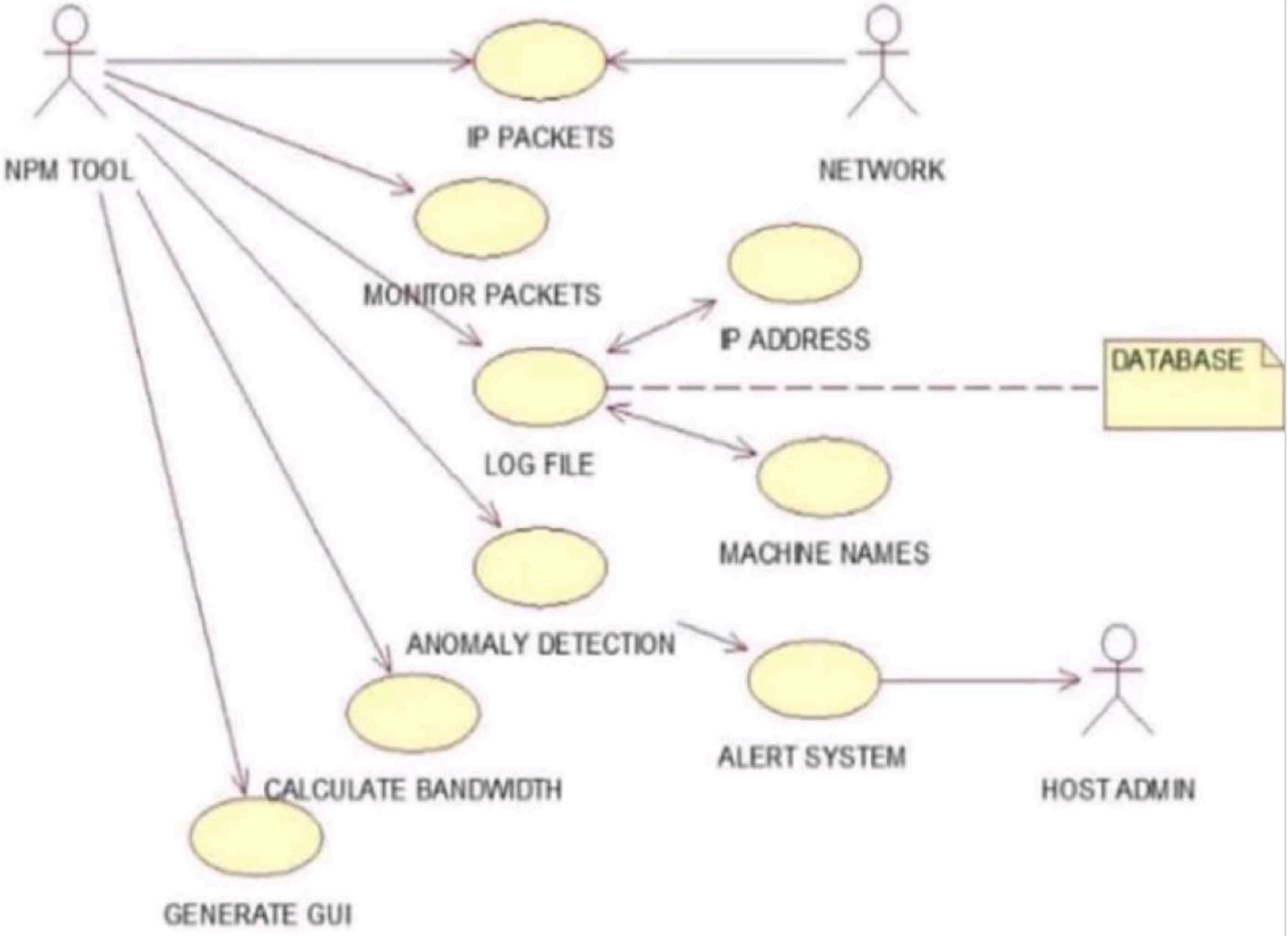
There are totally 7 layers of protocols for analysing network traffic

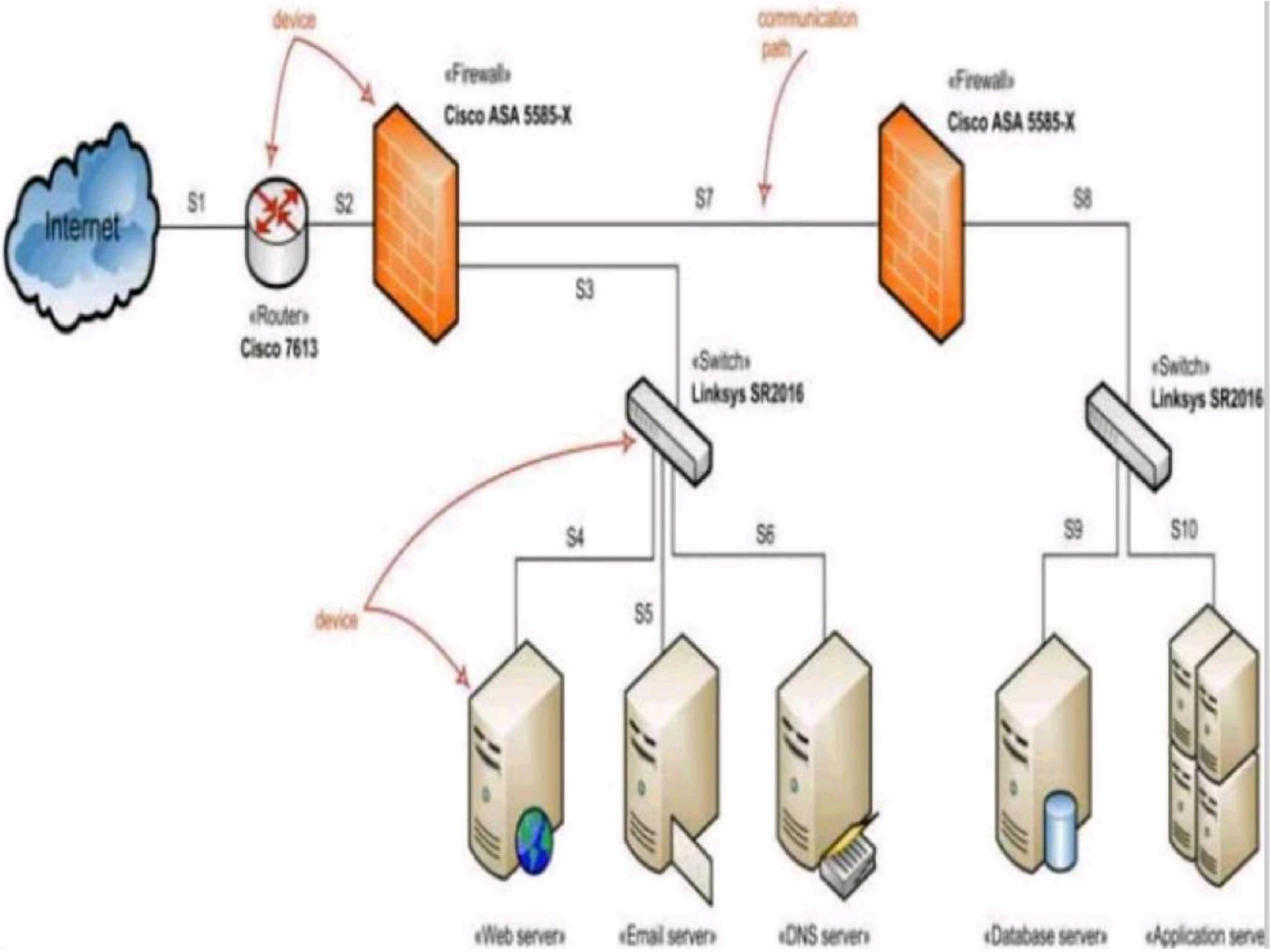


ARCHITECTURE DIAGRAM




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 serve

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.