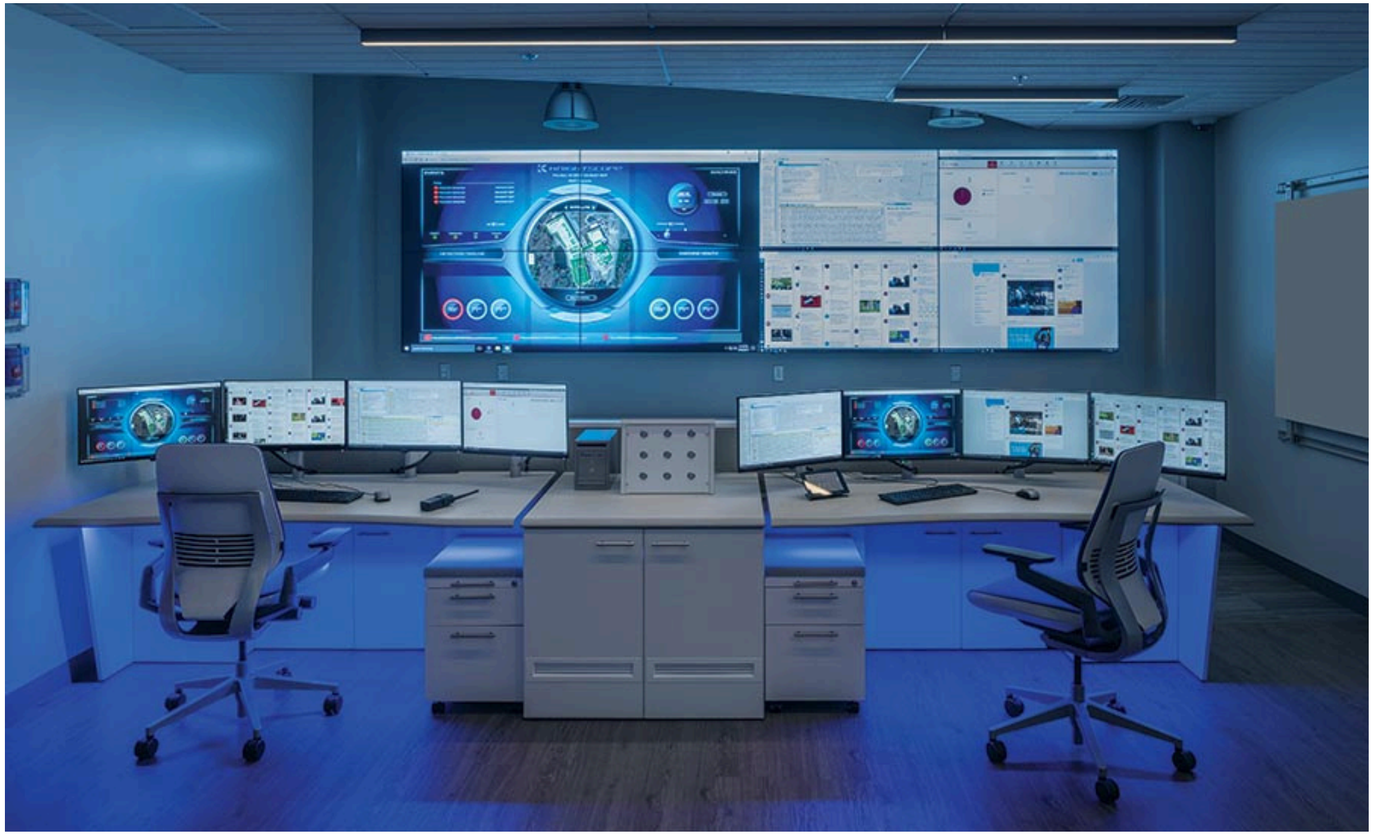
Security Operations Center (SOC)

Turki Al-Juaid Instructor
cybersecurity

- **Topics Outline**
- **Introduction to the Security Operations Center (SOC)**
- **Roles Within a Security Operations Center**
- **Incident Handling and Definition**
- **Cyber Kill Chain**
- **Incident Handling Process**
- **SOC analyst tools**
- **Security Information and Event Management (SIEM)**
- **Cyber Threat Intelligence (CTI)**
- **Introduction Forensics**
- **JavaScript obfuscation**
- **Malware Analysis**
- **Security Incident Reporting**
- **Required Skills and Knowledge**

- **A Security Operations Center (SOC) is an essential facility that houses a team of information security experts responsible for continuously monitoring and evaluating an organization's security status**
- **The main objective of a SOC team is to identify, examine, and address cybersecurity incidents by employing a mix of technology solutions and a comprehensive set of procedures.**

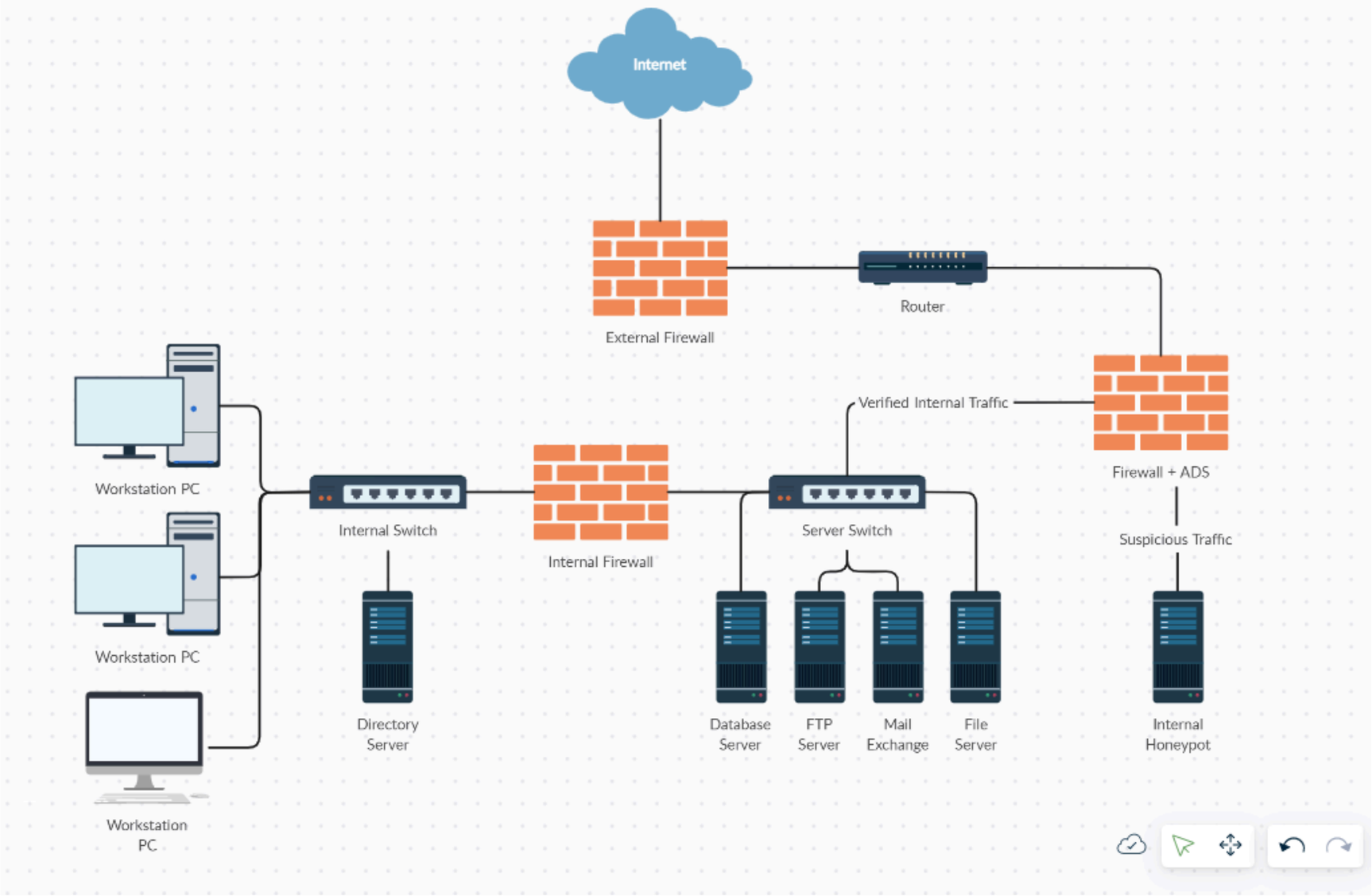


Turki Al-Juaid Instructor
cybersecurity

- **Roles Within A SOC**

1. **SOC Manager: Oversees day-to-day operations, manages the team, coordinates incident response efforts, and ensures smooth collaboration with other departments.**
2. **Tier 3 Analyst: Provides advanced expertise in handling complex security incidents**
3. **Tier 2 Analyst: Performs in-depth analysis of escalated incidents**
4. **Tier 1 Analyst: Monitors security alerts and events**

- **Example Infrastructure**



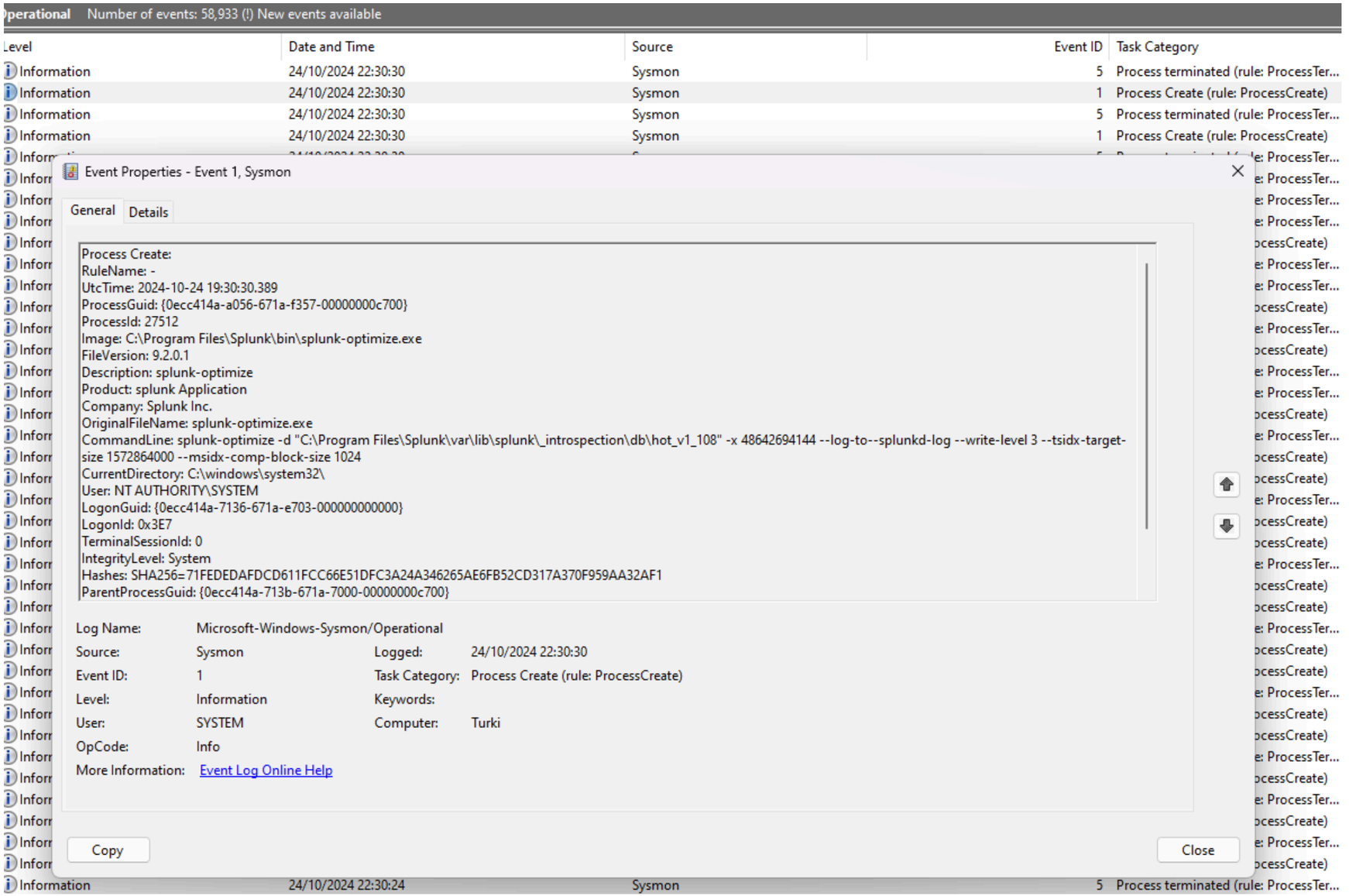
Turki Al-Juaid Instructor
cybersecurity

- **Incident Handling Definition & Scope**
- **Incident handling (IH) has become an important part of an organization's defensive capability against cybercrime.**
- **While protective measures are constantly being implemented to prevent or lower the amount of security incidents**

1. **An event is an action occurring in a system or network. Examples of events are:**
2. **A user sending an email**
3. **A mouse click**
4. **A firewall allowing a connection request**
5. **A file being downloaded**
6. **A user logging into an application**

Turki Al-Juaid Instructor
cybersecurity

- **Example event**



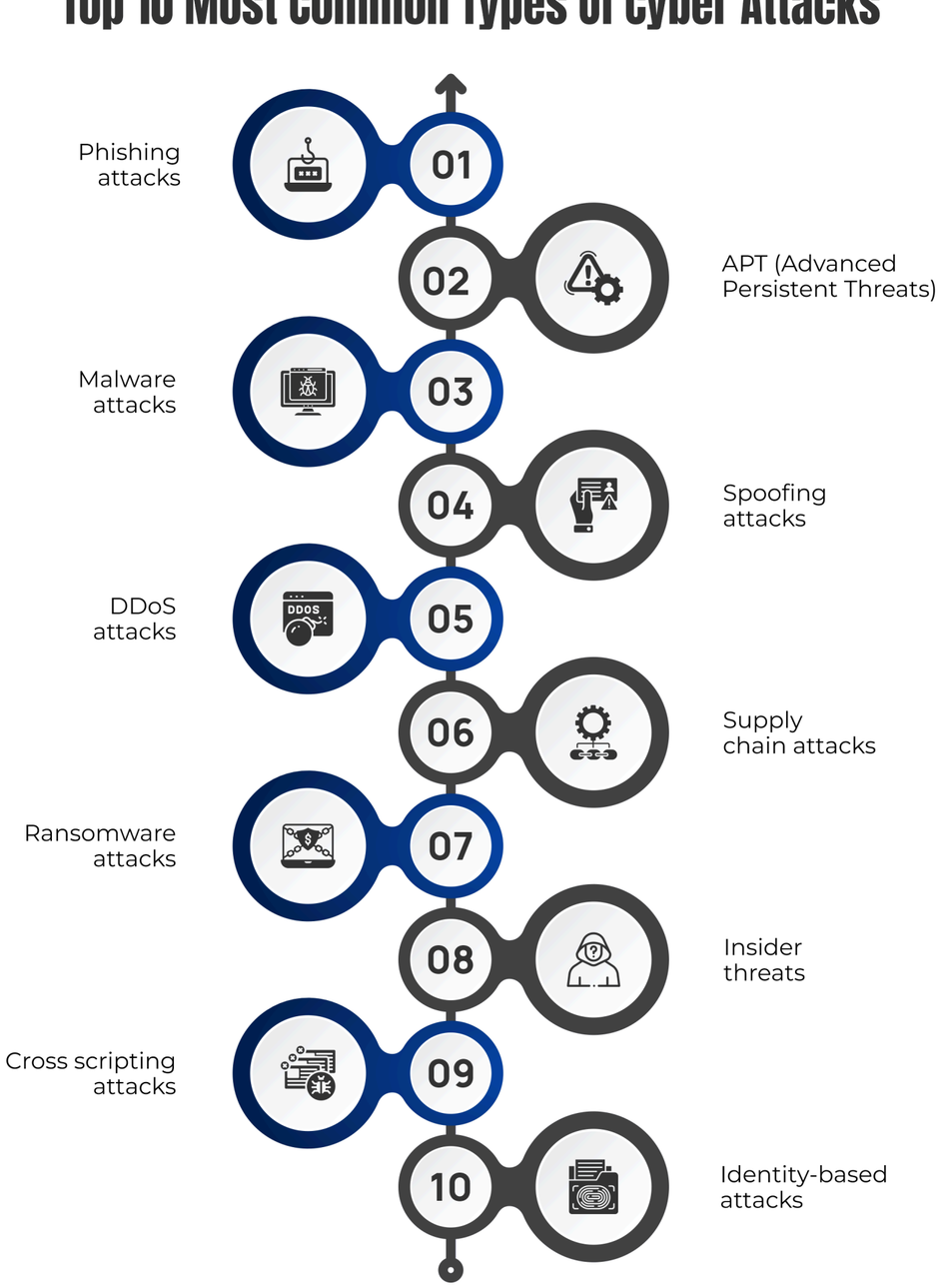
Turki Al-Juaid Instructor
cybersecurity

Protocol	Service	Port Number
FTP	File Transfer Protocol	20, 21
Telnet	Telnet	23
SSH	Secure Shell	22
SMTP	Simple Mail Transfer Protocol	25
DNS	Domain Name System	53
DHCP	Dynamic Host Configuration Protocol	67, 68
HTTP	Hyper Text Transfer Protocol	80
POP3	Post Office Protocol	110
NTP	Network Time Protocol	123
NetBIOS	NetBIOS Name Service	135 - 139
IMAP	Internet Message Access Protocol	143

Protocol	Service	Port Number
SNMP	Simple Network Management Protocol	161, 162
LDAP	Lightweight Directory Access Protocol	389
HTTPS	Secure Hyper Text Transfer Protocol	443
MS SQL	Microsoft SQL	1433
MySQL	mySQL Database	3306
RDP	Remote Desktop Protocol	3389
Syslog	Used to send logs to remote server	514
TLS Syslog	Secure Syslog	6514
SFTP	Secure File Transfer Protocol	22
Secure SMTP	Secure Simple Mail Transfer Protocol	587

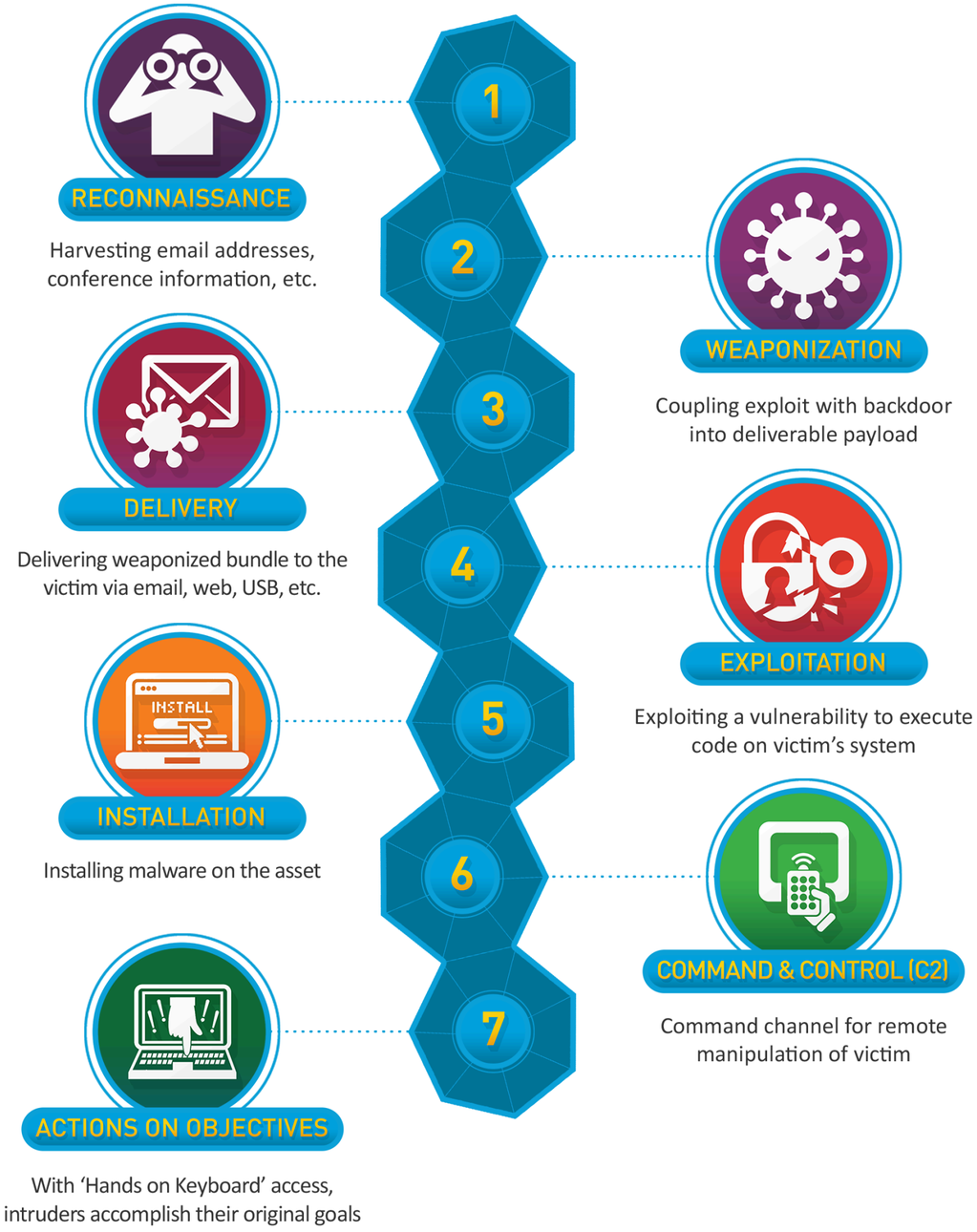
- **An incident is an event with a negative consequence. One example of an incident is a system crash. Another example is unauthorized access to sensitive data. Incidents can also occur due to natural disasters, power failures, etc.**
- **Data theft**
- **Funds theft**
- **Unauthorized access to data**
- **Installation and usage of malware and remote access tools**

- **Cyberattack**
- **A cyberattack is any intentional effort to steal, expose, alter, disable, or destroy data, applications, or other assets through unauthorized access to a network, computer system or digital device.**



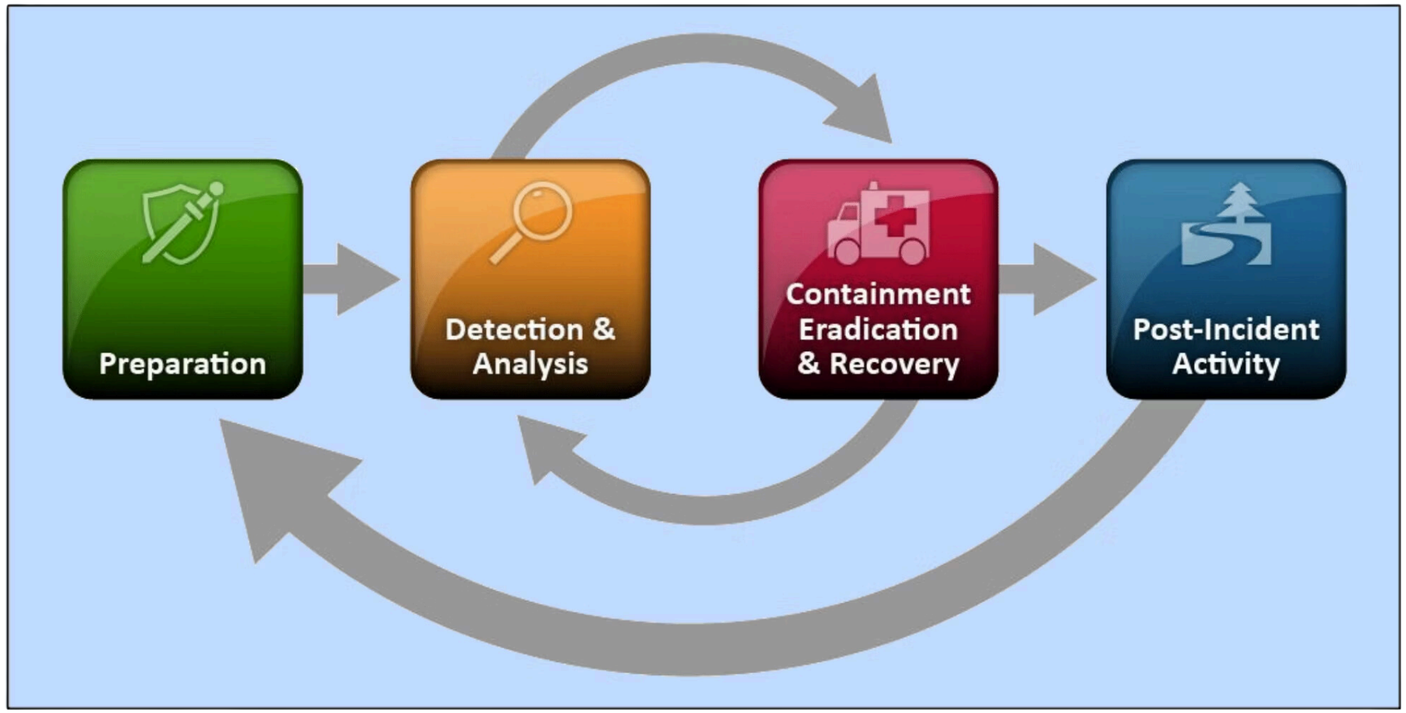
Turki Al-Juaid Instructor
cybersecurity

- **Cyber Kill Chain**
- **The cyber kill chain is a series of steps that trace stages of a cyberattack from the early reconnaissance stages to the exfiltration of data**



Turki Al-Juaid Instructor
cybersecurity

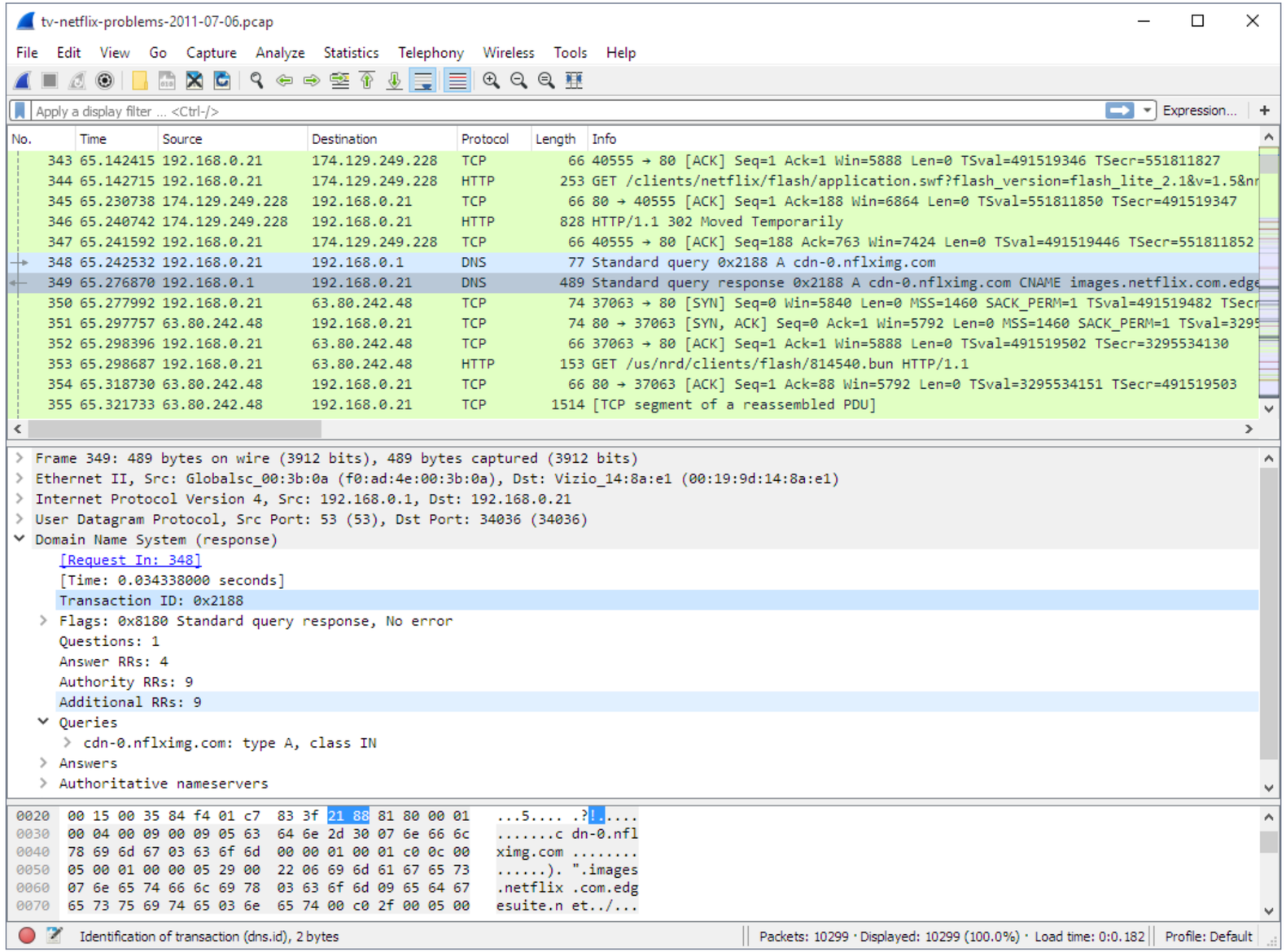
- **Incident Handling Process**



- **SOC analyst tools**

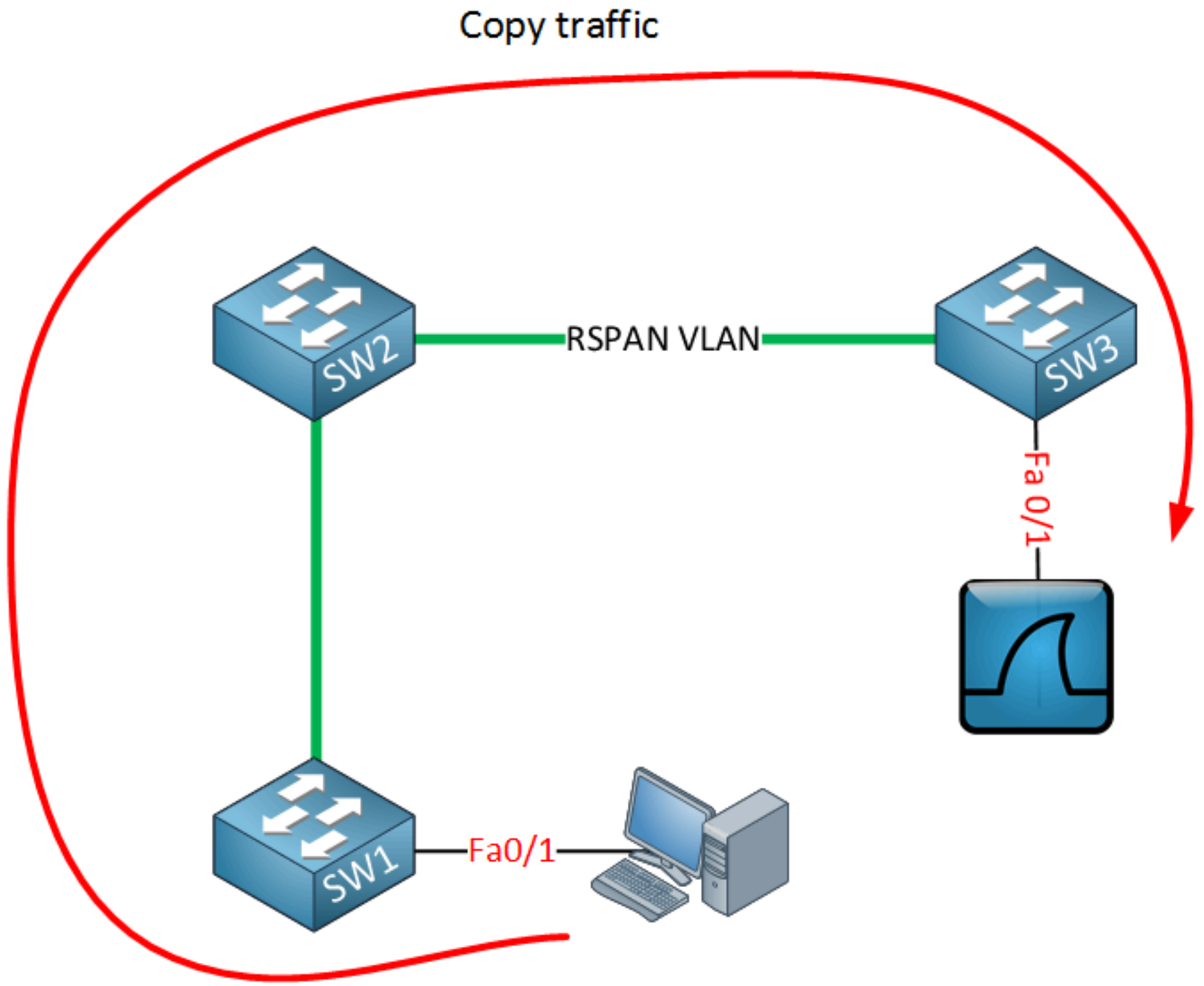
1. **Endpoint Detection and Response (EDR): Detect and respond to suspicious activities on endpoints like laptops, mobile devices, and servers.**
2. **Security Information and Event Management (SIEM): Collect and analyze data from an organization's applications, devices, servers, and users in real-time.**
3. **Vulnerability management (VM): Scan networks and computer systems for signs of vulnerabilities.**
4. **Intrusion detection systems (IDS): Observe network traffic, alerting security teams of any potential security threats.**
5. **Sandboxing: cybersecurity practice where you run code, observe and analyze and code in a safe**
6. **Virus Total : is an online service that analyzes suspicious files and URLs to detect types of malware and malicious content using antivirus engines and website scanners.**
7. **Cortex XSOAR : helps simplify security operations by unifying automation, case management, real-time collaboration and threat intel management**
8. **Wireshark capture and display real-time details of network traffic.**

- **Wireshark**
- **capture and display real-time details of network traffic.**



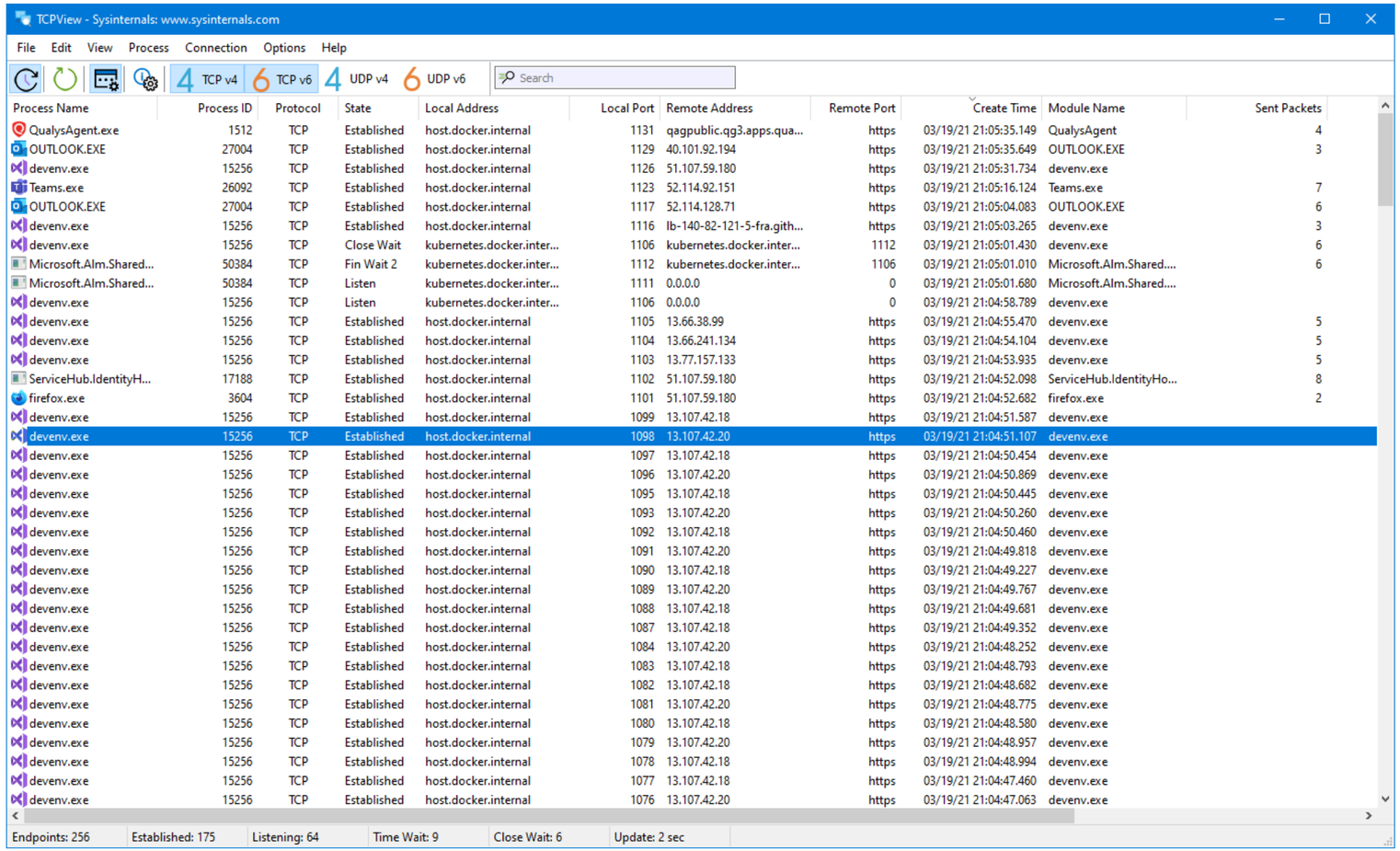
Turki Al-Juaid Instructor
cybersecurity

- **Switch Port Analyzer or SPAN**
- **feature of Cisco switches that allows you to copy all traffic from a single or multiple source ports or source VLANs to a destination interface**



Turki Al-Juaid Instructor
cybersecurity

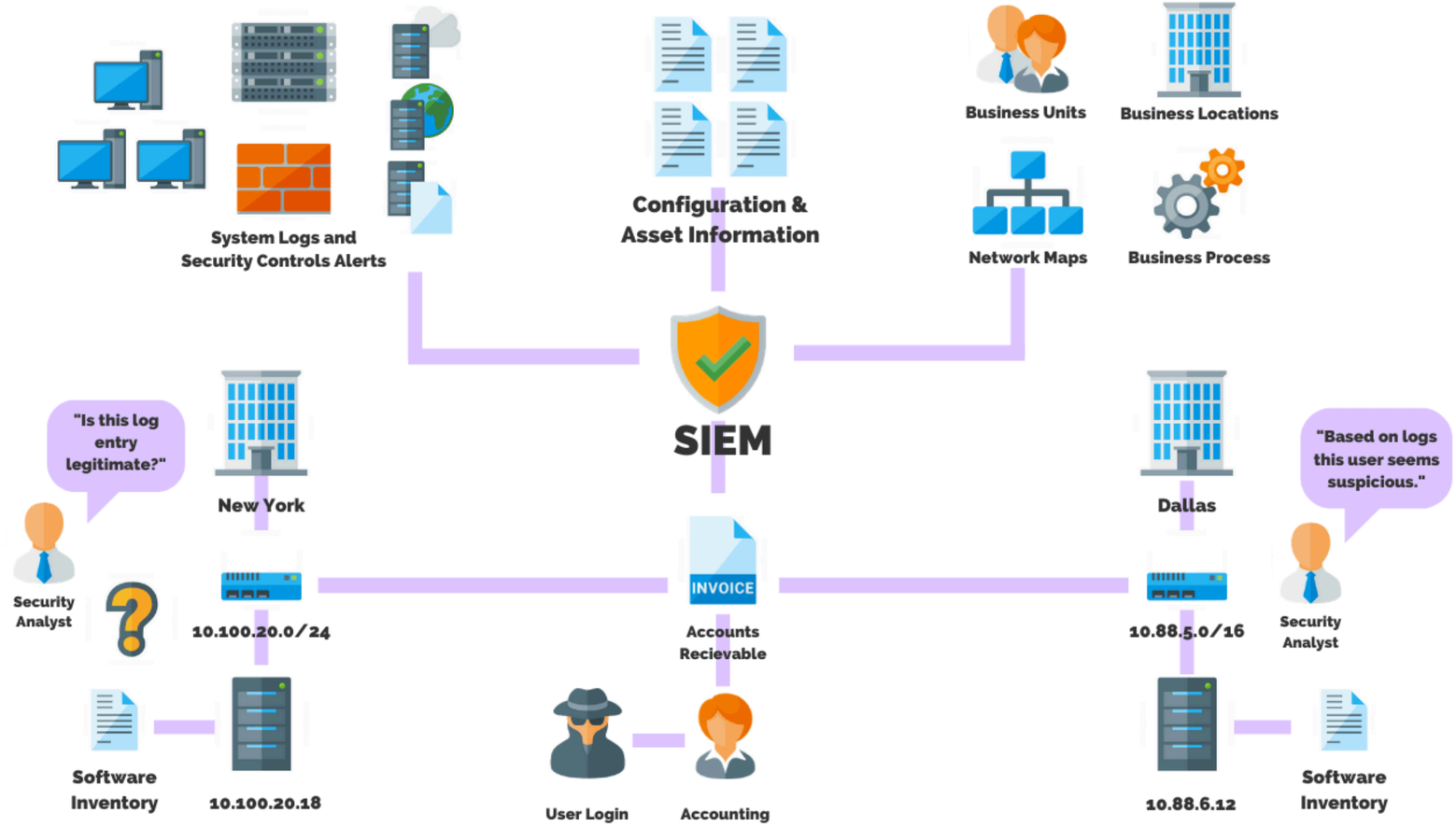
- **Monitoring Connections**
- **The process is doing something strange with the network, like connecting to a port, connecting to Twitter, downloading data, or doing something else that is not normal.**



Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create Time	Module Name	Sent Packets
QualysAgent.exe	1512	TCP	Established	host.docker.internal	1131	qagpublic.qg3.apps.qua...	https	03/19/21 21:05:35.149	QualysAgent	4
OUTLOOK.EXE	27004	TCP	Established	host.docker.internal	1129	40.101.92.194	https	03/19/21 21:05:35.649	OUTLOOK.EXE	3
devenv.exe	15256	TCP	Established	host.docker.internal	1126	51.107.59.180	https	03/19/21 21:05:31.734	devenv.exe	
Teams.exe	26092	TCP	Established	host.docker.internal	1123	52.114.92.151	https	03/19/21 21:05:16.124	Teams.exe	7
OUTLOOK.EXE	27004	TCP	Established	host.docker.internal	1117	52.114.128.71	https	03/19/21 21:05:04.083	OUTLOOK.EXE	6
devenv.exe	15256	TCP	Established	host.docker.internal	1116	lb-140-82-121-5-fra.gith...	https	03/19/21 21:05:03.265	devenv.exe	3
devenv.exe	15256	TCP	Close Wait	kubernetes.docker.inter...	1106	kubernetes.docker.inter...	1112	03/19/21 21:05:01.430	devenv.exe	6
Microsoft.Alm.Shared...	50384	TCP	Fin Wait 2	kubernetes.docker.inter...	1112	kubernetes.docker.inter...	1106	03/19/21 21:05:01.010	Microsoft.Alm.Shared....	6
Microsoft.Alm.Shared...	50384	TCP	Listen	kubernetes.docker.inter...	1111	0.0.0.0	0	03/19/21 21:05:01.680	Microsoft.Alm.Shared....	
devenv.exe	15256	TCP	Listen	kubernetes.docker.inter...	1106	0.0.0.0	0	03/19/21 21:04:58.789	devenv.exe	
devenv.exe	15256	TCP	Established	host.docker.internal	1105	13.66.38.99	https	03/19/21 21:04:55.470	devenv.exe	5
devenv.exe	15256	TCP	Established	host.docker.internal	1104	13.66.241.134	https	03/19/21 21:04:54.104	devenv.exe	5
devenv.exe	15256	TCP	Established	host.docker.internal	1103	13.77.157.133	https	03/19/21 21:04:53.935	devenv.exe	5
ServiceHub.IdentityH...	17188	TCP	Established	host.docker.internal	1102	51.107.59.180	https	03/19/21 21:04:52.098	ServiceHub.IdentityHo...	8
firefox.exe	3604	TCP	Established	host.docker.internal	1101	51.107.59.180	https	03/19/21 21:04:52.682	firefox.exe	2
devenv.exe	15256	TCP	Established	host.docker.internal	1099	13.107.42.18	https	03/19/21 21:04:51.587	devenv.exe	
devenv.exe	15256	TCP	Established	host.docker.internal	1098	13.107.42.20	https	03/19/21 21:04:51.107	devenv.exe	
devenv.exe	15256	TCP	Established	host.docker.internal	1097	13.107.42.18	https	03/19/21 21:04:50.454	devenv.exe	
devenv.exe	15256	TCP	Established	host.docker.internal	1096	13.107.42.20	https	03/19/21 21:04:50.869	devenv.exe	
devenv.exe	15256	TCP	Established	host.docker.internal	1095	13.107.42.18	https	03/19/21 21:04:50.445	devenv.exe	
devenv.exe	15256	TCP	Established	host.docker.internal	1093	13.107.42.20	https	03/19/21 21:04:50.260	devenv.exe	
devenv.exe	15256	TCP	Established	host.docker.internal	1092	13.107.42.18	https	03/19/21 21:04:50.460	devenv.exe	
devenv.exe	15256	TCP	Established	host.docker.internal	1091	13.107.42.20	https	03/19/21 21:04:49.818	devenv.exe	
devenv.exe	15256	TCP	Established	host.docker.internal	1090	13.107.42.18	https	03/19/21 21:04:49.227	devenv.exe	
devenv.exe	15256	TCP	Established	host.docker.internal	1089	13.107.42.20	https	03/19/21 21:04:49.767	devenv.exe	
devenv.exe	15256	TCP	Established	host.docker.internal	1088	13.107.42.18	https	03/19/21 21:04:49.681	devenv.exe	
devenv.exe	15256	TCP	Established	host.docker.internal	1087	13.107.42.18	https	03/19/21 21:04:49.352	devenv.exe	
devenv.exe	15256	TCP	Established	host.docker.internal	1084	13.107.42.20	https	03/19/21 21:04:48.252	devenv.exe	
devenv.exe	15256	TCP	Established	host.docker.internal	1083	13.107.42.18	https	03/19/21 21:04:48.793	devenv.exe	
devenv.exe	15256	TCP	Established	host.docker.internal	1082	13.107.42.18	https	03/19/21 21:04:48.682	devenv.exe	
devenv.exe	15256	TCP	Established	host.docker.internal	1081	13.107.42.20	https	03/19/21 21:04:48.775	devenv.exe	
devenv.exe	15256	TCP	Established	host.docker.internal	1080	13.107.42.18	https	03/19/21 21:04:48.580	devenv.exe	
devenv.exe	15256	TCP	Established	host.docker.internal	1079	13.107.42.20	https	03/19/21 21:04:48.957	devenv.exe	
devenv.exe	15256	TCP	Established	host.docker.internal	1078	13.107.42.18	https	03/19/21 21:04:48.994	devenv.exe	
devenv.exe	15256	TCP	Established	host.docker.internal	1077	13.107.42.18	https	03/19/21 21:04:47.460	devenv.exe	
devenv.exe	15256	TCP	Established	host.docker.internal	1076	13.107.42.20	https	03/19/21 21:04:47.063	devenv.exe	

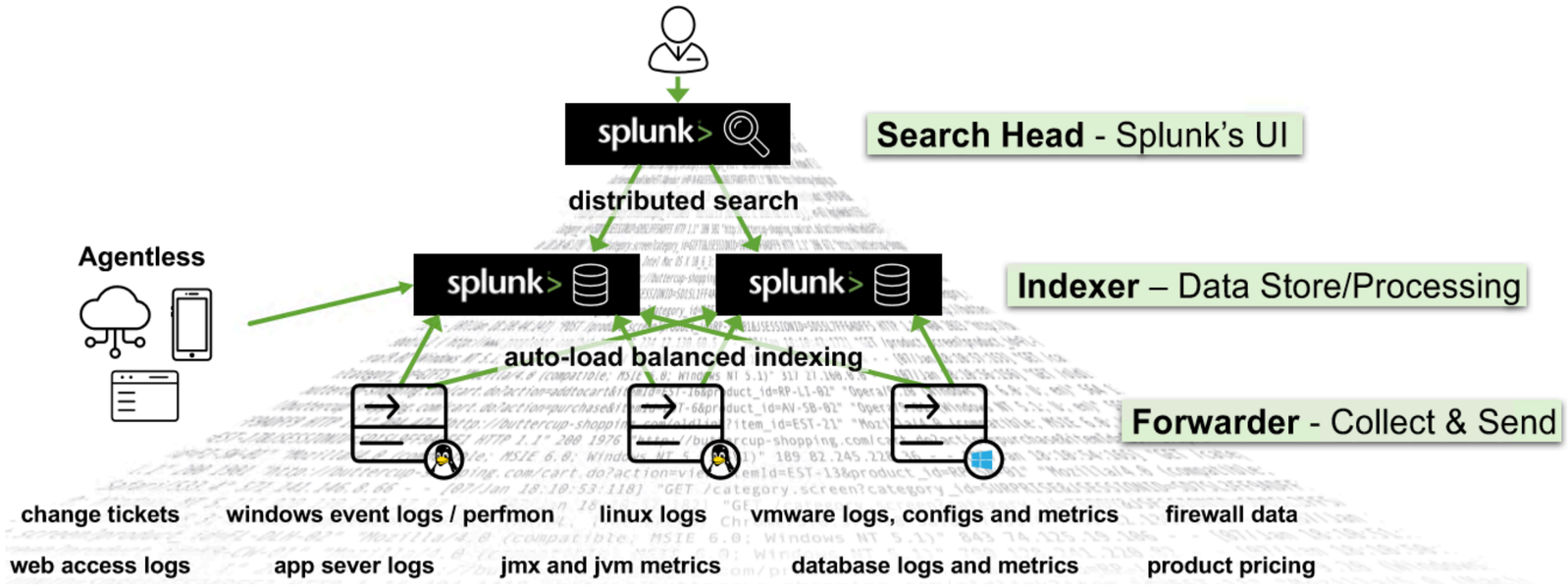
Turki Al-Juaid Instructor
cybersecurity

- **Security Information and Event Management (SIEM)**

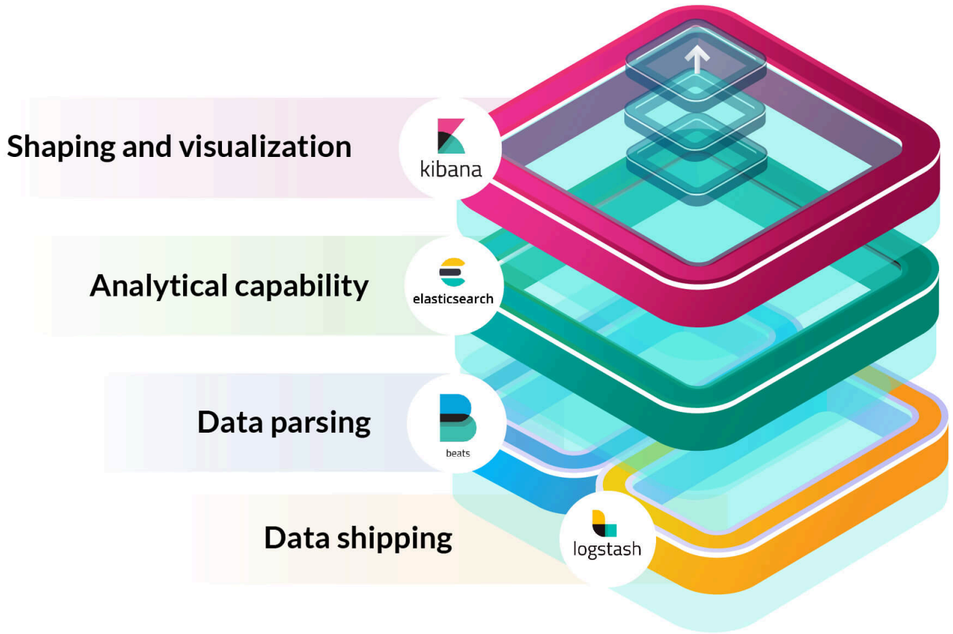


Turki Al-Juaid Instructor
cybersecurity

- **Security Information and Event Management (SIEM)**



- **Elastic Stack**



- **Elastic Stack**

- **Effectively Using ELK - LAB**

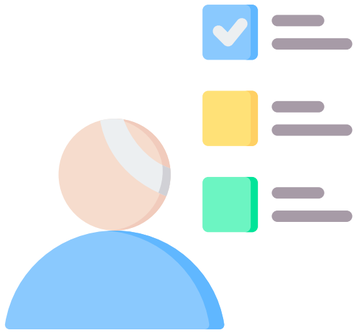
CLICK HERE

Turki Al-Juaid Instructor
cybersecurity

- **MITRE ATT&CK**
- **regularly updated resource outlining the tactics, techniques, and procedures (TTPs) employed by cyber threat actors.**

- **Alert Triaging**
- **process of evaluating and prioritizing security alerts generated by various monitoring and detection systems to determine their level of threat and potential impact on an organization's systems and data**

True Positive	False Positive
False Negative	True Negative



- **WebStrike Lab**

Turki Al-Juaid Instructor
cybersecurity

- **Cyber Threat Intelligence (CTI)**
- **cyber threat intelligence team investigates and tracks cyber attacks against organisations around the world**

CLICK HERE

Turki Al-Juaid Instructor
cybersecurity

- **Cyber Threat Intelligence (CTI)**
- **cyber threat intelligence team investigates and tracks cyber attacks against organisations around the world**

- **Yellow RAT Lab**

CLICK HERE

Turki Al-Juaid Instructor
cybersecurity

- **Windows Event Logs**
- **Windows event logging offers comprehensive logging capabilities for application errors, security events, and diagnostic information**

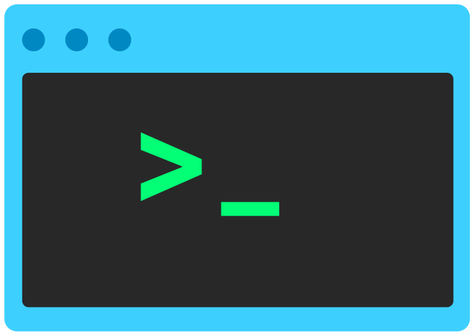
Turki Al-Juaid Instructor
cybersecurity

- **macOS Event Logs**

CLICK HERE

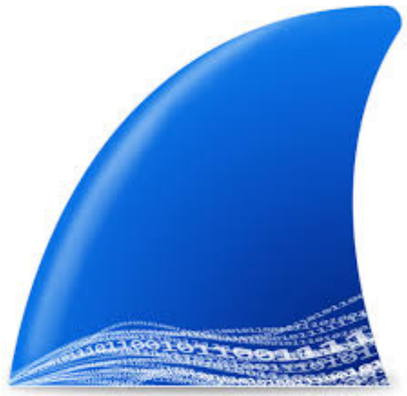
Turki Al-Juaid Instructor
cybersecurity

- **Linux Event Logs**



Turki Al-Juaid Instructor
cybersecurity

- **Wireshark**
- **Scanning Attack - LAB**



Turki Al-Juaid Instructor
cybersecurity

- **Foundational Forensics: Acquaint yourself with the core concepts of digital forensics, understanding its significance in today's interconnected world. Learn about evidence acquisition processes that stand robust against scrutiny.**
- **Tools covered include:**

1. **FTK Imager**
2. **Volatility**

- **Memory Forensics: Dive into the intricacies of volatile memory analysis**
- **Disk Forensics: Dissect disk images, examining their structures, files, and the tales they silently narrate.**

- **Endpoint Forensics**
- **Endpoint forensics is the process of collecting, analyzing, and preserving digital evidence from endpoints—devices like laptops, mobile phones.**
- **FTK Imager is one of the most widely used disk imaging tools in the cybersecurity field. It allows us to create perfect copies (or images) of computer disks for analysis**

- **Hunter Lab**

CLICK HERE

Turki Al-Juaid Instructor
cybersecurity

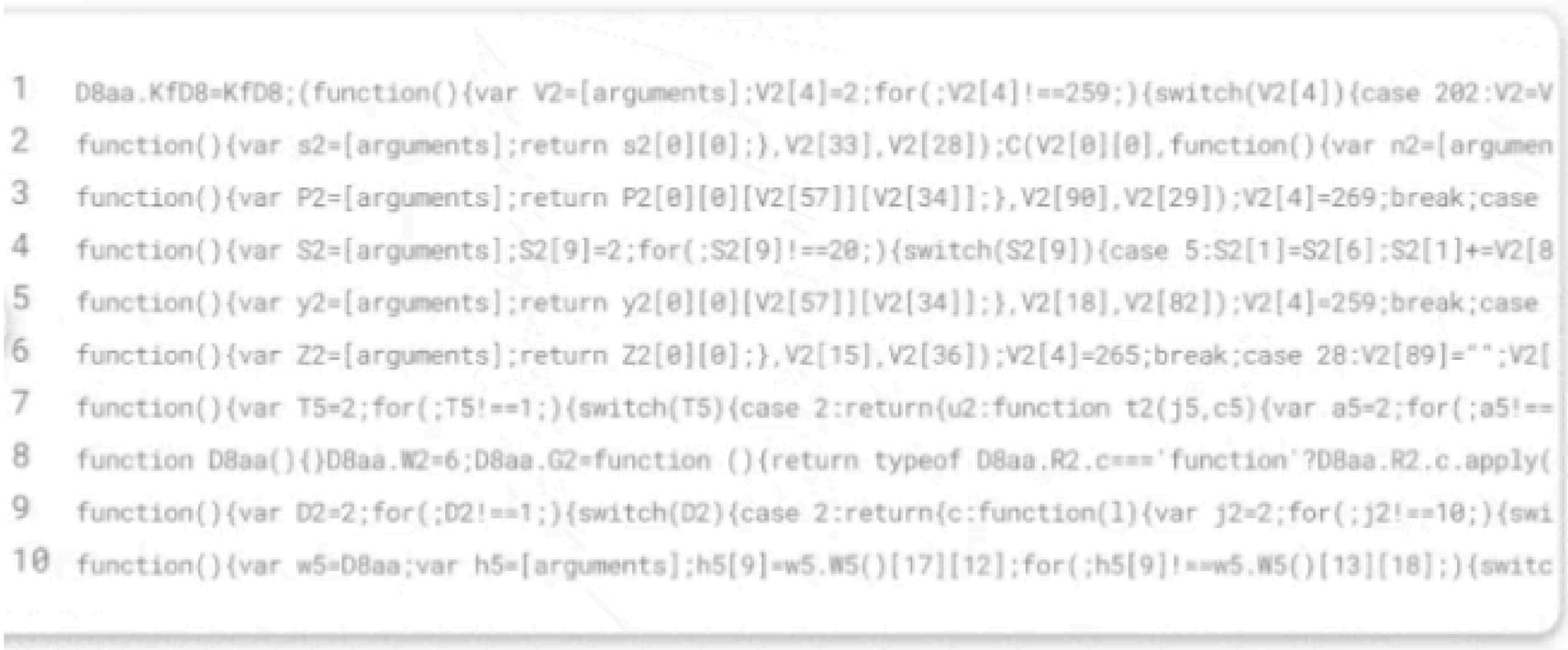
- **Endpoint Forensics**

- **Ramnit Lab**

CLICK HERE

Turki Al-Juaid Instructor
cybersecurity

- **JavaScript obfuscation**
- **process of transforming client-side JavaScript code into a format that is difficult for humans to understand while still being executable by browser**
- **Code deobfuscation is an important skill to learn if we want to be skilled in code analysis and reverse engineering.**



Original

Obfuscated

Turki Al-Juaid Instructor
cybersecurity

- **JavaScript obfuscation**
- **process of transforming client-side JavaScript code into a format that is difficult for humans to understand while still being executable by browser**
- **Code deobfuscation is an important skill to learn if we want to be skilled in code analysis and reverse engineering.**

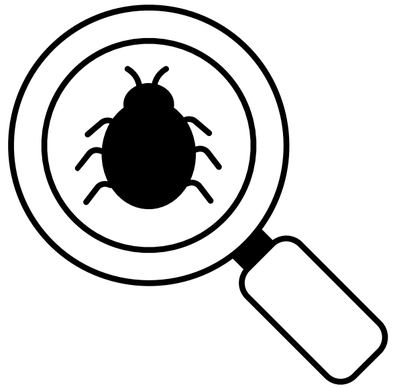
- **Malware Definition**
- **Malware, short for malicious software, is a term encompassing various types of software designed to infiltrate, exploit, or damage computer systems, networks, and data.**
- **Viruses**
- **Worms**
- **Trojans**
- **Ransomware**
- **Botnets**

The techniques employed in malware analysis encompass a wide array of methods and tools, including:

- **Static Analysis:** This approach involves scrutinizing the malware's code without executing
- **Dynamic Analysis:** Dynamic analysis entails executing the malware within a controlled environment, such as a sandbox or virtual machine,

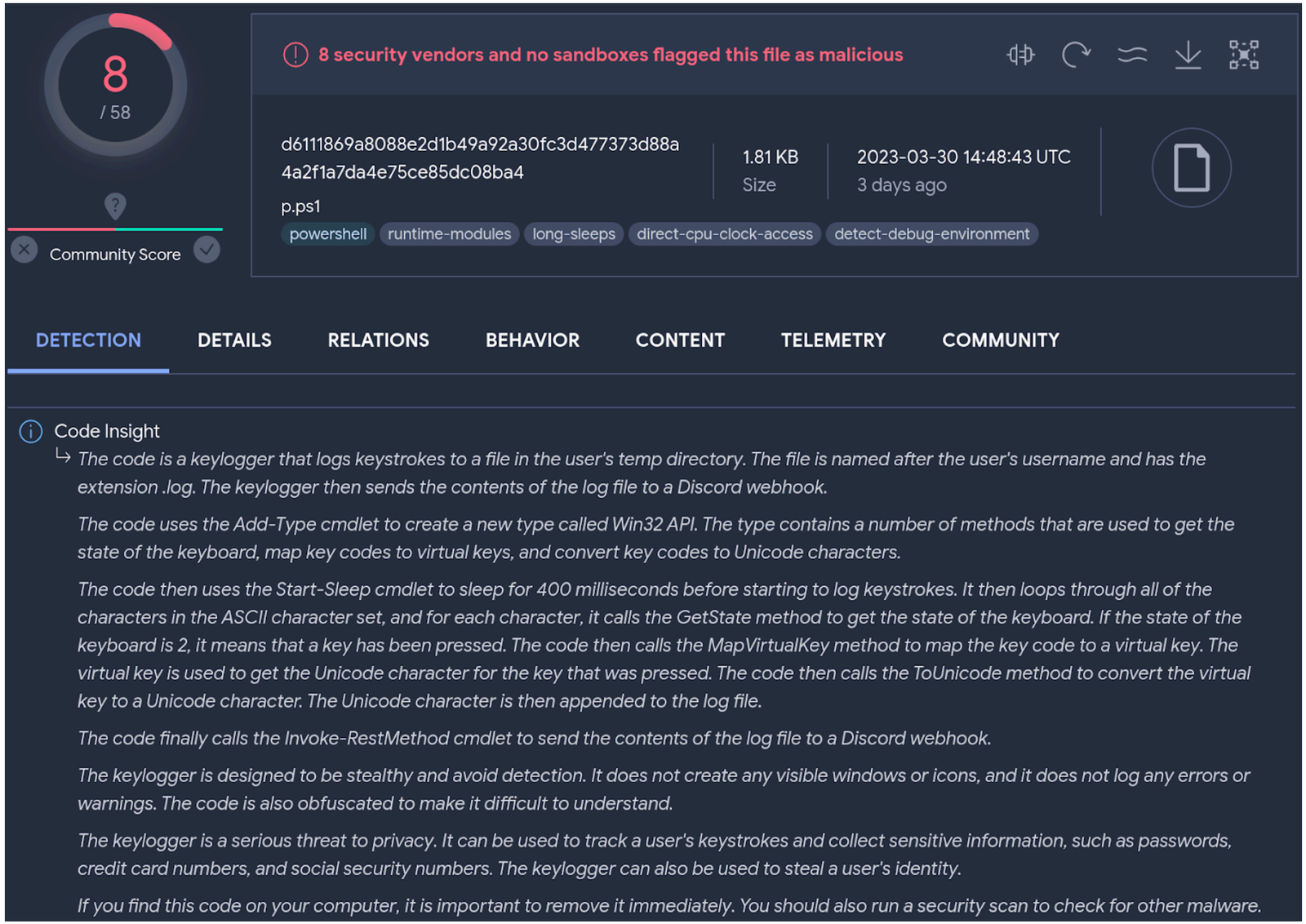
- **VirusTotal**: VirusTotal inspects items with over 70 antivirus scanners and URL/domain blocklisting services

- **ANY.RUN**: An interactive online sandbox for malware analysis. The service allows researchers to analyze malware behavior by running samples in a controlled environment



Turki Al-Juaid Instructor
cybersecurity

- **VirusTotal**


8
/ 58
Community Score
8 security vendors and no sandboxes flagged this file as malicious
d6111869a8088e2d1b49a92a30fc3d477373d88a
4a2f1a7da4e75ce85dc08ba4
p.ps1
1.81 KB
Size
2023-03-30 14:48:43 UTC
3 days ago
powershell
runtime-modules
long-sleeps
direct-cpu-clock-access
detect-debug-environment
DETECTION
DETAILS
RELATIONS
BEHAVIOR
CONTENT
TELEMETRY
COMMUNITY
Code Insight
The code is a keylogger that logs keystrokes to a file in the user's temp directory. The file is named after the user's username and has the extension .log. The keylogger then sends the contents of the log file to a Discord webhook.
The code uses the Add-Type cmdlet to create a new type called Win32 API. The type contains a number of methods that are used to get the state of the keyboard, map key codes to virtual keys, and convert key codes to Unicode characters.
The code then uses the Start-Sleep cmdlet to sleep for 400 milliseconds before starting to log keystrokes. It then loops through all of the characters in the ASCII character set, and for each character, it calls the GetState method to get the state of the keyboard. If the state of the keyboard is 2, it means that a key has been pressed. The code then calls the MapVirtualKey method to map the key code to a virtual key. The virtual key is used to get the Unicode character for the key that was pressed. The code then calls the ToUnicode method to convert the virtual key to a Unicode character. The Unicode character is then appended to the log file.
The code finally calls the Invoke-RestMethod cmdlet to send the contents of the log file to a Discord webhook.
The keylogger is designed to be stealthy and avoid detection. It does not create any visible windows or icons, and it does not log any errors or warnings. The code is also obfuscated to make it difficult to understand.
The keylogger is a serious threat to privacy. It can be used to track a user's keystrokes and collect sensitive information, such as passwords, credit card numbers, and social security numbers. The keylogger can also be used to steal a user's identity.
If you find this code on your computer, it is important to remove it immediately. You should also run a security scan to check for other malware.

- **ANY.RUN**

Turki Al-Juaid Instructor
cybersecurity

Turki Al-Juaid Instructor
cybersecurity

- **Security Incident Reporting**
- **Security Incident Reporting refers to the process of identifying, documenting, and communicating security incidents that may affect an organization's information systems, data integrity, or overall security posture**

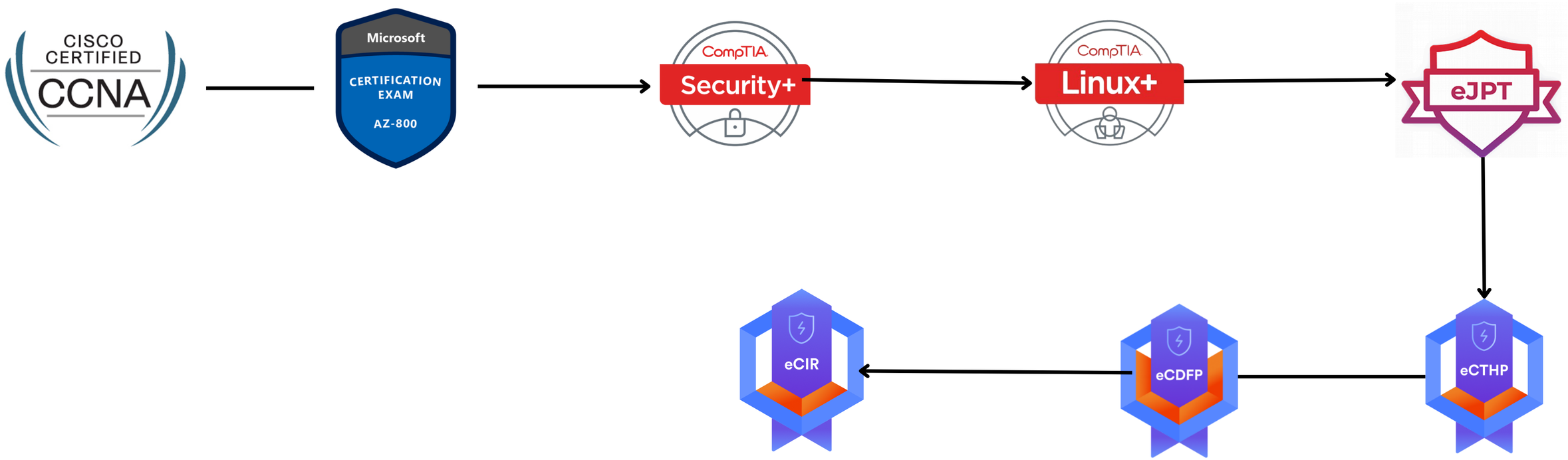
LAB - Security Incident Reporting

Turki Al-Juaid Instructor
cybersecurity

- **Scenario**

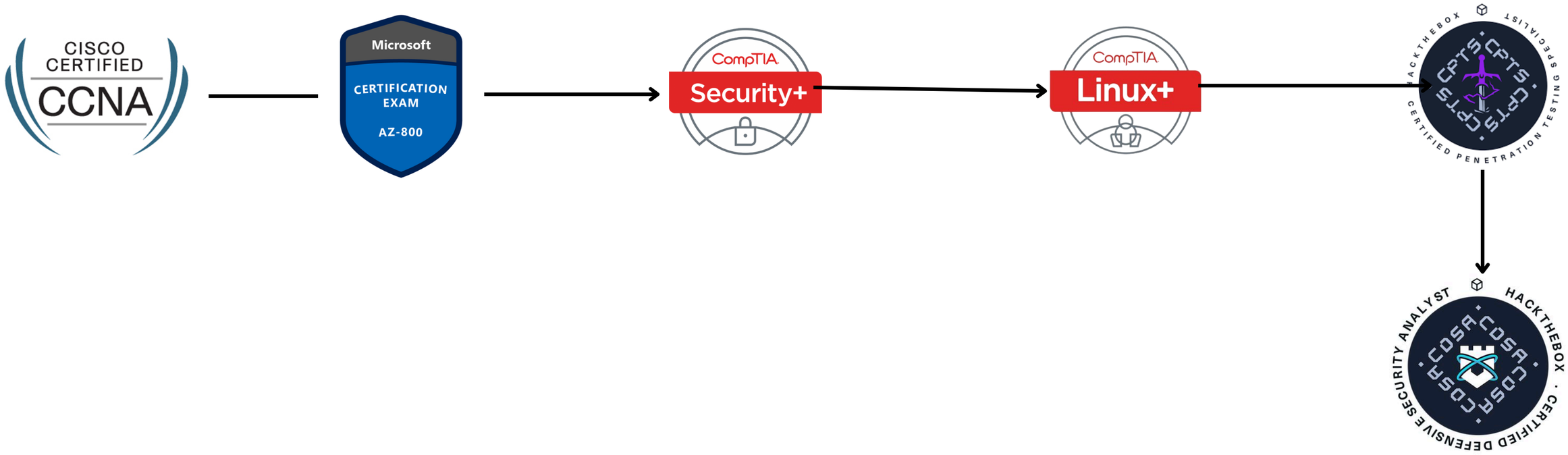
- **On Friday morning, while Abdullah was conducting his routine system review, he noticed unusual activity on one of the servers. Upon examining the logs, he discovered a significant number of login attempts originating from an unknown IP address. These attempts were increasing rapidly, raising his concerns.**
- **Despite the presence of some security measures, such as a firewall and intrusion detection system, the incident exposed vulnerabilities in the current security settings that could facilitate such attacks.**

- **Roadmap SOC - INE** CLICK HERE



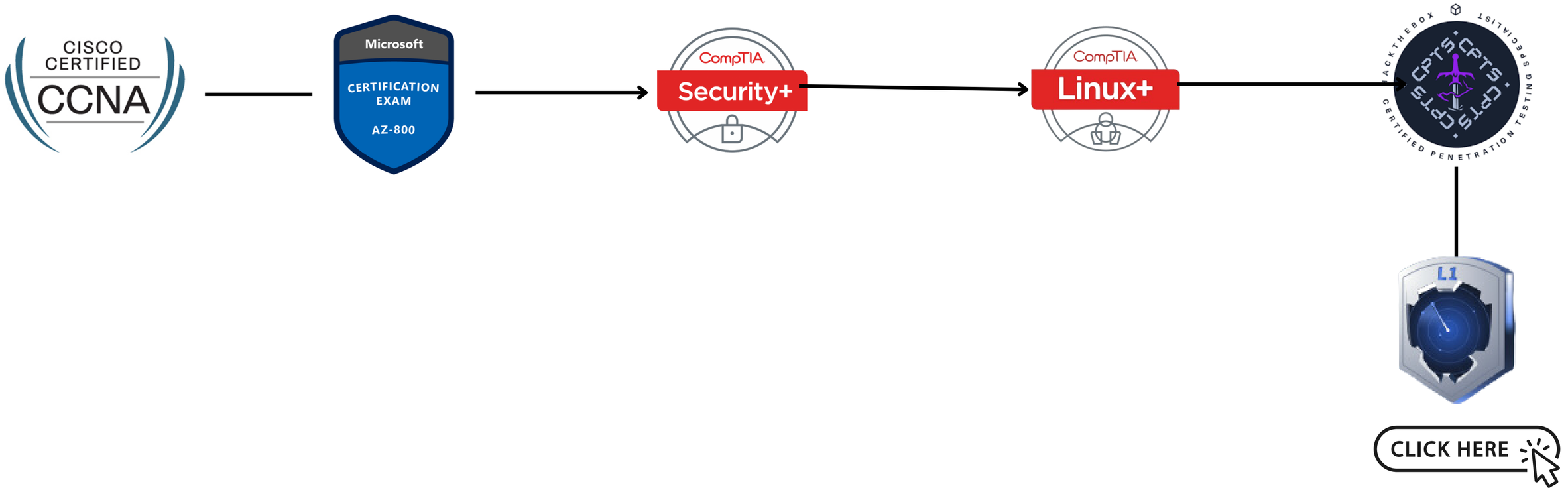
Turki Al-Juaid Instructor
cybersecurity

- **Roadmap SOC Hack the box** CLICK HERE



Turki Al-Juaid Instructor
cybersecurity

- **Roadmap SOC Tryhackme**



Turki Al-Juaid Instructor
cybersecurity

- **If you need help contact me**
- **Thank You**

Turki Al-Juaid Instructor
cybersecurity