Intrusion Detection and Incident Response

@ NFSU, 26 APRIL 2025

PRESENTED BY
-JALAJ BHASKAR

Who am I :

- Cybersecurity Enthusiast
- Various roles –
  - Security Operation Ceter Analyst (SOC)
  - Detection and Response Team
  - Security Engineer
  - Researching on Defensive AI

- Reach out to me at ..
  - Linkedin.com/in/teamblue

Today’s Agenda

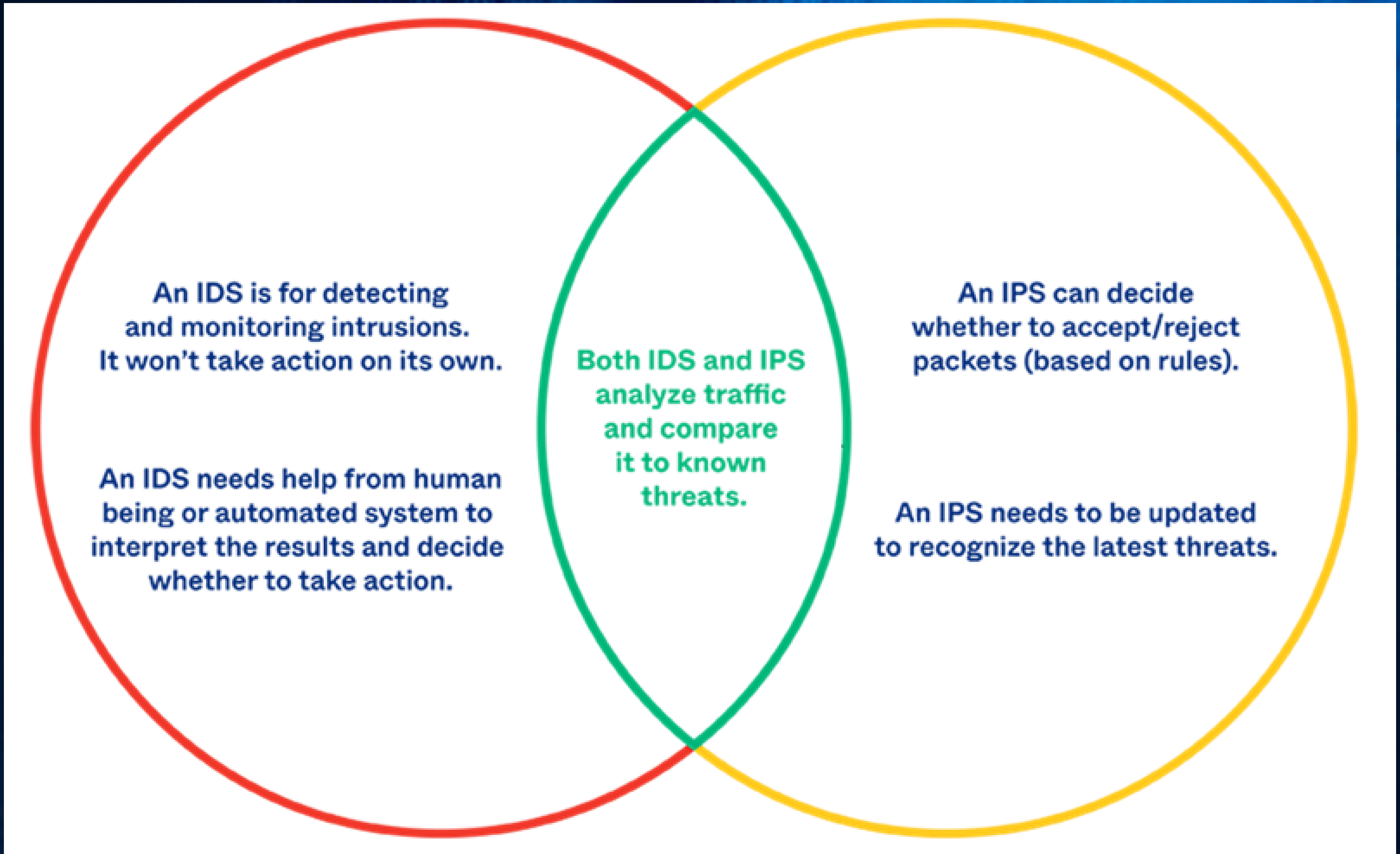
- Getting starting with detecting and responding to cyber intrusions
- Types of IDS
- Incident Response. What and Why ?
- Steps of Incident Response
- Live Demo: Simple Intrusion Detection System
- QnA

Intrusion Detection

Intrusion Detection is the process of monitoring systems or networks for unauthorized access or malicious activity

- Protects sensitive data (e.g., personal info, financial records).
- Prevents system damage or downtime

Intrusion Detection System vs Intrusion Prevention System



An IDS is for detecting and monitoring intrusions. It won't take action on its own.

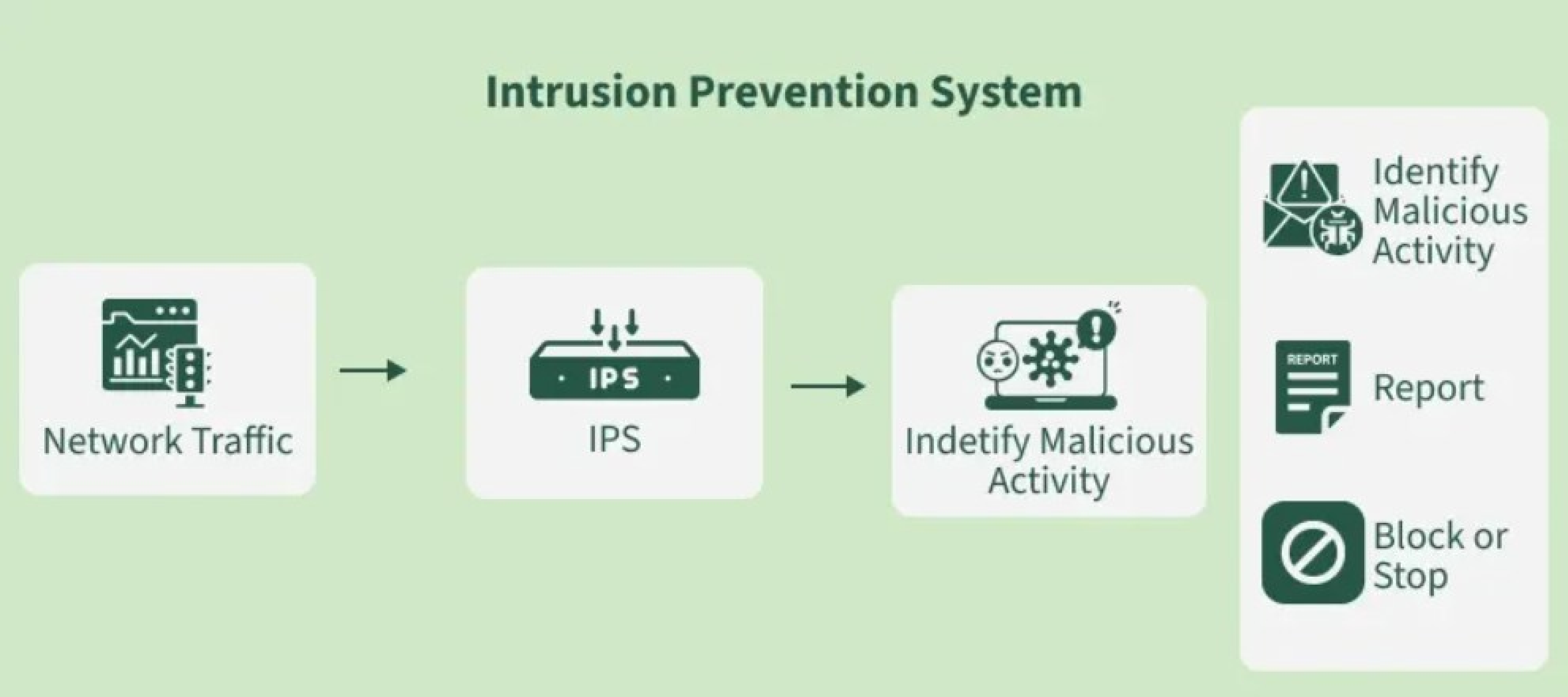
An IDS needs help from human being or automated system to interpret the results and decide whether to take action.

Both IDS and IPS analyze traffic and compare it to known threats.

An IPS can decide whether to accept/reject packets (based on rules).

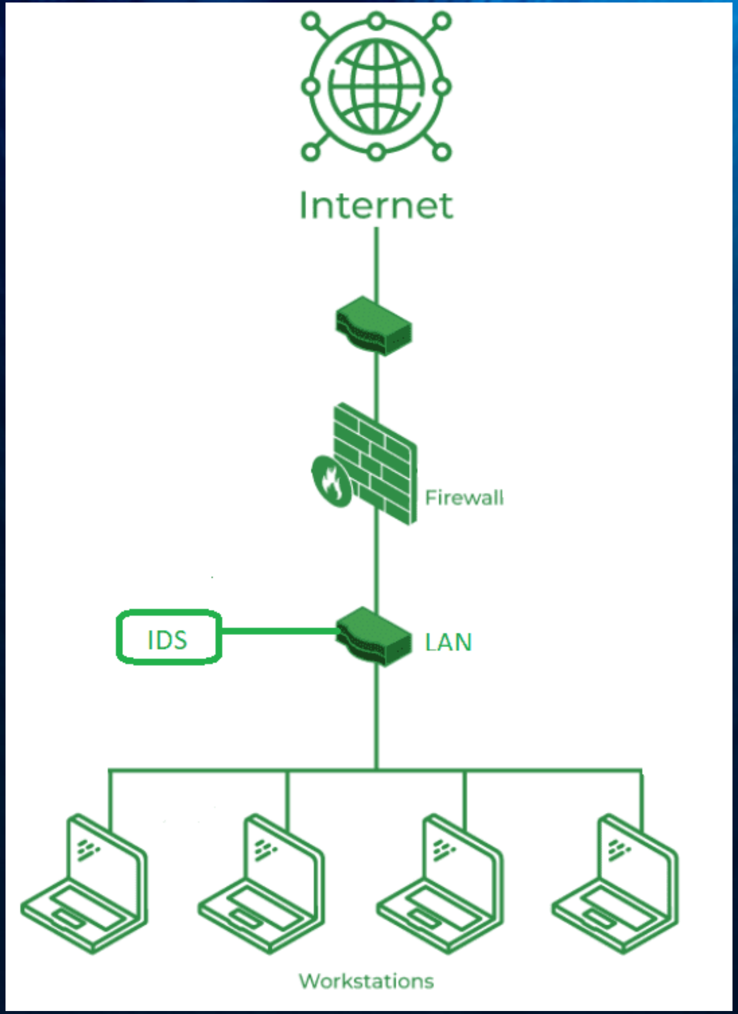
An IPS needs to be updated to recognize the latest threats.

Intrusion Detection System vs Intrusion Prevention System


Intrusion Prevention System
Network Traffic
IPS
IPS
Indetify Malicious Activity
Identify Malicious Activity
REPORT
Report
Block or Stop

Inline Deployment

Intrusion Detection System vs Intrusion Prevention System



'behind-the-firewall' placement

Types of Intrusion Detection System

1. Network-Based IDS (NIDS)

Monitors network traffic for suspicious patterns.
Example: Snort, Suricata.
Use case: Detecting malware spreading across a network.

2. Host-Based IDS (HIDS)

Monitors individual devices for unusual activity.
Example: OSSEC, Tripwire.
Use case: Detecting unauthorized changes to system files.

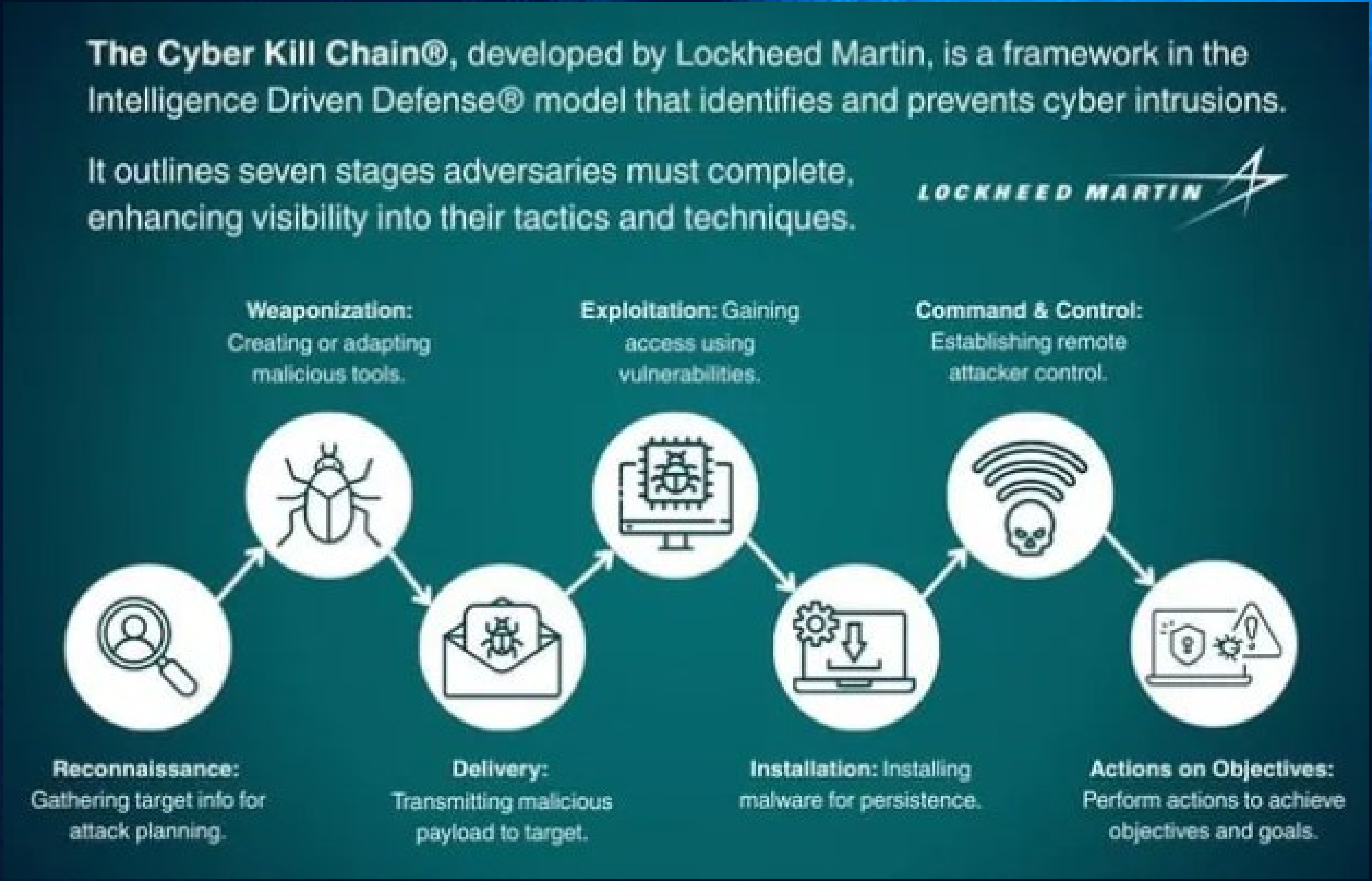
3. Signature-Based vs. Anomaly-Based

Signature: Matches known attack patterns (e.g., virus definitions).
Anomaly: Detects deviations from normal behavior (e.g., unusual login times).

What is Incident Response

A structured approach to identifying, responding to, and recovering from cybersecurity incidents.

- Key Goals
  - Minimize damage (e.g., data loss, downtime)
  - Restore normal operations quickly.
  - Learn to prevent future incidents



The Cyber Kill Chain®, developed by Lockheed Martin, is a framework in the Intelligence Driven Defense® model that identifies and prevents cyber intrusions.

It outlines seven stages adversaries must complete, enhancing visibility into their tactics and techniques.

LOCKHEED MARTIN

Reconnaissance: Gathering target info for attack planning.

Weaponization: Creating or adapting malicious tools.

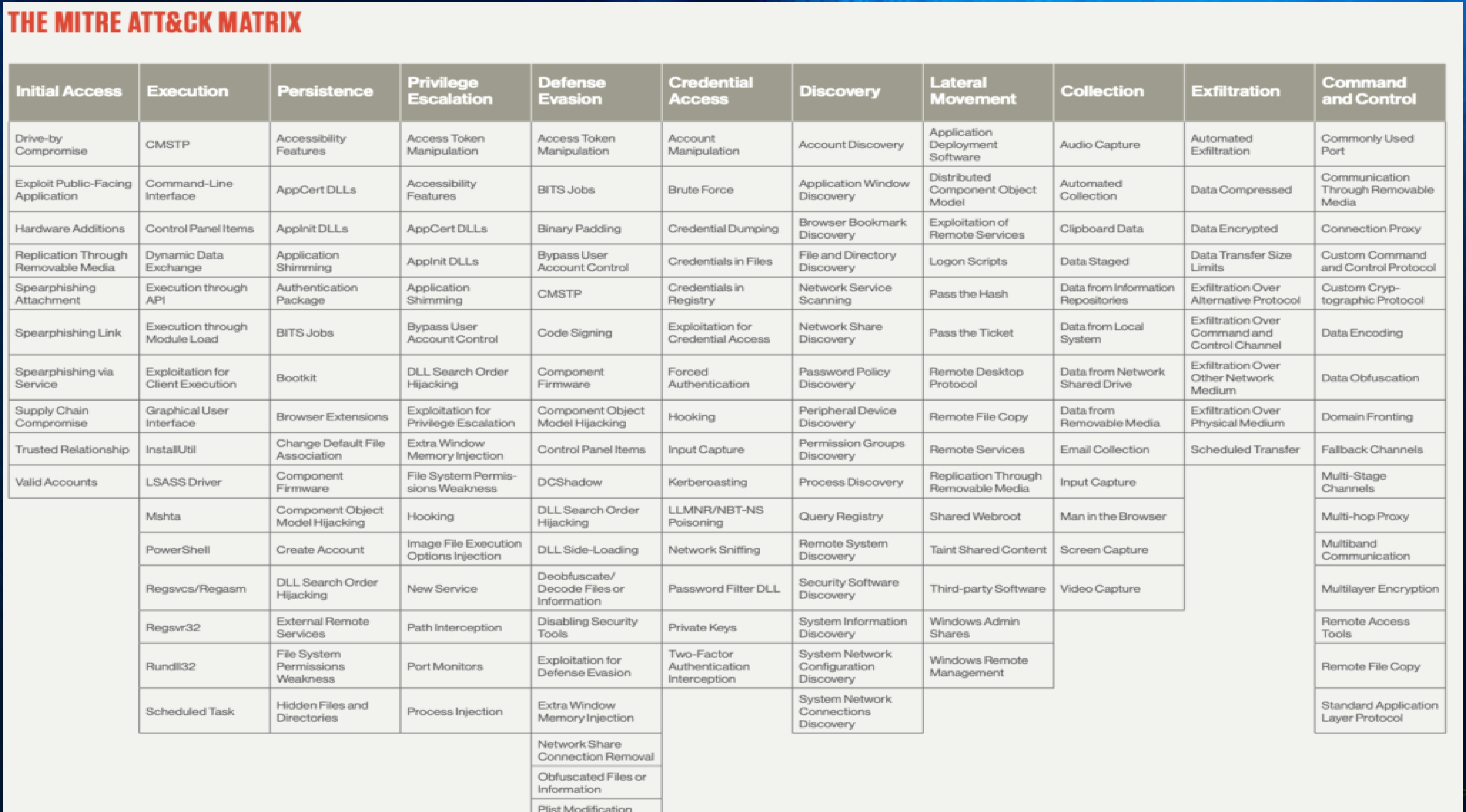
Delivery: Transmitting malicious payload to target.

Exploitation: Gaining access using vulnerabilities.

Installation: Installing malware for persistence.

Command & Control: Establishing remote attacker control.

Actions on Objectives: Perform actions to achieve objectives and goals.



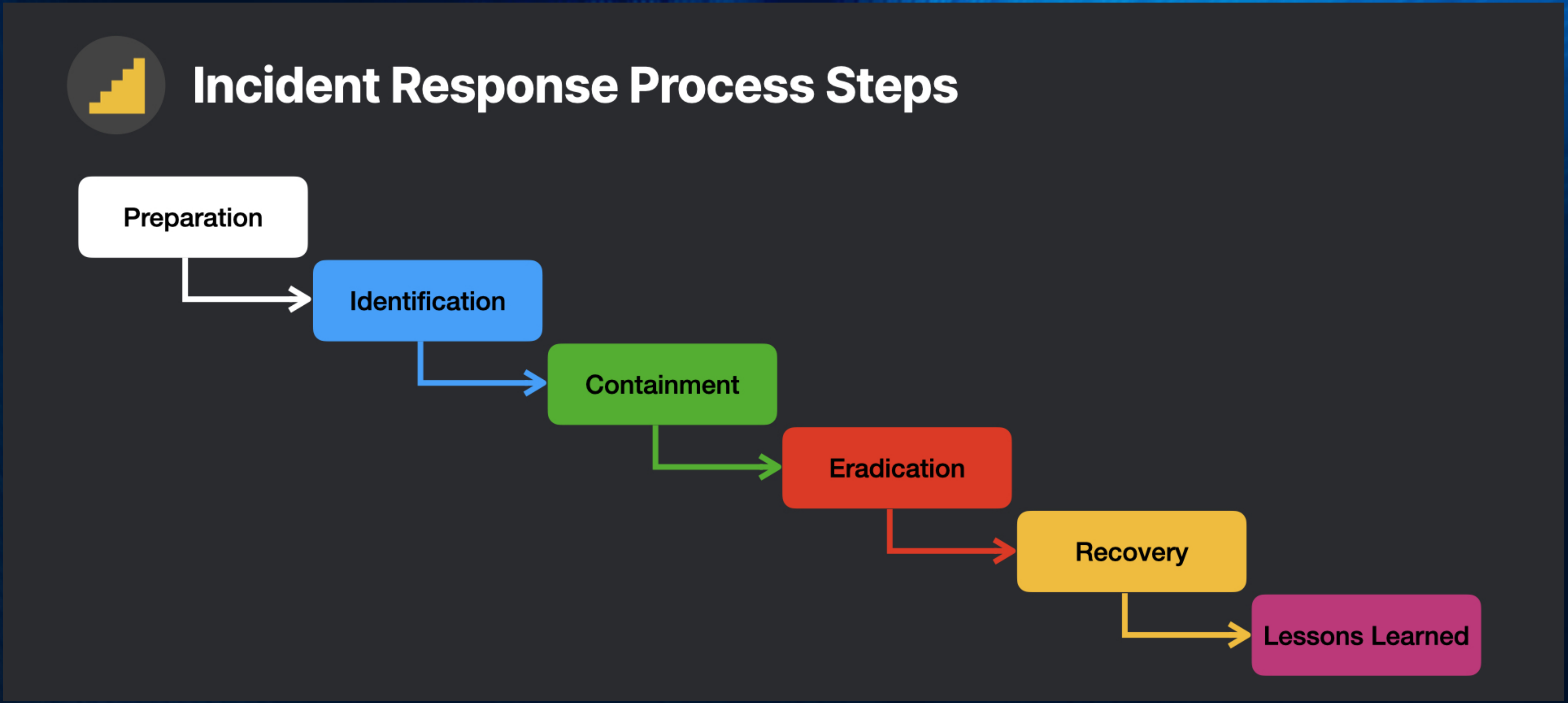
THE MITRE ATT&CK MATRIX

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Drive-by Compromise	CMSTP	Accessibility Features	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	Application Deployment Software	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	Command-Line Interface	AppCert DLLs	Accessibility Features	BITS Jobs	Brute Force	Application Window Discovery	Distributed Component Object Model	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Control Panel Items	AppInit DLLs	AppCert DLLs	Binary Padding	Credential Dumping	Browser Bookmark Discovery	Exploitation of Remote Services	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Dynamic Data Exchange	Application Shimming	AppInit DLLs	Bypass User Account Control	Credentials in Files	File and Directory Discovery	Logon Scripts	Data Staged	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Attachment	Execution through API	Authentication Package	Application Shimming	CMSTP	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Information Repositories	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Execution through Module Load	BITS Jobs	Bypass User Account Control	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Local System	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing via Service	Exploitation for Client Execution	Bootkit	DLL Search Order Hijacking	Component Firmware	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Data from Network Shared Drive	Exfiltration Over Other Network Medium	Data Obfuscation
Supply Chain Compromise	Graphical User Interface	Browser Extensions	Exploitation for Privilege Escalation	Component Object Model Hijacking	Hooking	Peripheral Device Discovery	Remote File Copy	Data from Removable Media	Exfiltration Over Physical Medium	Domain Fronting
Trusted Relationship	InstallUtil	Change Default File Association	Extra Window Memory Injection	Control Panel Items	Input Capture	Permission Groups Discovery	Remote Services	Email Collection	Scheduled Transfer	Fallback Channels
Valid Accounts	LSASS Driver	Component Firmware	File System Permissions Weakness	DCShadow	Kerberoasting	Process Discovery	Replication Through Removable Media	Input Capture		Multi-Stage Channels
	Mshta	Component Object Model Hijacking	Hooking	DLL Search Order Hijacking	LLMNR/NBT-NS Poisoning	Query Registry	Shared Webroot	Man in the Browser		Multi-hop Proxy
	PowerShell	Create Account	Image File Execution Options Injection	DLL Side-Loading	Network Sniffing	Remote System Discovery	Taint Shared Content	Screen Capture		Multiband Communication
	Regsvcs/Regasm	DLL Search Order Hijacking	New Service	Deobfuscate/Decode Files or Information	Password Filter DLL	Security Software Discovery	Third-party Software	Video Capture		Multilayer Encryption
	Regsvr32	External Remote Services	Path Interception	Disabling Security Tools	Private Keys	System Information Discovery	Windows Admin Shares			Remote Access Tools
	Rundll32	File System Permissions Weakness	Port Monitors	Exploitation for Defense Evasion	Two-Factor Authentication Interception	System Network Configuration Discovery	Windows Remote Management			Remote File Copy
	Scheduled Task	Hidden Files and Directories	Process Injection	Extra Window Memory Injection		System Network Connections Discovery				Standard Application Layer Protocol
				Network Share Connection Removal						
				Obfuscated Files or Information						
				Plist Modification						

Incident Response Process

1. **Preparation**:
   Create an incident response plan.
   Train staff and set up tools (e.g., IDS, backups).
2. **Identification**:
   Detect the incident (e.g., IDS alert, user report).
   Determine scope and impact.
3. **Containment**:
   Short-term: Isolate affected systems (e.g., disconnect from network).
   Long-term: Apply patches or reconfigure systems.
4. **Eradication**:
   Remove malware, close vulnerabilities.
   Example: Delete malicious files, update software.
5. **Recovery**:
   Restore systems and verify they’re secure.
   Example: Restore from clean backups.
6. **Lessons Learned**:
   Document the incident and improve defenses.
   Example: Update firewall rules after an attack.

Incident Response Process



Incident Response Process Steps

Preparation

Identification

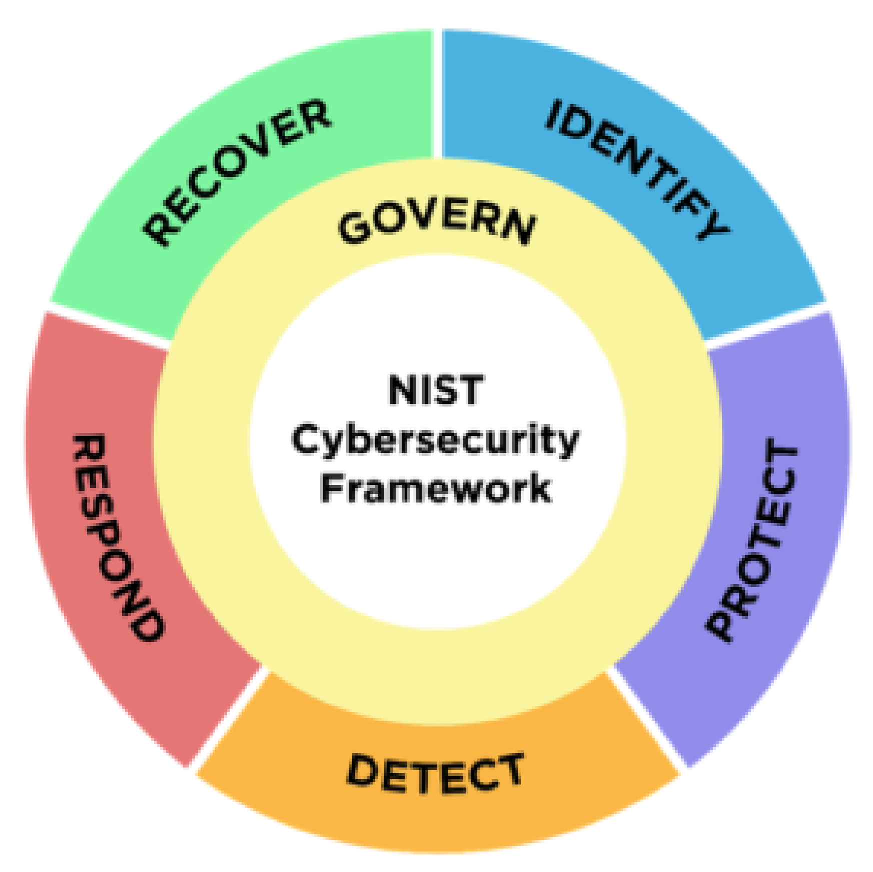
Containment

Eradication

Recovery

Lessons Learned

The NIST Cybersecurity Framework (CSF) is a set of voluntary guidelines designed to help organizations assess and improve their ability to prevent, detect, and respond to cybersecurity risks



Challenges in Intrusion Detection and Incident Response

- Challenges -
  - False positives: IDS flagging normal activity as malicious.
  - Evolving threats: New attack methods (e.g., zero-day exploits).
  - Resource constraints: Limited staff or tools.
- Solutions –
  - Fine-tune IDS to reduce false positives.
  - Stay updated with threat intelligence.
  - Automate repetitive tasks (e.g., log analysis).

DEMO

Free Tools and Resources–

- NIST
- IDS vs IPS by Palo Alto
- MITRE ATT&CK
- Lockheed martin Kill Chain
- Incident management lifecycle
- Malware PCAP analysis
- Zeek , Snort and Surricata

Have any questions ? Reach out …

- Get your files here …

Mob – 8851458452

LinkedIn – Linkedin.com/in/teamblue