



# **Introduction to Security Operation Centre (SOC)**

Presenter – Jalaj  
@ NFSU, Delhi Campus  
18<sup>th</sup> November'24

# \$ whoami

- Proud Blurple Teamer
- Cloud Security
- SOC Analyst at Birlasoft
- Got questions ?
  - [Linkedin.com/in/teamblue](https://www.linkedin.com/in/teamblue)
  - Telegram - @senditfast



# What will you learn in this presentation ?

- Overview of SOC structure
- Skills required
- Discussion on real world scenarios
- Role-play : Incident Responder



# Relevant Certifications ?

- Experience in IT
- Good to have : Sec+ or equivalent
- Just passion for catching “Bad Guys”

# Security Operations Centre

- 24x7 Operations
- Incident Response
- Types : In-House SOC/Outsourced SOC/Hybrid SOC
- Detection, automation, threat hunt, threat intelligence
- Challenges : High volume alerts , Shortage of skilled professional

# Why SOC ??

- Monitor

- Prevent

- Investigate

- Detect

- Respond

- Compliance and Reporting



# People

01

- Tier 1 SOC Analyst (Triage)

03

- Tier 2 SOC Analyst (Threat Hunters)

02

- Tier 2 SOC Analyst (Incident response)

04

- SOC Manager

# Process









# Tools




- SIEM (Security Information and Event Management)
  - EDR (Endpoint Detection and Response)
  - XDR (Extended Detection and Response)
  - IDS (Intrusion Detection System)
  - IPS (Intrusion Prevention System)
  - UEBA (User and Entity Behavior Analytics)
  - DLP (Data Loss Prevention)
  - NGFW (Next-Generation Firewall)
  - SASE (Secure Access Service Edge)
  - WAF (Web Application Firewall)
  - CASB (Cloud Access Security Broker)
  - FIM (File Integrity Monitoring)
- 
- 




# SIEM



- Security Information and event management
  - **Collecting, normalizing, and correlating data** from various systems and devices.
  - Dashboards and Reporting
  - Incident Detection and Response
  - Threat Intelligence Integration
  - Compliance Management
  - Ex : Splunk, Microsoft Sentinel, IBM Qradar, LogRhythm, etc.
- 



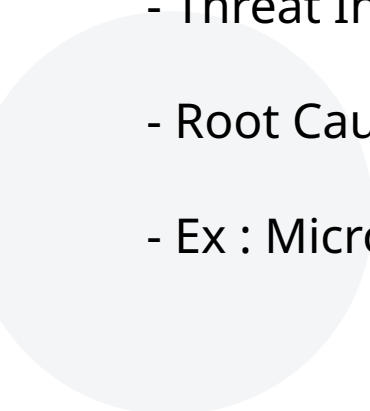

# SOAR

- Orchestration enables all tools to work together, share data, and trigger actions based on predefined rules
  - **Automation of Repetitive Tasks**
  - **Incident Response Playbooks**
  - Real-Time Alerts and Notifications
  - Ex: Microsoft LogicApps, Palo Alto Cortex XSOAR, Splunk SOAR
- 



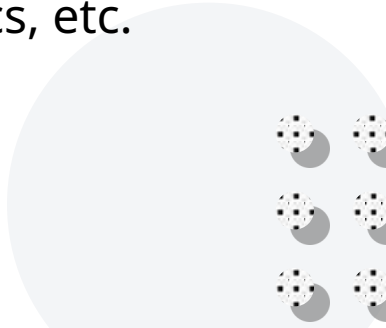
# XDR



- Extended Detection and Response
  - **Behavioural Analytics**
  - **Cloud and Hybrid Environment Coverage**
  - Threat Intelligence Integration
  - Root Cause Analysis
  - Ex : Microsoft Defender, Crowdstrike Falcon, Palo Alto Cortex, SentinelOne, etc.
- 
- 



# UEBA

- User and Entity Behaviour Analytics
  - UEBA helps detect unusual behaviour by users
  - User and Entity Profiling
  - **Insider Threat Detection**
  - **Risk Scoring**
  - Ex : Microsoft UEBA, LogRhythm UEBA, Splunk User Behavior Analytics, etc.
- 

# Threat Intelligence

- Gather threat information from multiple sources (e.g., logs, dark web)
- Analyze patterns, tactics, and techniques to understand threats
- Indicators of Compromise (IOCs), relevant to industry
- Use intelligence to anticipate and prevent cyber threats

# Threat Hunting

- Proactively seek hidden threats
- Data Analysis: Examine logs, traffic, and endpoints for anomalies
- Hypothesis-Driven: Use specific assumptions to guide searches for threats
- Detection: Find threats that bypass automated defenses like firewalls or antivirus

# Normalized Log

```
2024-11-17 08:35:42 | WAF_ALERT | SrcIP=192.168.1.100 | DstIP=93.184.216.34 | SrcPort=12345 |  
DstPort=80 | Method=POST | URI=/login.php | Status=Blocked | Rule=SQLInjectionRule |  
Message=SQL Injection Attempt Detected | Data=<script>alert('hack');</script>
```

```
Timestamp: 2024-11-17 08:35:42  
Source IP: 192.168.1.100  
Destination IP: 93.184.216.34  
Method: POST  
URI: /login.php  
Action: Blocked  
Rule: SQLInjectionRule  
Threat: SQL Injection  
Payload: <script>alert('hack');</script>
```



# Normalized Log

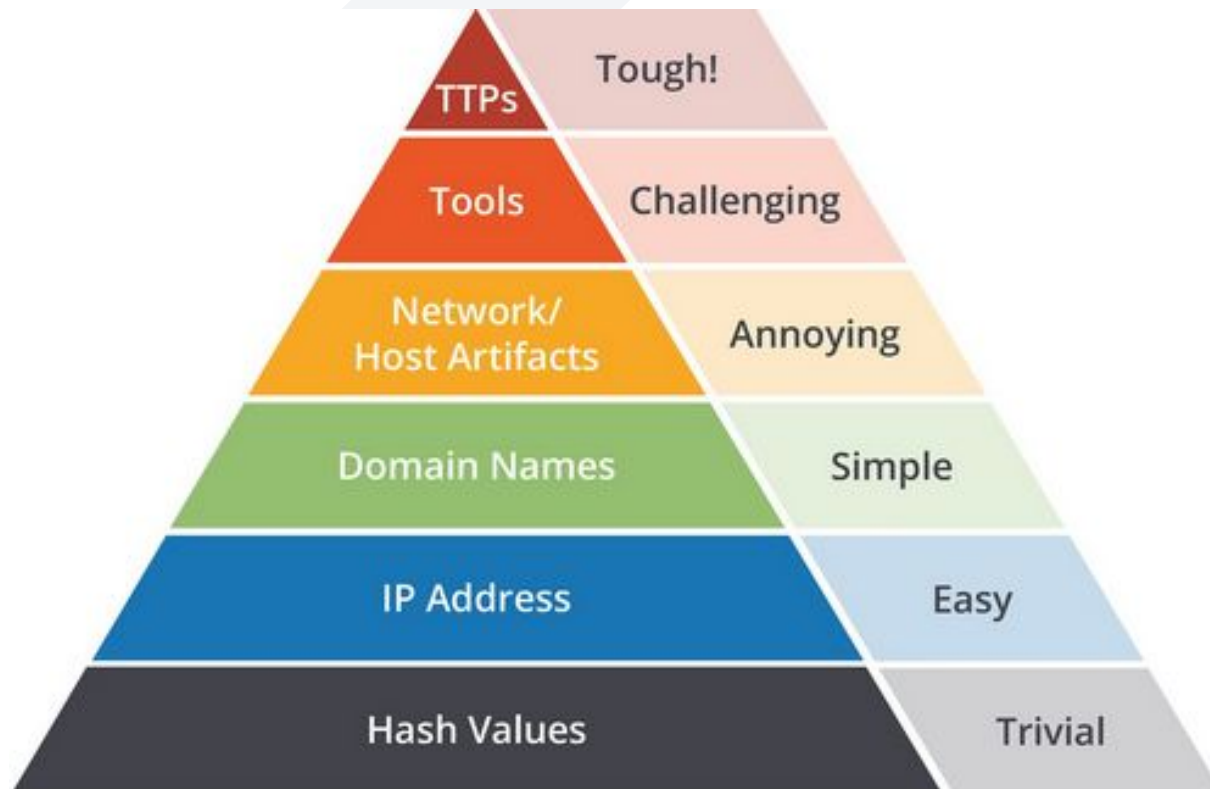
2024-11-17 09:12:45 | Event ID=4624 | User=admin | Source IP=192.168.1.10 | Process=explorer.exe | Action=Logon | Domain=corp.local | Logon Type=RemoteInteractive | Logon GUID={12345678-1234-1234-1234-123456789012} | Target User=admin | Target Domain=corp.local | Source Port=3389 | Destination Port=443

```
{
  "timestamp": "2024-11-17 09:12:45",
  "event_type": "Logon",
  "user": "admin",
  "source_ip": "192.168.1.10",
  "process_name": "explorer.exe",
  "action": "Logon",
  "logon_type": "RemoteInteractive",
  "source_port": "3389",
  "destination_port": "443",
  "event_id": "4624",
  "target_user": "admin",
  "target_domain": "corp.local",
  "threat_level": "low",
  "risk_score": 10,
  "description": "User admin logged in via RDP to a remote machine"
}
```

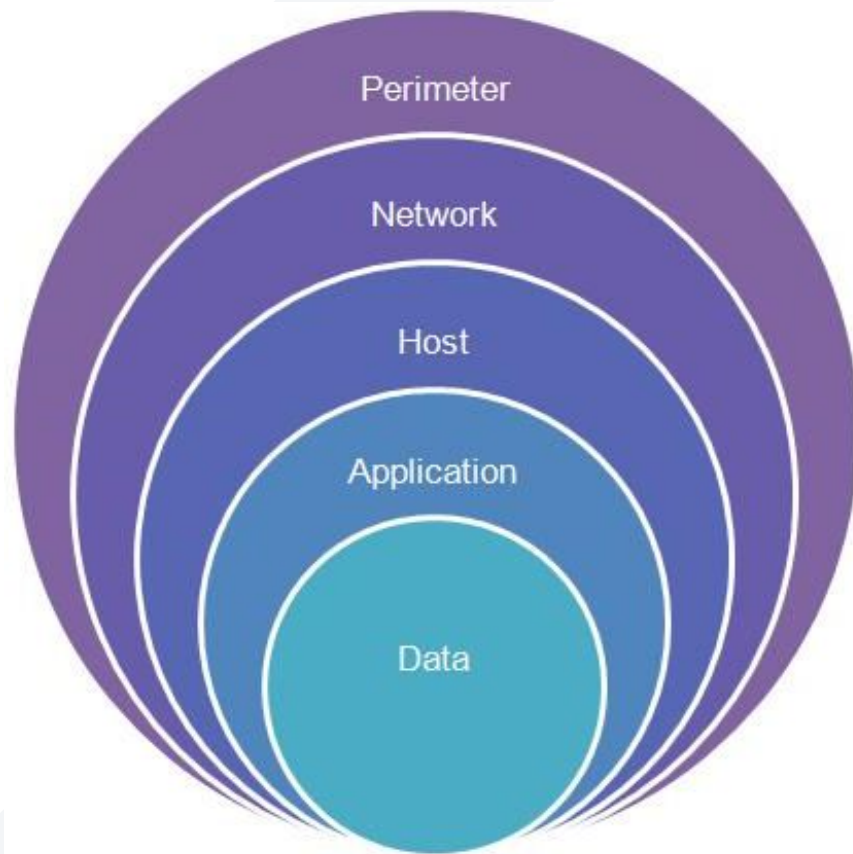
# Windows event ID

- Event ID 4624 – Successful Logon
- Event ID 4625 – Failed Logon Attempt
- Event ID 4672 – Special Privileges Assigned to New Logon
- Event ID 4740 – Account Lockout
- Event ID 4769 – Kerberos Service Ticket Request
- Event ID 4771 – Kerberos Pre-Authentication Failed
- Event ID 4688 – New Process Created
- Event ID 4663 – Access to an Object
- Event ID 1102 – Audit Log Cleared
- Event ID 4720 – User Account Created

# Pyramid of pain



# Defence in depth



# MITRE ATTACK

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command And Control
10 Items	31 Items	56 Items	28 Items	59 Items	20 Items	19 Items	17 Items	13 Items	9 Items	21 Items
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Command-Line Interface	AppCert DLLs	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Control Panel Items	Appinit DLLs	Appinit DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery	Exploitation of Remote Services	Data from Information Repositories	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Application Shimming	Clear Command History	Credentials in Files	Credentials in Registry	Logon Scripts	Data from Local System	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Execution through API	Authentication Package	Bypass User Account Control	Code Signing	Exploitation for Credential Access	Network Service Scanning	Pass the Hash	Data from Network Shared Drive	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing via Service	Execution through Module Load	Bootkit	DLL Search Order Hijacking	Component Firmware	Forced Authentication	Network Share Discovery	Pass the Ticket	Data from Removable Media	Exfiltration Over Other Network Medium	Data Obfuscation
Supply Chain Compromise	Graphical User Interface	Change Default File Association	Dylib Hijacking	Component Object Model Hijacking	Hooking	Password Policy Discovery	Remote Desktop Protocol	Data Staged	Exfiltration Over Physical Medium	Domain Fronting
Trusted Relationship	InstallUtil	Component Firmware	Exploitation for Privilege Escalation	Control Panel Items	Input Capture	Peripheral Device Discovery	Remote File Copy	Email Collection	Scheduled Transfer	Fallback Channels
Valid Accounts	Launchctl	Component Object Model Hijacking	Extra Window Memory Injection	DCShadow	Input Prompt	Permission Groups Discovery	Remote Services	Input Capture		Multi-hop Proxy
	LSASS Driver	Create Account	File System Permissions Weakness	Deobfuscate/Decode Files or Information	Kerberoasting	Process Discovery	Replication Through Removable Media	Screen Capture		Multi-Stage Channels
	Mshst	DLL Search Order Hijacking	Hooking	Disabling Security Tools	Keychain	Query Registry	Shared Webroot	Video Capture		Multiband Communication
	PowerShell	Dylib Hijacking	Image File Execution Options Injection	DLL Search Order Hijacking	Network Sniffing	Remote System Discovery	SSH Hijacking			Multilayer Encryption
	Regsvcs/Regasm	External Remote Services	Launch Daemon	DLL Side-Loading	Password Filter DLL	Security Software Discovery	Taint Shared Content			Port Knocking
	Regsvr32	File System Permissions Weakness	New Service	Exploitation for Defense Evasion	Private Keys	System Information Discovery	Third-party Software			Remote Access Tools
	Rundll32	Hidden Files and Directories	Path Interception	Extra Window Memory Injection	Replication Through Removable Media	System Network Configuration Discovery	Windows Admin Shares			Remote File Copy
	Scheduled Task	Hooking	Plist Modification	File Deletion	Securityd Memory	System Network Connections Discovery	Windows Remote Management			Standard Application Layer Protocol
	Scripting	Hypervisor	Port Monitors	File System Logical Offsets	Two-Factor Authentication Interception	System Owner/User Discovery				Standard Cryptographic Protocol
	Service Execution	Image File Execution Options Injection	Process Injection	Gatekeeper Bypass		System Service Discovery				Standard Non-Application Layer Protocol
	Signed Binary Proxy Execution	Kernel Modules and Extensions	Scheduled Task	Hidden Files and Directories						Uncommonly Used Port
	Signed Script Proxy Execution	Launch Agent	Service Registry Permissions Weakness	Hidden Users						Web Service
	Source		Setuid and Setgid	Hidden Window						
	Space after Filename			HISTCONTROL						
				Image File Execution Options Injection						

# MITRE ENGAGE

Prepare	Expose		Affect			Elicit		Understand
Plan	Collect	Detect	Prevent	Direct	Disrupt	Reassure	Motivate	Analyze
Cyber Threat Intelligence	API Monitoring	Introduced Vulnerabilities	Baseline	Attack Vector Migration	Isolation	Application Diversity	Application Diversity	After-Action Review
Engagement Environment	Network Monitoring	Lures	Hardware Manipulation	Email Manipulation	Lures	Artifact Diversity	Artifact Diversity	Cyber Threat Intelligence
Gating Criteria	Software Manipulation	Malware Detonation	Isolation	Introduced Vulnerabilities	Network Manipulation	Burn-In	Information Manipulation	Threat Model
Operational Objective	System Activity Monitoring	Network Analysis	Network Manipulation	Lures	Software Manipulation	Email Manipulation	Introduced Vulnerabilities	
Persona Creation			Security Controls	Malware Detonation		Information Manipulation	Malware Detonation	
Storyboarding			Network Manipulation	Network Diversity		Network Diversity		
Threat Model			Peripheral Management	Peripheral Management		Personas		
			Security Controls	Pocket Litter				
				Software Manipulation				



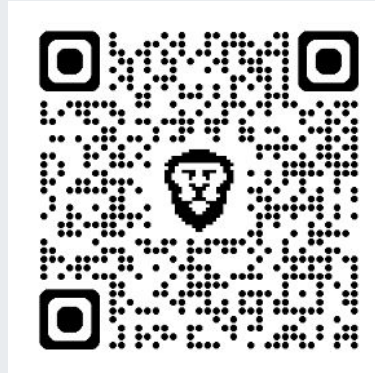
# **Recent Incidents Discussion**

## **Prevention and Detection**



# Any Questions ?

// Continue the conversation on  
LinkedIn ...



//



# Hands-on exercise

