DAY 4

SECURITY USE CASES

PRESENTED BY: ADITYA JAMKHANDE

WHAT IS A SECURITY USECASE

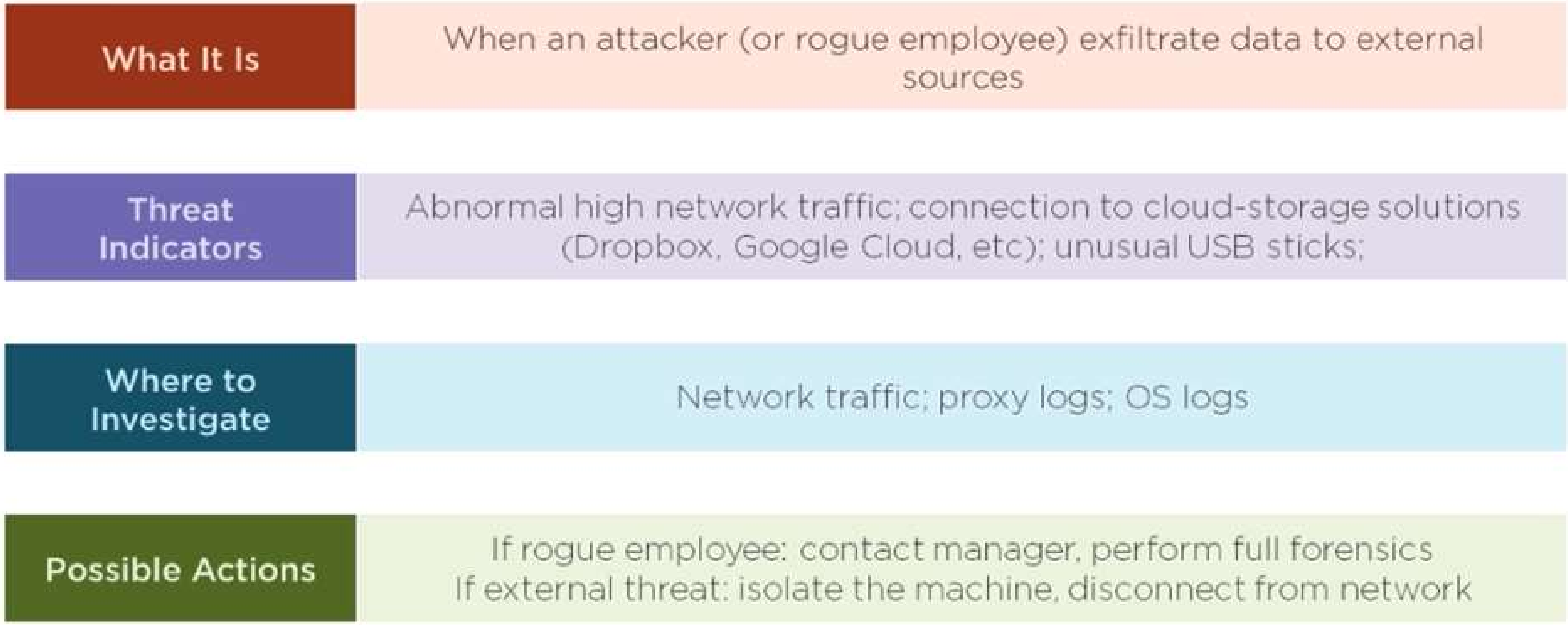
- A use case – sometimes referred to as an attack scenario – represents the outcome of an attack, or the attacker's desired outcome state vis-à-vis a specific asset (or set of assets). This outcome should map to the MITRE ATT&CK Matrix Impact category

- Handling such a scenario effectively in a way that mitigates risks and minimizes damage to an organization involves several kinds of preparatory work – including:
  - Collecting the right security data to perform security analytics
  - Enriching security alerts for better contextualization
  - Creating alerts, dashboards & reports for real-time visibility
  - Orchestrating security monitoring & incident response technologies

SECURITY DEVICES/TECHNOLOGIES

- Firewall
- Proxy / Forward proxy
- WAF (Web application firewall) – application level logs
- Antivirus
- EDR
- Authentication devices (AAA)
- PAM
- IDS / IPS
- Sandboxes
- DLP
- CASB
- Email gateway appliances
- IOT
- Cloud endpoints
- OS logs

DATA EXFILTRATION



What It Is	When an attacker (or rogue employee) exfiltrate data to external sources
Threat Indicators	Abnormal high network traffic; connection to cloud-storage solutions (Dropbox, Google Cloud, etc); unusual USB sticks;
Where to Investigate	Network traffic; proxy logs; OS logs
Possible Actions	If rogue employee: contact manager, perform full forensics If external threat: isolate the machine, disconnect from network

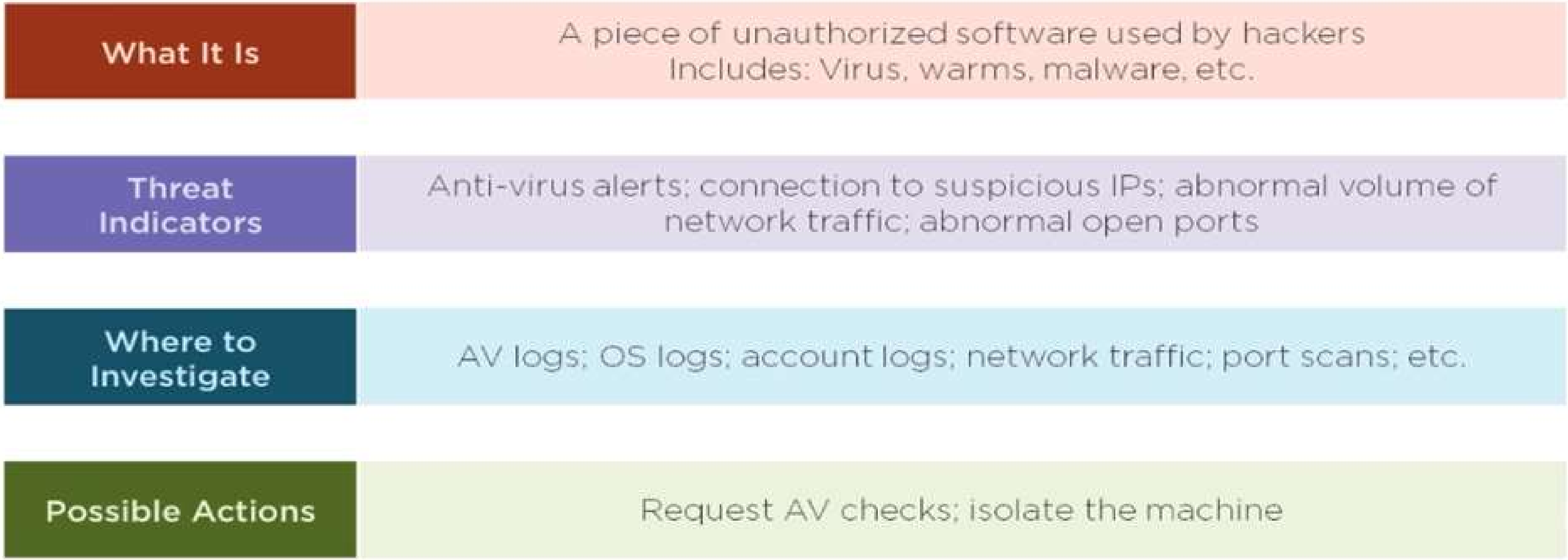
USE CASE SCENARIO: IDENTIFY DATA EXFILTRATION (PROXY)

Rule Name	**Potential data ex-filtration attempt through proxy**
Description	When attacker / insider tries to exfiltrate the data and the attempt is identified via the proxy logs
Threat Indicator	Abnormal traffic - This rule detects if there is an attempt of one GB transfer of the data in a single HTTP request using proxy
Data Source to be investigated	This rule is specifically applicable to proxy data sources like Symantec bluecoat, cisco IronPort, etc.
Possible Pro-active Actions	Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary can be used to mitigate activity at the network level.
Possible reactive Actions	Terminate the user session and contact the manager
Tips & Tricks for Security Analyst	• Check the source and destination IP associated with this activity • Check if the source is infected with a malware • Identify the user name / AD user name • Contact the user via mail/phone or inform his manager using the organization chart • Escalate to L2 / CIRT for further investigation if analysts feel severity is high/insufficient information

USE CASE SCENARIO: IDENTIFY DATA EXFILTRATION (EMAIL)

Rule Name	**Potential data ex-filtration attempt through email**
Description	This rule detects if there is a transfer of more than15 MB data in a mail through an attachment
Threat Indicator	Abnormal traffic - The leak of sensitive data that might lead the cyber attack/incident in the future or violation of policy/compliance
Data Source to be investigated	This rule is specifically applicable to Email gateway appliance
Possible Pro-active Actions	Use email security systems like the Microsoft Defender for Office 365 to limit the transfer outside organization
Possible reactive Actions	Block the email at the gateway and contact the manager
Tips & Tricks for Security Analyst	• Check the Sender email address & Check associated user with email • Check recipient email address • Check the attachment contents and file • Contact the user via mail/phone or inform his manager using the organization chart • Escalate to L2 / CIRT for further investigation is analysts feel severity is high/insufficient information

MALWARE IDENTIFICATION

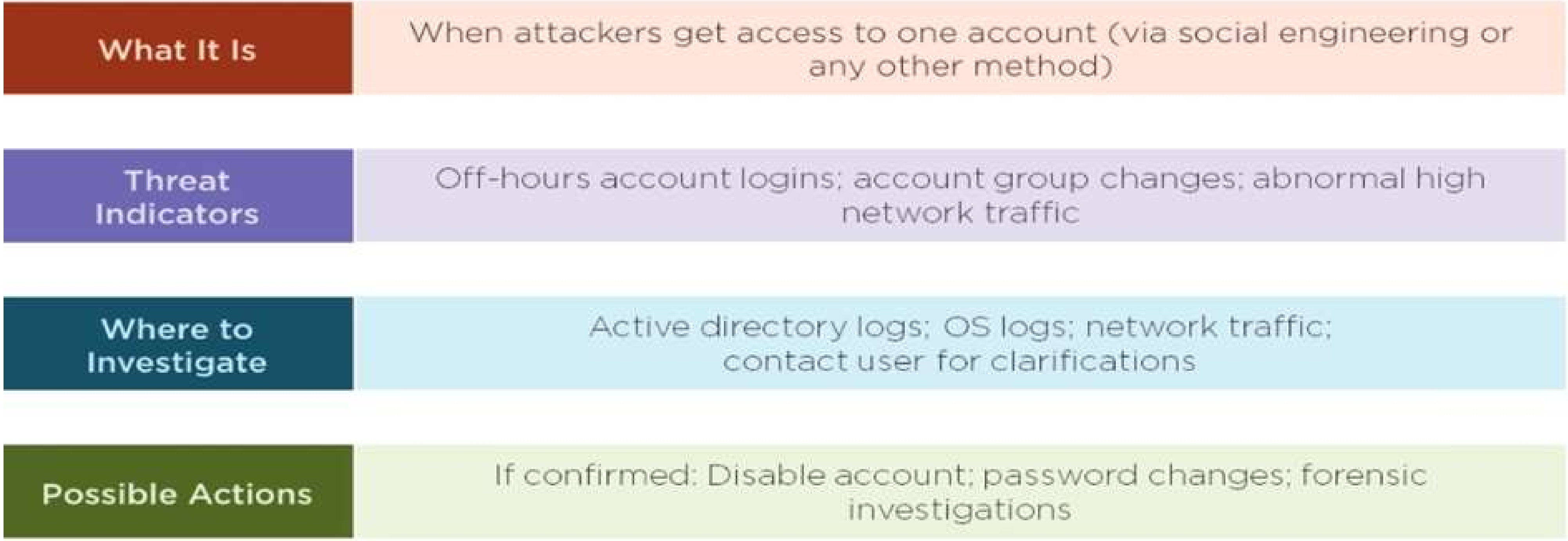


What It Is	A piece of unauthorized software used by hackers Includes: Virus, warms, malware, etc.
Threat Indicators	Anti-virus alerts; connection to suspicious IPs; abnormal volume of network traffic; abnormal open ports
Where to Investigate	AV logs; OS logs; account logs; network traffic; port scans; etc.
Possible Actions	Request AV checks; isolate the machine

USE CASE SCENARIO: IDENTIFY MALWARE USING AN EDR

Rule Name	**Potential malware activity identified**
Description	This rule detects if there is a presence of a malware on the endpoint using the AI/ML capabilities of the EDR
Threat Indicator	Monitor for contextual data about a malicious payload, such as compilation times, file hashes, as well as watermarks or other identifiable configuration information
Data Source to be investigated	This rule is specifically applicable to all endpoints (laptops, desktops, servers, cloud based endpoints)
Possible Pro-active Actions	Using the EDR prevention policy to kill the malware at the detection stage
Possible reactive Actions	Quarantining the infected endpoint and performing a deep dive forensics on the machine
Tips & Tricks for Security Analyst	• Check the EDR detections for the endpoint • Identify the infected files and a cnc connection • Check for the lateral movement in the network • Verify the actions taken by an EDR (file quarantined and process blocked) • Escalate to L2 / CIRT for further investigation is analysts feel severity is high/insufficient information

COMPROMISED ACCOUNTS



What It Is	When attackers get access to one account (via social engineering or any other method)
Threat Indicators	Off-hours account logins; account group changes; abnormal high network traffic
Where to Investigate	Active directory logs; OS logs; network traffic; contact user for clarifications
Possible Actions	If confirmed: Disable account; password changes; forensic investigations

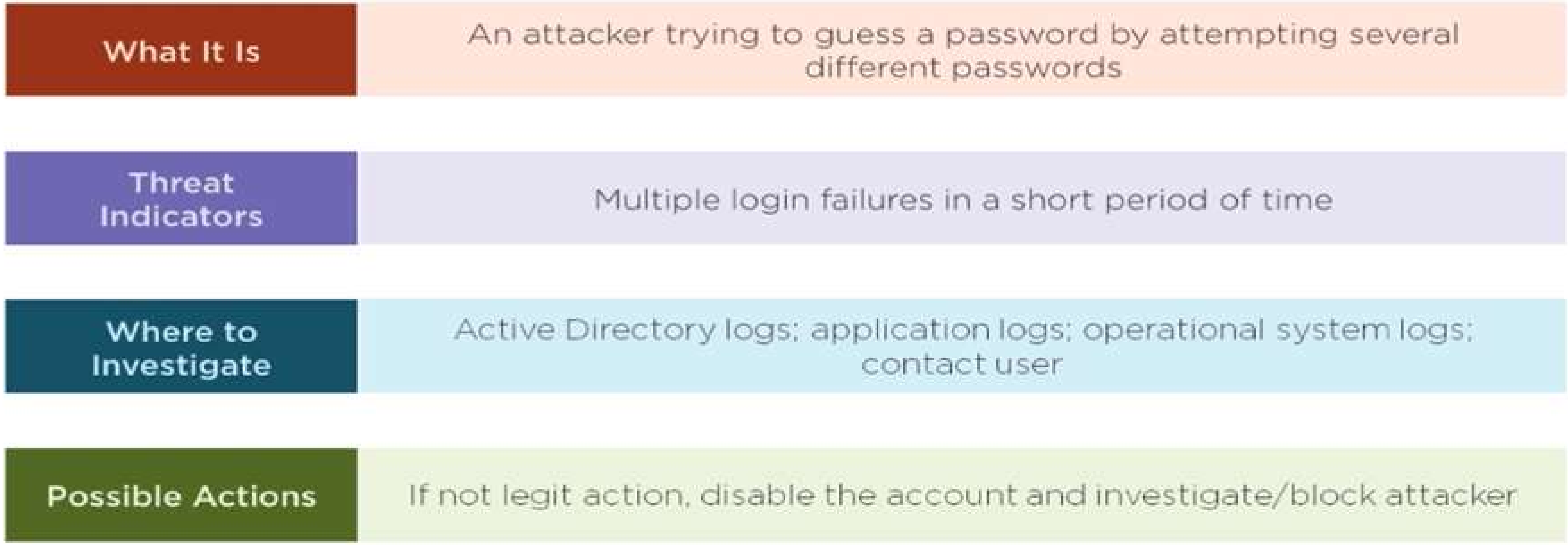
USE CASE SCENARIO: IDENTIFY SUSPICIOUS ACTIVITY

Rule Name	**Audit log cleared on windows system**
Description	This rule detects if the audit logs on the endpoint are cleared and the account which performed the activity
Threat Indicator	Monitor executed commands and arguments for actions that would delete Windows event logs (via PowerShell)
Data Source to be investigated	This rule is specifically applicable to all the windows systems
Possible Pro-active Actions	Protect generated event files that are stored locally with proper permissions and authentication and limit opportunities for adversaries to increase privileges by preventing Privilege Escalation opportunities.
Possible reactive Actions	Identify the suspicious activity and the user who performed it
Tips & Tricks for Security Analyst	• Check the Client User Name / Account Name associated with this. • Identify the user name / AD user name. • Contact the User and his / her manager and ask for justification. • Contact the user via mail/phone or inform his manager using the organization chart • Escalate to L2 / CIRT for further investigation, if analysts feel severity is high/insufficient information. • Maybe CIRT will suspend the account until further clarity. Normally CIRT also works for 8 hours but there is • somebody always available if needed called Watch duty.

USE CASE SCENARIO: IDENTIFY SUSPICIOUS ACTIVITY

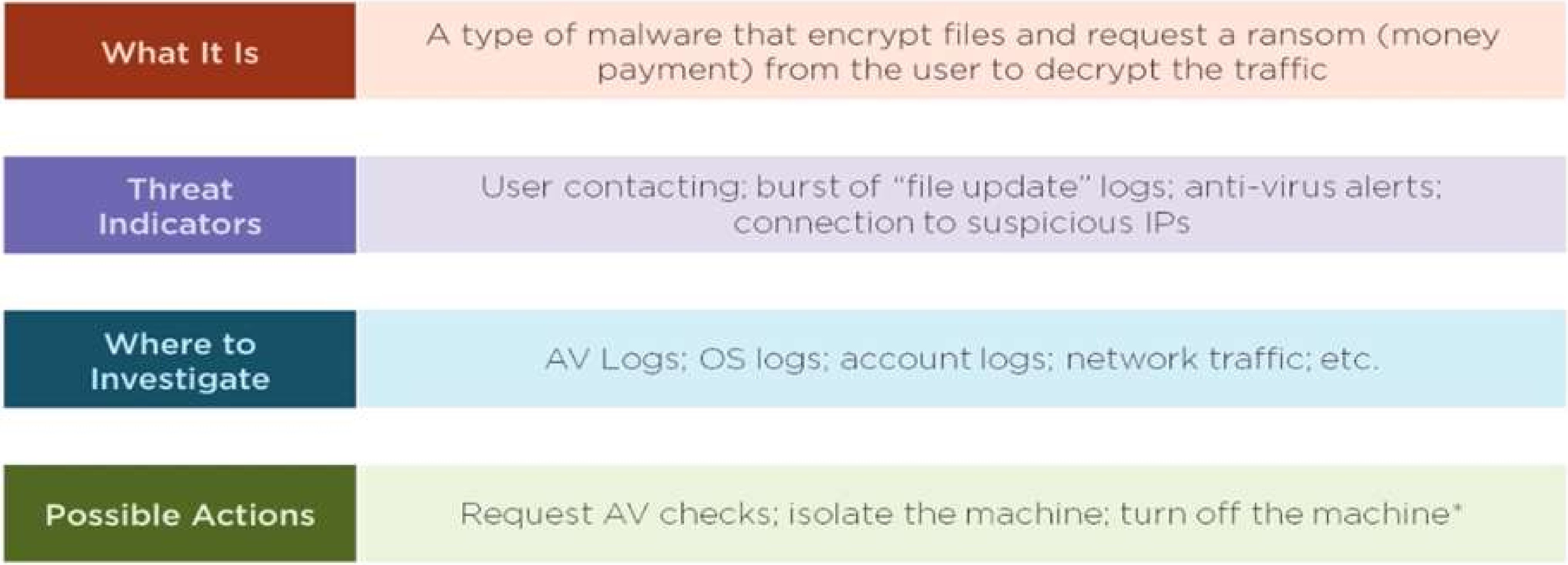
Rule Name	Password Changed by someone other than Windows Administrator / Account Owner
Description	Normally Account password is changed by the account owner. But if it reach to an expired period of account password (due to employee on vacation or any other reason), then the employee may request to windows Admin via ticket or call to reset the password.
Threat Indicator	Monitor for suspicious account behavior across systems that share accounts, either user, admin, or service accounts. Examples: one account logged into multiple systems simultaneously; multiple accounts logged into the same machine simultaneously; accounts logged in at odd times or outside of business hours.
Data Source to be investigated	This rule is specifically applicable to all the windows systems
Possible Pro-active Actions	Protect generated event files that are stored locally with proper permissions and authentication and limit opportunities for adversaries to increase privileges by preventing Privilege Escalation opportunities.
Possible reactive Actions	Identify the suspicious activity and the user who performed it and suspend the account
Tips & Tricks for Security Analyst	• Check the Client User Name / Account Name associated with this. • Identify the user name / AD user name. • Contact the User and his / her manager and ask for justification. • Contact the user via mail/phone or inform his manager using the organization chart • Escalate to L2 / CIRT for further investigation, if analysts feel severity is high/insufficient information. • Maybe CIRT will suspend the account until further clarity. Normally CIRT also works for 8 hours but there is • somebody always available if needed called Watch duty.

BRUTE FORCE ATTACK



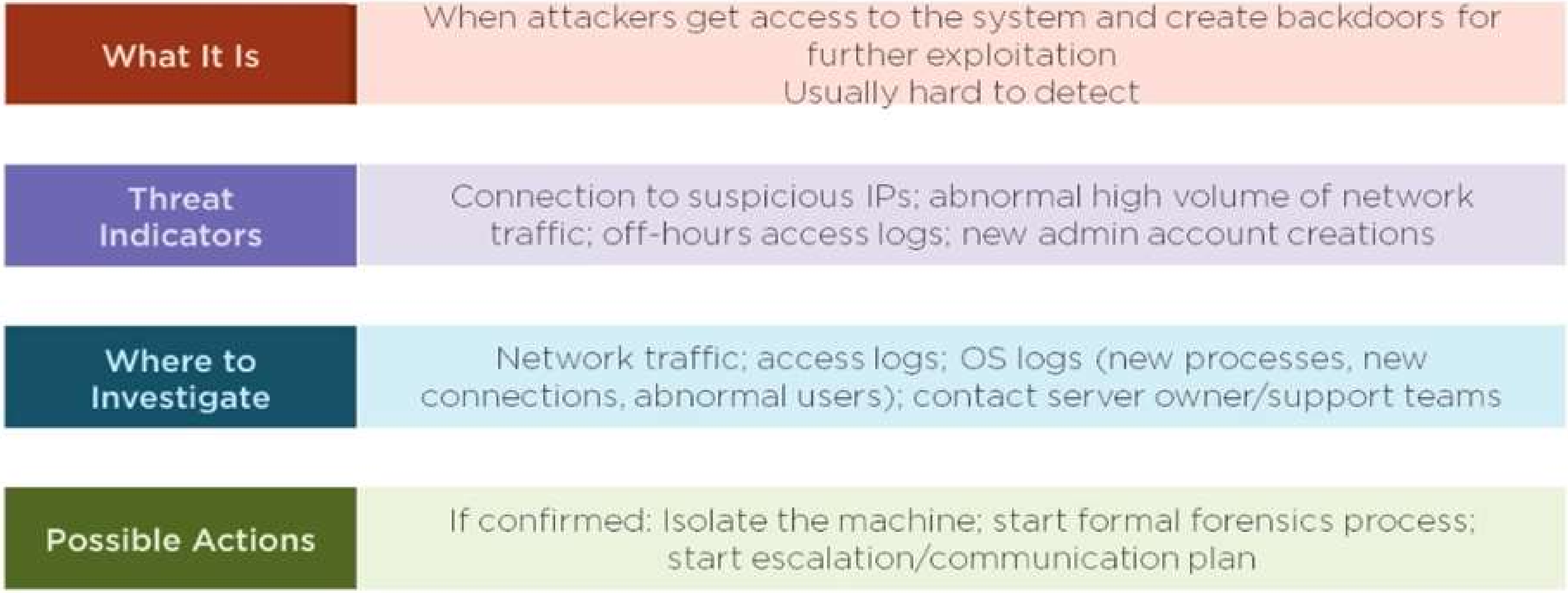
What It Is	An attacker trying to guess a password by attempting several different passwords
Threat Indicators	Multiple login failures in a short period of time
Where to Investigate	Active Directory logs; application logs; operational system logs; contact user
Possible Actions	If not legit action, disable the account and investigate/block attacker

RANSOMWARE



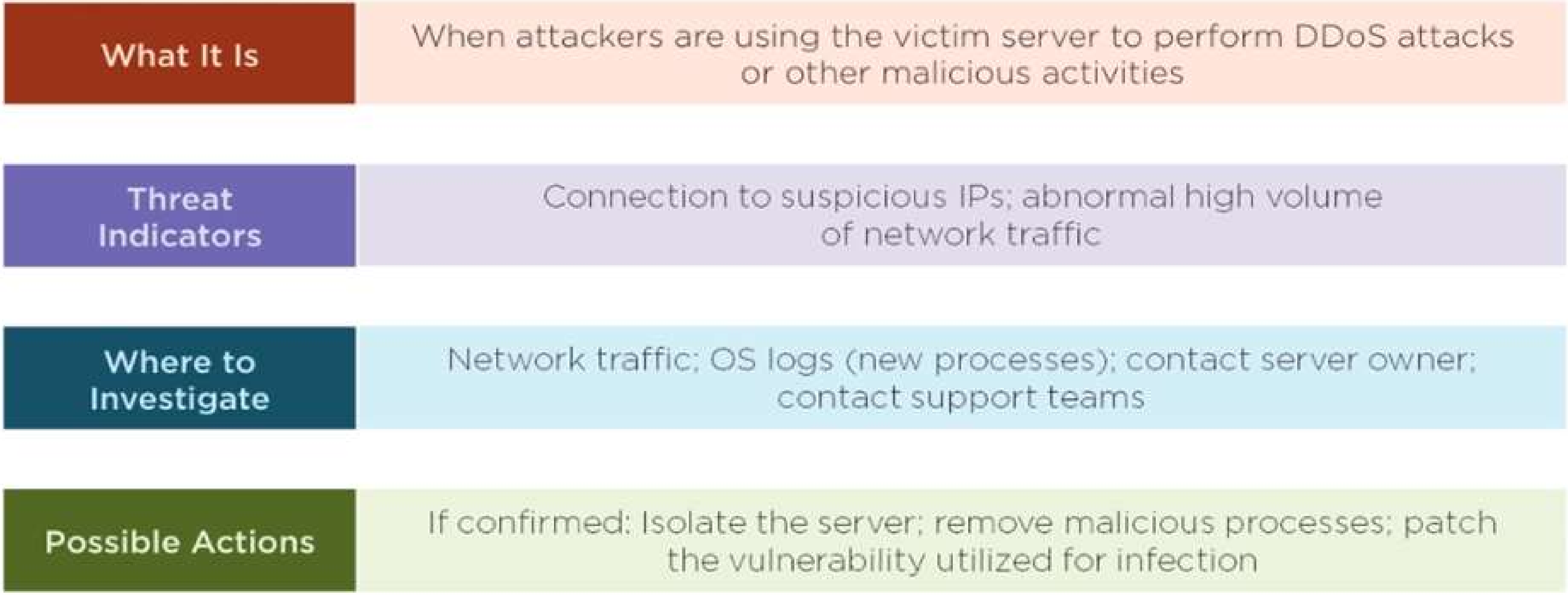
What It Is	A type of malware that encrypt files and request a ransom (money payment) from the user to decrypt the traffic
Threat Indicators	User contacting; burst of “file update” logs; anti-virus alerts; connection to suspicious IPs
Where to Investigate	AV Logs; OS logs; account logs; network traffic; etc.
Possible Actions	Request AV checks; isolate the machine; turn off the machine*

ADVANCED PERSISTENT THREATS



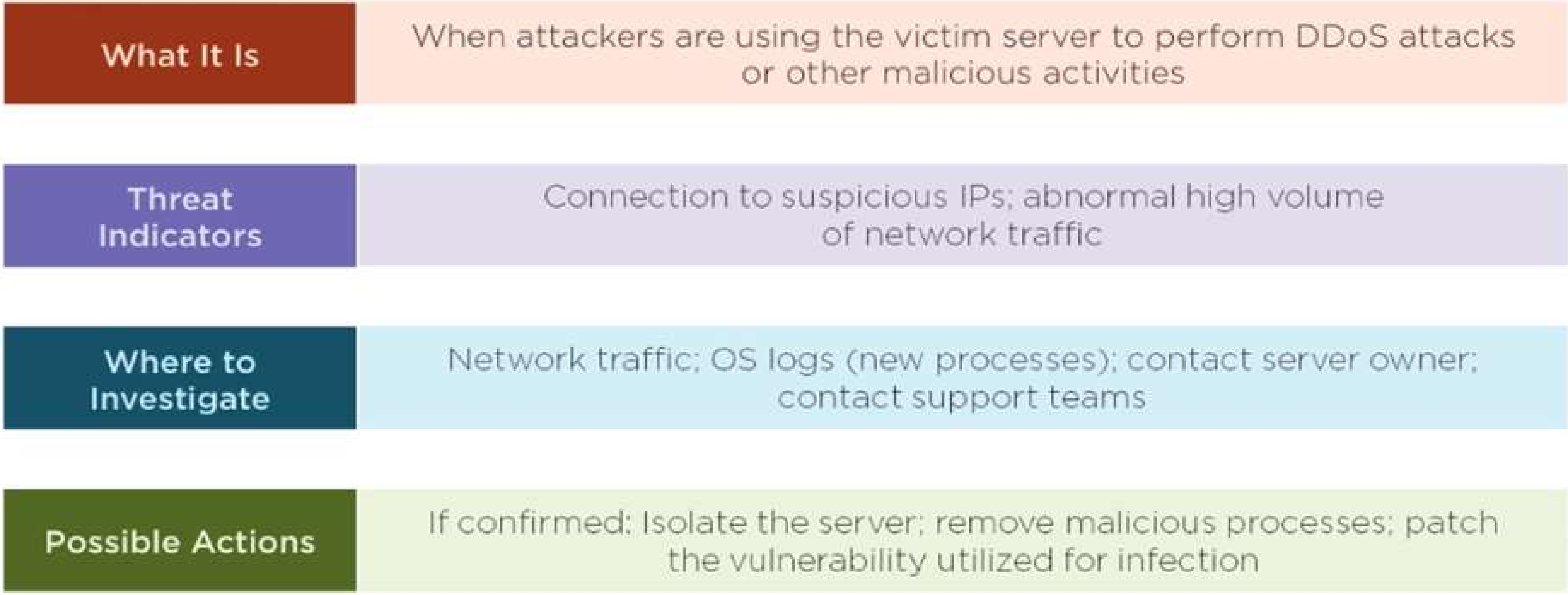
What It Is	When attackers get access to the system and create backdoors for further exploitation Usually hard to detect
Threat Indicators	Connection to suspicious IPs; abnormal high volume of network traffic; off-hours access logs; new admin account creations
Where to Investigate	Network traffic; access logs; OS logs (new processes, new connections, abnormal users); contact server owner/support teams
Possible Actions	If confirmed: Isolate the machine; start formal forensics process; start escalation/communication plan

BOTNETS



What It Is	When attackers are using the victim server to perform DDoS attacks or other malicious activities
Threat Indicators	Connection to suspicious IPs; abnormal high volume of network traffic
Where to Investigate	Network traffic; OS logs (new processes); contact server owner; contact support teams
Possible Actions	If confirmed: Isolate the server; remove malicious processes; patch the vulnerability utilized for infection

DENIAL OF SERVICE (DOS AND DDOS)



What It Is	When attackers are using the victim server to perform DDoS attacks or other malicious activities
Threat Indicators	Connection to suspicious IPs; abnormal high volume of network traffic
Where to Investigate	Network traffic; OS logs (new processes); contact server owner; contact support teams
Possible Actions	If confirmed: Isolate the server; remove malicious processes; patch the vulnerability utilized for infection

THANK YOU

HAPPY LEARNING !!