Full Incident Response Flow Table for 17 Common Attack Scenarios (Expanded - Alphabetical) / usage: left to right

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Attack Technique** | MITRE ID | **Identification Actions (3)** | Identification Defensive MITRE IDs (3) | **Containment Actions (3)** | Containment Defensive MITRE IDs (3) | **Eradication Actions (3)** | Eradication Defensive MITRE IDs (3) |
|  |  |  |  |  |  |  |  |
| Command and Control Over HTTPS | T1071.001 | 1. Analyze SSL traffic anomalies 2. Analyze related logs 3. Alert on behavior | T1071.001 T1082 T1040 | 1. Terminate C2 sessions 2. Quarantine system 3. Disable related accounts | T1071.001 T1021.001 T1078 | 1. Clean persistence mechanisms 2. Malware scan 3. Rebuild clean image | T1071.001 T1204 T1486 |
| Credential Dumping (Mimikatz) | T1003 | 1. Detect Memory Scraping 2. Monitor LSASS Access 3. Alert Unusual Credential Access | T1003 T1003 T1082 | 1. Reset Affected Credentials 2. Isolate Suspicious Hosts 3. Audit Domain Controllers | T1078 T1021.001 T1082 | 1. Remove Credential Dump Tools 2. Patch Vulnerabilities 3. Reimage Compromised Hosts | T1003 T1070 T1486 |
| DNS Tunneling Exfiltration | T1071.004 | 1. Monitor DNS query patterns 2. Analyze related logs 3. Alert on behavior | T1071.004 T1082 T1040 | 1. Block suspicious DNS domains 2. Quarantine system 3. Disable related accounts | T1071.004 T1021.001 T1078 | 1. Reimage data-exfiltrating hosts 2. Malware scan 3. Rebuild clean image | T1071.004 T1204 T1486 |
| Data Encrypted for Impact (Ransomware) | T1486 | 1. Detect mass encryption behavior 2. Analyze related logs 3. Alert on behavior | T1486 T1082 T1040 | 1. Isolate infected systems 2. Quarantine system 3. Disable related accounts | T1486 T1021.001 T1078 | 1. Restore from offline backups 2. Malware scan 3. Rebuild clean image | T1486 T1204 T1486 |
| Exfiltration Over Web Service | T1567 | 1. Monitor outbound traffic size anomalies 2. Analyze related logs 3. Alert on behavior | T1567 T1082 T1040 | 1. Block access to upload sites 2. Quarantine system 3. Disable related accounts | T1567 T1021.001 T1078 | 1. Investigate for exfil traces 2. Malware scan 3. Rebuild clean image | T1567 T1204 T1486 |
| **Attack Technique** | **MITRE ID** | **Identification Actions (3)** | **Identification Defensive MITRE IDs (3)** | **Containment Actions (3)** | **Containment Defensive MITRE IDs (3)** | **Eradication Actions (3)** | **Eradication Defensive MITRE IDs (3)** |
|  |  |  |  |  |  |  |  |
| Input Capture (Keylogging) | T1056 | 1. Detect input capture behavior 2. Analyze related logs 3. Alert on behavior | T1056 T1082 T1040 | 1. Kill keylogging processes 2. Quarantine system 3. Disable related accounts | T1056 T1021.001 T1078 | 1. Remove malware and reimage 2. Malware scan 3. Rebuild clean image | T1056 T1204 T1486 |
| Kerberoasting | T1558.003 | 1. Monitor TGS request volume 2. Analyze related logs 3. Alert on behavior | T1558.003 T1082 T1040 | 1. Reset vulnerable service accounts 2. Quarantine system 3. Disable related accounts | T1558.003 T1021.001 T1078 | 1. Deploy strong service account passwords 2. Malware scan 3. Rebuild clean image | T1558.003 T1204 T1486 |
| Lateral Movement (SMB Admin Shares) | T1021.002 | 1. Detect abnormal SMB activity 2. Analyze related logs 3. Alert on behavior | T1021.002 T1082 T1040 | 1. Audit SMB sessions 2. Quarantine system 3. Disable related accounts | T1021.002 T1021.001 T1078 | 1. Kill unauthorized sessions 2. Malware scan 3. Rebuild clean image | T1021.002 T1204 T1486 |
| Malicious Macro Execution | T1566.001 | 1. Analyze attachments 2. Analyze related logs 3. Alert on behavior | T1566.001 T1082 T1040 | 1. Block macros at email gateway 2. Quarantine system 3. Disable related accounts | T1566.001 T1021.001 T1078 | 1. Remove infected Office files 2. Malware scan 3. Rebuild clean image | T1566.001 T1204 T1486 |
| Obfuscated Malware Files | T1027 | 1. Static analysis of binaries 2. Analyze related logs 3. Alert on behavior | T1027 T1082 T1040 | 1. Quarantine suspicious files 2. Quarantine system 3. Disable related accounts | T1027 T1021.001 T1078 | 1. Reimage compromised hosts 2. Malware scan 3. Rebuild clean image | T1027 T1204 T1486 |
| Password Spraying | T1110.003 | 1. Alert on failed logins 2. Analyze related logs 3. Alert on behavior | T1110.003 T1082 T1040 | 1. Lock suspected accounts 2. Quarantine system 3. Disable related accounts | T1110.003 T1021.001 T1078 | 1. Reset passwords and apply MFA 2. Malware scan 3. Rebuild clean image | T1110.003 T1204 T1486 |
|  |  |  |  |  |  |  |  |
| **Attack Technique** | **MITRE ID** | **Identification Actions (3)** | **Identification Defensive MITRE IDs (3)** | **Containment Actions (3)** | **Containment Defensive MITRE IDs (3)** | **Eradication Actions (3)** | **Eradication Defensive MITRE IDs (3)** |
|  |  |  |  |  |  |  |  |
| Persistence via Registry Run Keys | T1547.001 | 1. Audit autostart registry entries 2. Analyze related logs 3. Alert on behavior | T1547.001 T1082 T1040 | 1. Block unauthorized registry writes 2. Quarantine system 3. Disable related accounts | T1547.001 T1021.001 T1078 | 1. Clean malicious registry keys 2. Malware scan 3. Rebuild clean image | T1547.001 T1204 T1486 |
| Phishing (Attachment/Link) | T1566 | 1. Block Sender Domain 2. Analyze Email Headers 3. Quarantine Suspicious Emails | T1566  T1566.00(spear…) T1082 T1114 | 1. Disable Affected User Accounts 2. Quarantine Devices 3. Block Phishing URLs | T1078 T1021.001 T1071.001 | 1. Reset Passwords 2. Malware Scan 3. Reimage Systems | T1078 T1204 T1486 |
| Privilege Escalation (Token Impersonation) | T1134.001 | 1. Alert on token usage 2. Analyze related logs 3. Alert on behavior | T1134.001 T1082 T1040 | 1. Kill malicious token sessions 2. Quarantine system 3. Disable related accounts | T1134.001 T1021.001 T1078 | 1. Patch elevation exploits 2. Malware scan 3. Rebuild clean image | T1134.001 T1204 T1486 |
| Remote Desktop Protocol Abuse | T1021.001 | 1. Monitor unexpected RDP usage 2. Analyze related logs 3. Alert on behavior | T1021.001 T1082 T1040 | 1. Restrict RDP to whitelisted IPs 2. Quarantine system 3. Disable related accounts | T1021.001 T1021.001 T1078 | 1. Terminate suspicious sessions 2. Malware scan 3. Rebuild clean image | T1021.001 T1204 T1486 |
| Scheduled Task for Persistence | T1053 | 1. Identify new scheduled tasks 2. Analyze related logs 3. Alert on behavior | T1053 T1082 T1040 | 1. Disable suspicious tasks 2. Quarantine system 3. Disable related accounts | T1053 T1021.001 T1078 | 1. Delete and audit scheduled tasks 2. Malware scan 3. Rebuild clean image | T1053 T1204 T1486 |
| Web Shell Deployment | T1505.003 | 1. Monitor web server file changes 2. Analyze related logs 3. Alert on behavior | T1505.003 T1082 T1040 | 1. Block webshell traffic patterns 2. Quarantine system 3. Disable related accounts | T1505.003 T1021.001 T1078 | 1. Remove uploaded webshell 2. Malware scan 3. Rebuild clean image | T1505.003 T1204 T1486 |

**Phishing line:**

Instead of: Identification MITRE ID: **T1566.001**

You could say: Identification MITRE ID: **T1566** (or T1566.001 if spearphishing attachment detected)

**Recognition Signs for Each Attack Type:**

**1. Command and Control Over HTTPS (T1071.001)**

* Unusual encrypted traffic patterns (non-browser SSL traffic)
* Beaconing behavior (regular small outbound packets)
* SSL/TLS anomalies or suspicious certificates

**2. Credential Dumping (Mimikatz) (T1003)**

* Unusual LSASS.exe access by non-standard processes
* Memory scraping attempts detected
* Unusual read operations on Security Account Manager (SAM) files

**3. DNS Tunneling Exfiltration (T1071.004)**

* High volume of DNS requests with unusual patterns
* DNS queries to uncommon domains
* Data encoded inside DNS query strings

**4. Data Encrypted for Impact (Ransomware) (T1486)**

* Mass file modifications or file extensions changing rapidly
* Spikes in CPU/disk usage on endpoints
* Backup systems being tampered with or deleted

**5. Exfiltration Over Web Service (T1567)**

* High outbound data transfer to cloud storage sites (e.g., Dropbox, Google Drive)
* Unusual HTTPS POST traffic volume
* Use of unauthorized applications to upload files

**6. Input Capture (Keylogging) (T1056)**

* Hidden or unauthorized processes hooking into input devices
* Detection of known keylogger signatures
* Outbound connections to C2 servers transmitting keystrokes

**7. Kerberoasting (T1558.003)**

* High volume of Kerberos Ticket-Granting Service (TGS) requests
* Service tickets requested for multiple service accounts
* Authentication requests without prior need for services

**8. Lateral Movement via SMB Admin Shares (T1021.002)**

* SMB traffic outside of normal administrative hours
* Creation of administrative shares on multiple hosts
* Abnormal use of admin credentials over SMB

**9. Malicious Macro Execution (T1566.001)**

* Opening Office documents triggering child processes (e.g., cmd.exe, powershell.exe)
* Macro settings overridden by GPO or user
* Suspicious email attachments with macros

**10. Obfuscated Malware Files (T1027)**

* Unusual encoding or packing observed in binary files
* Malware using base64 or other encoding to hide payloads
* Antivirus triggering on heuristic or obfuscation alerts

**11. Password Spraying (T1110.003)**

* Multiple failed authentication attempts across many accounts
* Login attempts using common passwords (e.g., Password123, Welcome2024)
* Logins from unusual IPs or geographic locations

**12. Persistence via Registry Run Keys (T1547.001)**

* Creation or modification of suspicious registry keys (e.g., HKCU\Software\Microsoft\Windows\CurrentVersion\Run)
* New auto-start entries appearing unexpectedly
* Changes in registry without legitimate software installations

**13. Phishing (Attachment/Link) (T1566)**

* Emails with suspicious links or attachments
* Domains mimicking legitimate organizations (e.g., micr0soft.com)
* User reports or spam filter detections on inbound emails

**14. Privilege Escalation via Token Impersonation (T1134.001)**

* Processes accessing or impersonating security tokens
* Privilege escalation alerts from security monitoring tools
* Abnormal use of SYSTEM or Admin-level tokens by non-system processes

**15. Remote Desktop Protocol (RDP) Abuse (T1021.001)**

* Unexpected RDP session initiation, especially from external IPs
* Multiple RDP connections from the same account within short timeframes
* Use of RDP during off-hours or from unrecognized devices

**16. Scheduled Task for Persistence (T1053)**

* Creation of new or unusual scheduled tasks
* Tasks triggering suspicious executables or scripts
* Scheduled task names that mimic legitimate system processes but are misspelled or slightly altered

**17. Web Shell Deployment (T1505.003)**

* Unexpected changes in web server directories (especially uploads folder)
* Web server sending outbound connections or reverse shells
* Scripts (.php, .aspx) behaving like backdoors

**🧹 Quick Style Summary:**

* **Network anomalies** (weird traffic): ➔ *Command and Control, DNS Tunneling, Exfiltration, Web Shells*
* **Endpoint anomalies** (weird behavior): ➔ *Credential Dumping, Keylogging, Malware Files, Persistence, Scheduled Tasks*
* **Authentication anomalies** (login issues): ➔ *Kerberoasting, Password Spraying, Token Impersonation, RDP Abuse*
* **User behavior anomalies** (user opened bad stuff): ➔ *Phishing, Malicious Macros, Ransomware encryption*