CYBERSECURITY · SEC-06

Attacks & Mitigations

Use this when: you map an alert or incident to MITRE ATT&CK, or need the controls that stop the attacks seen most.

BreakFixLearn

MITRE ATT&CK v20 · Security+ · CySA+
Sheet v1.0 · Nov 2026

Scan to visit

The 15 Enterprise tactics: the attacker's "why"

Amber = split from Defense Evasion in v19

Reconnaissance TA0043 Gather info	**Resource Dev.** TA0042 Buy, build tools	**Initial Access** TA0001 Get in	**Execution** TA0002 Run code	**Persistence** TA0003 Stay in
Privilege Esc. TA0004 Get admin	**Stealth** TA0005 Look normal	**Defense Impairment** TA0112 Break security tools	**Credential Access** TA0006 Steal passwords	**Discovery** TA0007 Map the network
Lateral Movement TA0008 Spread	**Collection** TA0009 Gather data	**Command & Control** TA0011 Talk to home	**Exfiltration** TA0010 Steal data	**Impact** TA0040 Encrypt, destroy

Common attacks: spot them, stop them

ATTACK	TECHNIQUE	SPOT IT	KEY MITIGATIONS
Phishing	T1566	User reports, mail filter hits	M1017 training · M1049 AV
Exploit public app	T1190	WAF and IDS alerts, odd errors	M1051 patch · M1016 scanning
Stolen valid account	T1078	Logon at odd time or place	M1032 MFA · M1026 PAM
Password spraying	T1110.003	4625 across many users	M1032 MFA · M1036 account policy
Malicious PowerShell	T1059.001	Script block log 4104	M1038 app control · M1045 signing
Credential dumping	T1003	LSASS access alerts	M1043 cred. protection · M1026
RDP to spread	T1021.001	4624 logon type 10	M1035 limit access · M1032 MFA
Scheduled task	T1053.005	4698 task created	M1047 audit · M1028 OS config
Clear event logs	T1685.005	1102 log cleared	M1029 send logs off-host
Adversary in the middle	T1557	ARP or DHCP oddities	M1041 encrypt · M1030 segment
Ransomware	T1486	Mass file renames	M1053 offline backup · M1040
Exfil over C2	T1041	Big outbound to one host	M1057 DLP · M1031 IPS

Read an ID

T1110 **.003** Brute Force › Password Spraying

TA	Tactic: the goal
T	Technique; .00x = sub-technique
M	Mitigation
G · S	Threat group · software

Mitigations seen most

M1032	**MFA** accounts, spraying, RDP
M1026	**Privileged accounts** fewer, separate admins
M1051	**Update software** close known holes
M1053	**Data backup** offline, tested restores
M1017	**User training** phishing, reporting

Use it right

LEGAL Emulate attacks only in your lab or with written permission.

CAUTION IDs change between versions (T1562 is now T1685). Note the version.

REMEMBER

- Tactic = **why**; technique = **how**
- MFA appears in many mitigations
- Map every alert to a technique ID

Sources: MITRE ATT&CK Enterprise v20.1 and v19 notes · Microsoft Learn Events to Monitor

CC BY-NC 4.0 · SEC-06 v1.0