CHAPTER 13

Continuous Improvement

Chapter Overview

01

Document, Document, Document

Incident reports, timelines, and lessons learned

02

Validating Mitigations

Confirming remediations actually worked

03

Improving Your Defenses

Privileged accounts, execution controls, and segmentation

Document, Document, Document

Turn incident pain into organizational learning

Incident Documentation

Every incident produces intelligence — capture it or lose it

Incident report: executive summary, technical timeline, IOCs, affected systems

Technical timeline: every attacker action with timestamp and evidence source

IOC list: file hashes, IP addresses, domain names, registry keys, signatures

Gap analysis: what controls failed? what visibility was missing?

Lessons learned meeting: blameless, forward-looking, scheduled within 2 weeks

Feed IOCs into SIEM detection rules — next attacker won't get a free pass

Incident Report Structure

Executive Summary: 1 page — what happened, business impact, current status, key recommendations

Technical Timeline: chronological events with timestamps, evidence sources, and attacker actions

Affected Systems: complete inventory of compromised hosts, accounts, and data

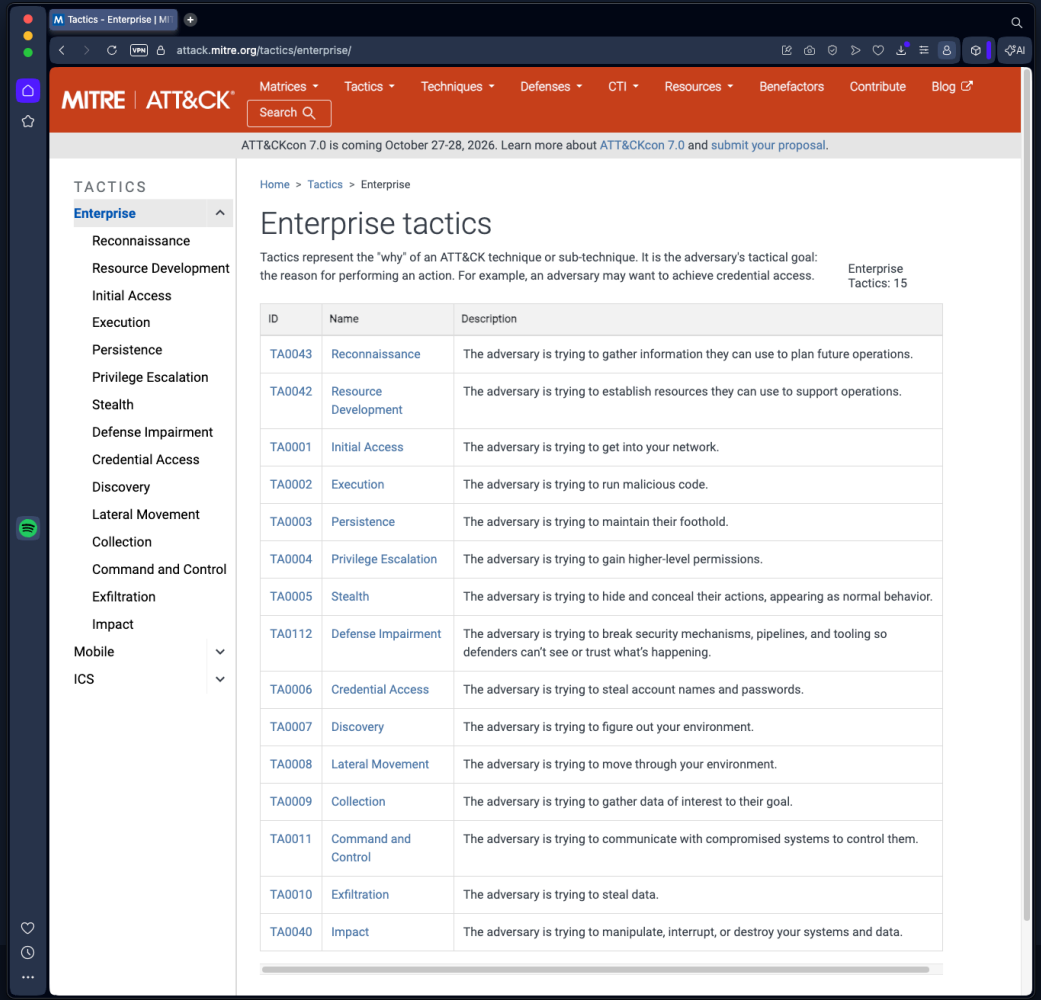
IOC Appendix: hashes, IPs, domains, registry keys, file paths — machine-readable format preferred

Attack Analysis: TTPs mapped to MITRE ATT&CK — enables measurement of detection gaps

Gap Analysis: which controls failed? what detection was missing? what delayed discovery?

Recommendations: specific, actionable, prioritized — not generic advice

Legal consideration: reports may be discoverable — coordinate with legal before sharing widely


Tactics - Enterprise | MI
attack.mitre.org/tactics/enterprise/
MITRE | ATT&CK
Matrices
Tactics
Techniques
Defenses
CTI
Resources
Benefactors
Contribute
Blog
Search
ATT&CKcon 7.0 is coming October 27-28, 2026. Learn more about ATT&CKcon 7.0 and submit your proposal.
TACTICS
Enterprise
Reconnaissance
Resource Development
Initial Access
Execution
Persistence
Privilege Escalation
Stealth
Defense Impairment
Credential Access
Discovery
Lateral Movement
Collection
Command and Control
Exfiltration
Impact
Mobile
ICS
Home > Tactics > Enterprise
Enterprise tactics
Tactics represent the "why" of an ATT&CK technique or sub-technique. It is the adversary's tactical goal: the reason for performing an action. For example, an adversary may want to achieve credential access.
Enterprise Tactics: 15
ID
Name
Description
TA0043
Reconnaissance
The adversary is trying to gather information they can use to plan future operations.
TA0042
Resource Development
The adversary is trying to establish resources they can use to support operations.
TA0001
Initial Access
The adversary is trying to get into your network.
TA0002
Execution
The adversary is trying to run malicious code.
TA0003
Persistence
The adversary is trying to maintain their foothold.
TA0004
Privilege Escalation
The adversary is trying to gain higher-level permissions.
TA0005
Stealth
The adversary is trying to hide and conceal their actions, appearing as normal behavior.
TA0112
Defense Impairment
The adversary is trying to break security mechanisms, pipelines, and tooling so defenders can't see or trust what's happening.
TA0006
Credential Access
The adversary is trying to steal account names and passwords.
TA0007
Discovery
The adversary is trying to figure out your environment.
TA0008
Lateral Movement
The adversary is trying to move through your environment.
TA0009
Collection
The adversary is trying to gather data of interest to their goal.
TA0011
Command and Control
The adversary is trying to communicate with compromised systems to control them.
TA0010
Exfiltration
The adversary is trying to steal data.
TA0040
Impact
The adversary is trying to manipulate, interrupt, or destroy your systems and data.

Creating a Technical Timeline

Timeline is the central artifact of incident documentation

Format: Timestamp | System | EventType | Evidence Source | Detail

Start: when was the initial compromise? (earliest confirmed IOC with evidence)

End: when was the attacker contained/evicted? (last confirmed attacker activity)

Tools: Timeline Explorer, Timesketch, Excel PivotTable, SIEM query export

Sources: EVTX, Sysmon, EDR, Zeek logs, proxy logs, DNS logs, memory artifacts

Dwell time: time from first evidence to detection — industry average is 200+ days

Gaps in timeline: honest documentation of unknown periods avoids overconfident conclusions

IOC Management & Threat Intel Feed

IOCs should be extracted and operationalized within 24 hours of initial discovery

STIX 2.1: standard format for threat intelligence — attackers, techniques, IOCs, relationships

TAXII: transport protocol for sharing STIX data between organizations

MISP (Malware Information Sharing Platform): open-source TI — share IOCs with sector partners

Add file hashes to EDR block list immediately

Add C2 IPs/domains to firewall/DNS blocklist

Add YARA signatures to AV/EDR detection engines

Closed-loop: feed IOCs into SIEM and verify the new rules fire on test data

Validating Mitigation Efforts

Trust but verify

Validating That Mitigations Worked

Never assume a remediation worked — test it

Re-run attacker TTPs against your environment after remediation

Purple team validation: red team retests specific techniques after blue team fixes them

Check that IOCs are blocked: test firewall rules, AV detection, EDR response

Verify new detection rules fire: inject test data that triggers the rule

Validate log coverage: confirm new audit policy settings are applied via GPO

Document results: evidence of effective remediation for management and audit

Purple Team Exercise Workflow

Purple team: red and blue team members work together with shared visibility

Purpose: validate that defensive controls detect the specific techniques used against you

Step 1 — Select TTPs: use ATT&CK techniques from the incident OR with no coverage

Step 2 — Red team executes: run the specific technique in a controlled lab environment

Step 3 — Blue team observes: check SIEM, EDR, and logs — did the detection fire?

Step 4 — Gap identified: if detection missed, immediately write a detection rule

Step 5 — Verify: red team re-executes; blue team confirms the new rule fires

Step 6 — Document: record technique, data source, rule, false positive rate, and result

NIST Cybersecurity Framework v2.0 — the continuous improvement cycle

Improving Your Defenses

Harden after every incident

Privileged Accounts & Execution Controls

Privileged Account Hardening

Tiered admin model: Tier 0 (DC), Tier 1 (Server), Tier 2 (Workstation)

PAWs (Privileged Access Workstations): dedicated admin systems

JIT (Just-in-Time) access: elevate privileges only when needed, expire quickly

No admin accounts for email or web browsing

LAPS: randomized local admin passwords per machine

Execution Controls

AppLocker / WDAC: whitelist approved executables and scripts

PowerShell Constrained Language Mode: limits dangerous cmdlets

Software Restriction Policies: block execution from %TEMP%, %APPDATA%

AMSI: scan PowerShell, VBScript, JavaScript at runtime

Segmentation & Isolation

Network segmentation limits lateral movement blast radius

East-west controls: don't just filter north-south (perimeter) traffic

Workstations should not communicate directly with other workstations

Servers should communicate only on required ports to required systems

VLANs + ACLs for isolation; micro-segmentation (SDN) for granular control

Zero Trust: verify explicitly, use least privilege, assume breach

Emergency isolation capability: ability to quarantine systems in under 5 minutes

ATT&CK Coverage Mapping

ATT&CK Navigator: free web tool for visualizing detection and response coverage

Coverage assessment: for each technique, mark Detected, Prevented, Respond, or No Coverage

Heat map: gaps in red — prioritize for next hunt, detection rule, or control investment

Process: import technique list → score each → export heat map → present to leadership

Frequency scoring: weight techniques by how often adversaries targeting your sector use them

After each incident: update ATT&CK layer with new IOCs and techniques observed

Goal: no ATT&CK technique with zero coverage — every technique needs at least one detection

Use case: demonstrates security maturity to auditors, executives, and cyber insurance underwriters

Detection Engineering & Security Logging

Detection-as-Code: store detection logic in version-controlled files

SIGMA rules: vendor-neutral detection rules compilable to any SIEM query language

Rule lifecycle: Hypothesis → Draft → Test → Tune → Deploy → Monitor → Retire

Test data: use Atomic Red Team tests as synthetic ground truth for rule validation

False positive tuning: every new rule runs in 'alert only' mode for 1 week first

Log retention: 90 days online (searchable), 12 months cold storage — minimum for IR

Immutable log storage: object storage with object lock — attacker cannot delete

Log sources priority: EDR → Windows Security.evtx → Sysmon → DNS → Proxy → NetFlow

Metrics — Measuring Security Posture

MTTD (Mean Time to Detect): average days between compromise and discovery — minimize this

MTTR (Mean Time to Respond): average hours from detection to containment

Detection coverage: % of ATT&CK techniques with at least one active detection

False positive rate: ratio of false alerts to true positives — high rate burns analyst time

Alert volume trend: rising trend without increased threats = detection needs tuning

Incident recurrence rate: same attack vector hitting twice = remediation failed

Hunt yield: incidents discovered via hunting vs. automated detection

Logging coverage: % of systems with centralized log forwarding — gaps = blind spots

Building a Security Improvement Program

Program structure: quarterly review cycle — assess, plan, implement, validate, repeat

Ownership: assign each recommendation to a specific team with a deadline

Priority matrix: score findings by likelihood × impact × ease of fix

Quick wins: low-effort, high-impact controls first (e.g., enable Script Block Logging in one GPO)

Technical debt: document deferred items — acknowledge and schedule, not ignore

Executive alignment: translate technical gaps into business risk to get budget

Third-party assessment: annual red team or external audit provides unbiased validation

Program maturity model: use CMMI or CMM to track security program maturity over time

Conclusion

Continuous improvement converts incident pain into defensive strength

Documentation and lessons learned prevent the same attack from working twice

Validate mitigations — assumption of effectiveness is not evidence

Tiered admin model and PAWs dramatically reduce privilege escalation success

ATT&CK coverage mapping makes gaps visible and prioritization objective

Segmentation is the force multiplier: even successful attackers can't spread far

Knowledge Check