Incident Response

Ondřej Šrámek

24.3.2026

czechitas

Linktree

Ondřej Šrámek

GMON, GNFA, GCTI

- Worked in the public sector and commercial sector
- 12+ years in the field, primarily Incident Response, DFIR, Threat Hunting and Threat Intelligence

czechitas

Agenda

What's ahead today

Agenda

❓ What is an incident?

 MITRE ATT&CK / Kill Chain

🔄 Incident Response (cycle)

🔍 Triage

 Escalation

🤖 AI in Incident Response

💬 Q&A

czechitas

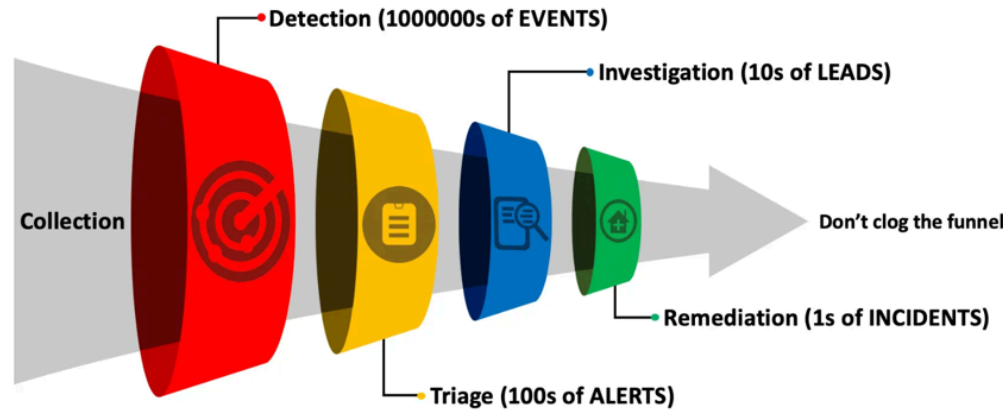
What is an Incident?

From event to incident

Event, Alert, Incident

Event – recorded activity in a system (log, record)
Alert – an event that matched a detection rule and notified the team
Incident – a confirmed security event requiring a response

> *Not every alert is an incident. Triage decides what comes next.*



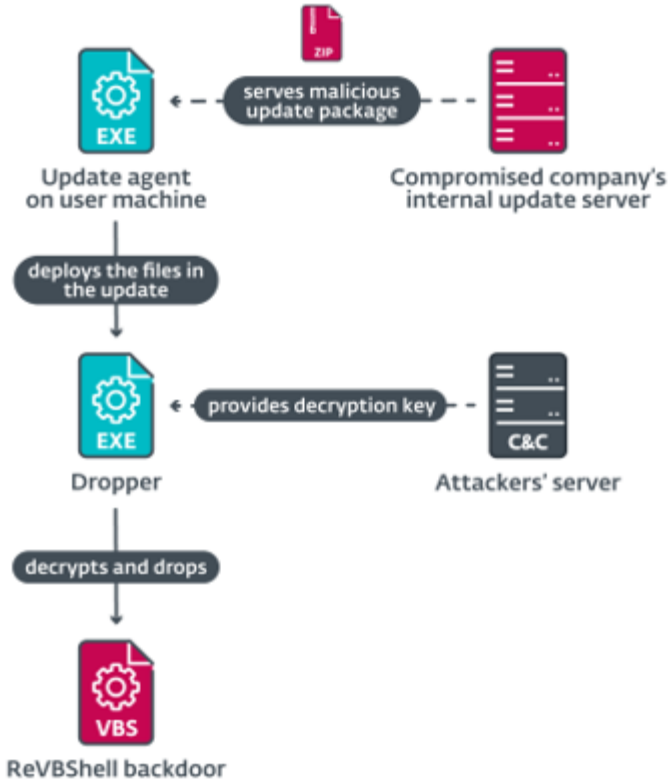
Attack Frameworks

Kill Chain, MITRE ATT&CK, Unified...

Attack Frameworks

Detection often reveals the **attack phase** – how far the attacker has progressed.

- How serious is it?
- Does the attacker still have user privileges, or have they escalated?
- **Response depends on the phase:**
  - Host Isolation vs. Process Kill
  - Password reset – on next login, or immediately?
  - Session / token revocation

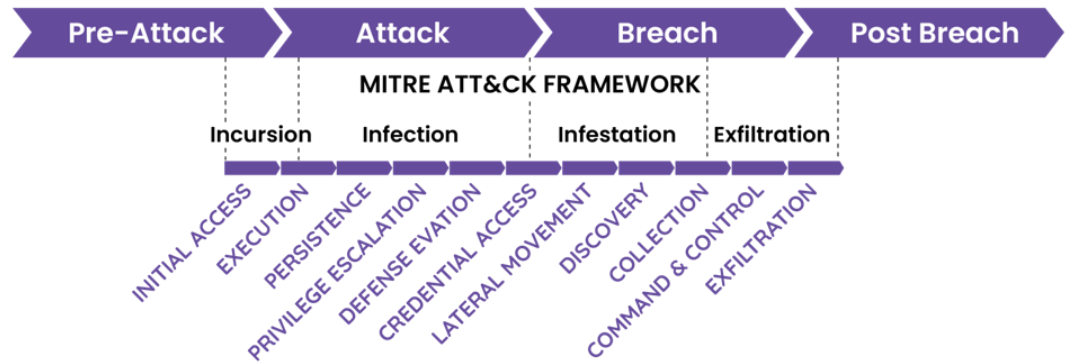


czechitas

MITRE ATT&CK

A globally shared knowledge base of attacker tactics and techniques.

- Structured description of behavior (TTPs)
- Mapping detections to specific techniques
- Foundation for Threat Intelligence and Threat Hunting



czechitas

Cyber / MITRE / Unified

Different framework coverage:

- Depends on the tooling used
- Kill Chain – linear, simple
- MITRE ATT&CK – detailed, non-linear
- Unified Kill Chain – combines both

	Cyber Kill Chain®	MITRE ATT&CK™	Unified Kill Chain
Reconnaissance	√	√	√
Resource Development	√	√	√
Delivery	√	√	√
Social Engineering	✖	✖	√
Exploitation	√	✖	√
Persistence	√	√	√
Defense Evasion	✖	√	√
Command & Control	√	√	√
Pivoting	✖	✖	√
Discovery	✖	√	√
Privilege Escalation	✖	√	√
Execution	✖	√	√
Credential Access	✖	√	√
Lateral Movement	✖	√	√
Collection	✖	√	√
Exfiltration	✖	√	√
Impact	✖	√	√
Objectives	√	✖	√

czechitas

Incident Response Cycle

According to NIST & SANS

Incident Response Cycle

Four fundamental phases according to NIST and SANS:

1. **Preparation**
2. **Detection & Analysis**
3. **Containment, Eradication & Recovery**
4. **Post-Incident Analysis**

1. Preparation

Creating an Incident Response Plan (IRP), defining roles and responsibilities, building the team, and implementing security controls.

Team structure: SOC / CIRT / CERT

Team model: Flat vs. Layered

Skills: Specialization vs. generalist knowledge

Coverage: 8/5 · 24/7 · Follow the Sun · On-call

SOP: General and threat-category specific

Contacts: CISO · Physical Security · IT · PR · HR…

2. Detection & Analysis

Incidents are detected using monitoring and alerting mechanisms. Analysts investigate, collect evidence, and assess impact.

Tools: SIEM · EDR · SOAR · Forensics

Detection: Signatures · Behavioral detection · Threat Intelligence…

Triage: Impact · Severity

IR > DF – Incident Response takes precedence over digital forensic analysis

3. Containment, Eradication & Recovery

Once an incident is confirmed, immediate action is taken – containing the spread, eradicating the threat, and recovering affected systems.

Actions: Isolation vs. Process Kill / Artifact Removal (Business Continuity)

- Depends on the asset owner – security may lead, but…
- Business Continuity & Disaster Recovery plans
- Involvement of other business units (which may take the lead)

4. Post-Incident Analysis

After the incident is resolved, a comprehensive analysis is conducted – causes, weaknesses, and preventive measures.

- **Root Cause** – root cause analysis
- **Reporting & Sharing** – information sharing
- **Lessons Learned**
- **Weakness → Hardening / Patching**
- **Improve detections / log coverage**
- **Missing or insufficient processes**

Triage

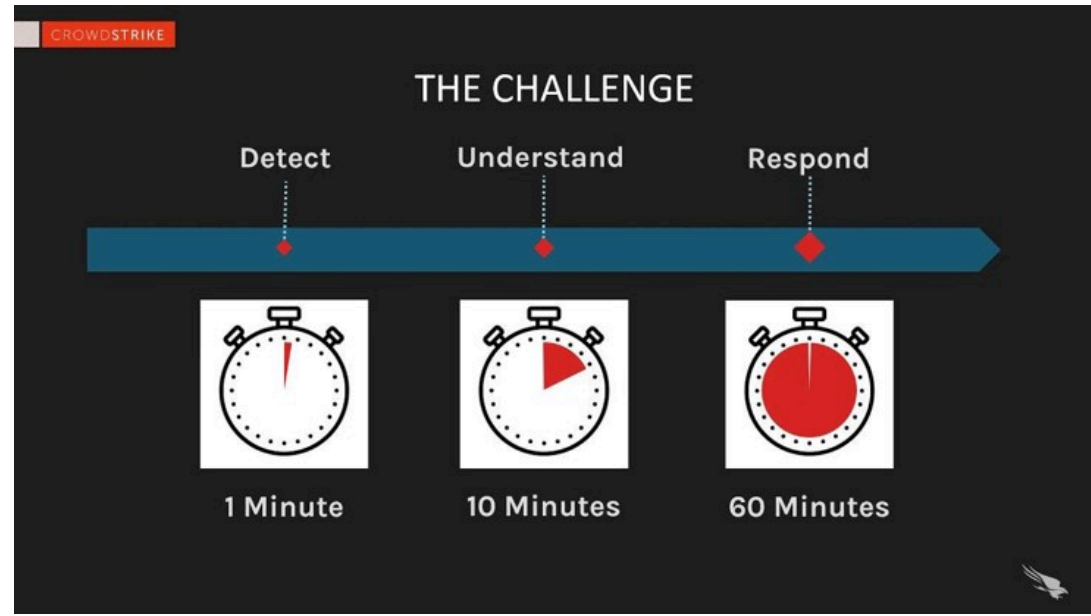
1-10-60

1 – 10 – 60

Target response times according to CrowdStrike:

Time	Action
1 min	Detection and alert
10 min	Investigation (triage)
60 min	Containment

The faster the team responds, the less damage the attacker causes.



czechitas

Attack Stage

Where is the attacker?

- Initial Access
- Privilege Escalation
- Action on Objectives

Impact Analysis:

- Worst tactic / technique reached
- What did the attacker do?

Reversibility:

- **Reversible** (standardization) → lower operational impact
- **Irreversible** (reimaging / restore from backup) → higher operational impact

Response

How to respond to...

How to respond to...

User clicked a phishing link

User opened a maldoc (Word / Excel / PDF)

AV detected malware (at runtime)

Ransomware

(D)DoS

Lost device / Leaked credentials

czechitas

Phishing – user clicked a link

1. Isolate the device from the network
2. Check if credentials were entered
3. Reset password – immediately / on next login based on risk
4. Revoke active sessions / tokens
5. Check mail server – block the phishing sender/domain
6. Threat Intelligence – is the link part of a broader campaign?

Maldoc – user opened a malicious document

1. Isolate the device
2. Determine if a macro / shell / payload was executed
3. EDR – check process tree and child processes
4. Artifact collection – samples for analysis
5. Eradication – delete artifacts or reimage
6. Lessons learned – how did the document pass through the mail gateway?

Ransomware

1. **Immediate isolation** – disconnect devices and network segments
2. Identify "patient zero" and the scope of spread
3. Business Continuity – what is critical for operations?
4. Backups – are they unaffected? Are they offline / immutable?
5. Communication – CISO, legal, PR, and possibly regulators
6. Decision: restore vs. reimage vs. payment (last resort)
7. Post-incident: how did ransomware enter? Initial access vector?

(D)DoS

1. **Identify type:** Volumetric, Protocol, Application-layer
2. Contact ISP / CDN / DDoS protection (Cloudflare, Akamai...)
3. Rate limiting, IP blacklisting, geo-blocking
4. Check whether DDoS is a smoke screen for another attack
5. Monitor service availability and customer impact

Lost Device

1. Contact physical security – in case of theft, also contact police
2. Police confirmation may be required (insurance, GDPR reporting)
3. **Brick the device** – rotate the disk encryption key
4. Remote wipe

Leaked Credentials

Notification from provider / CTI / OSINT / Law Enforcement.

Identification:

- Affected users
- What was leaked and from which device

Leak types: Password · Session tokens · Hash · Phone number · PII

Actions:

1. Password reset / Session revocation / Token revocation
2. Notify users – everything leaked must be changed / protected!

Escalation

From L1 to L3

Escalation Process

Higher tiers (L2 / L3) – when to escalate:

- You need help with the investigation
- Immediate action is required (Hands on Keyboard)

Detection Engineering:

- Detection tuning is needed
- False Positive / False Negative
- Whitelisting a legitimate process / domain / ...
- Detection of legitimate behavior

General rule: Escalate before it's too late. Better a needless escalation than a late response.

AI in Incident Response

Working smarter, not harder

Where AI Fits in the IR Cycle

IR Phase	AI Use Case
Preparation	Threat modeling assistance, playbook drafting
Detection	Anomaly detection, alert correlation
Triage	Priority scoring, false-positive filtering
Response	Automated containment, IR report generation
Post-incident	Root cause summarization, timeline reconstruction

Practical AI Tools for Analysts

Tool	Use Case
Microsoft Copilot for Security	Log analysis, KQL query generation
Google SecOps / Gemini	SIEM query assistance, threat summaries
Claude / ChatGPT	Phishing analysis, malware explanation, report drafting
Darktrace / Vectra	Autonomous network anomaly detection

Limitations & Risks

Hallucinations — confident but wrong answers

Data privacy — never paste sensitive logs into public LLMs

Alert fatigue can be amplified if AI is misconfigured

AI is a force multiplier — not a replacement for analyst judgment

Summary

Summary – Incident Response

Triage is key

- 1-10-60 as the response target
- Attack phase determines severity and response type

Response

- Depends on the incident type
- Isolation, eradication, recovery

Escalation

- Escalate early, not too late

Resources & Further Reading

Resource	Description
NIST 800-61	Computer Security Incident Handling Guide
SANS Cheat Sheet Booklet	Quick reference sheets for IR analysts
Awesome Incident Response	Curated list of IR tools and resources
IR Playbooks → MITRE	Playbooks mapped to MITRE ATT&CK

Further Courses & Practice

TryHackMe

LetsDefend

SANS (GIAC) · EC-Council

CTF competitions

czechitas

Q&A

Thank You for Your Attention!

Ondřej Šrámek

Czechitas · DA Cybersecurity · 2026

czechitas

Feedback

Feedback form

czechitas