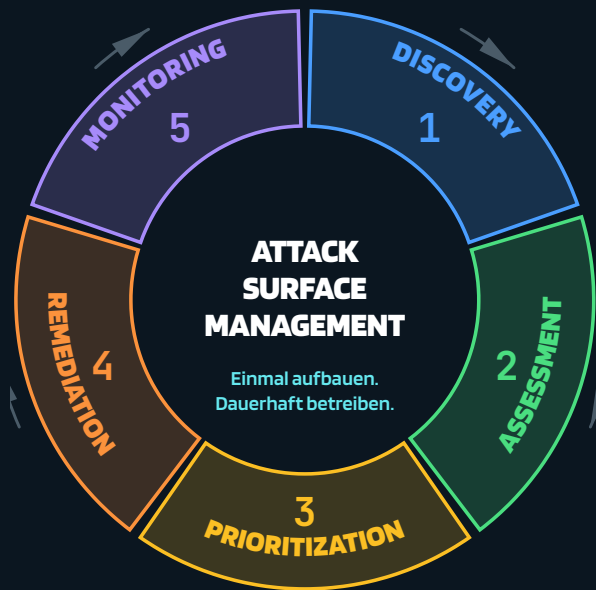


Der ASM-Kreislauf

ASM ist kein Projekt mit einem Enddatum, sondern ein Betriebsprinzip. Fünf Phasen, ein Kreislauf, kontinuierliche Reduktion des Risikos.



Neue Erkenntnisse aus dem Monitoring starten die nächste Discovery-Runde. ASM ist ein Dauerprozess, kein Projekt. Das Risiko sinkt nur, wenn der Kreislauf nie endet.

1 Discovery Was ist öffentlich sichtbar?

Initial 1 bis 3 Tage

- Externe Perspektive: Was sieht ein Angreifer ohne Insider-Wissen?
- Alle IPs, Domains und Subdomains kartieren
- Zertifikate durchsuchen, sie zeigen vergessene Subdomains
- Cloud-Ressourcen inventarisieren, auch die vergessenen
- Service-Banner analysieren: Welche Software läuft auf welchem Port?

WERKZEUGE [Shodan](#) [Censys](#) [Amass](#) [Nmap](#) [Qualys](#) [EASM](#)

2 Assessment Wie exponiert sind die Assets?

Wöchentlich

- Für jedes Asset: Ist es tatsächlich aus dem Internet erreichbar?
- Softwareversionen gegen CVE-Datenbanken abgleichen
- Fehlkonfigurationen finden: offene Datenbanken, Default-Credentials, fehlendes TLS
- Kritikalität des Assets bewerten: Welche Daten sind gefährdet?
- Schatten-IT erkennen: Ist das System im Inventar?

WERKZEUGE [Nuclei](#) [OpenVAS](#) [Nessus](#) [Qualys](#) [CISA KEV](#) [ENISA EUVD](#)

3 Prioritization Was muss zuerst behoben werden?

Nach jedem Assessment

- CVSS-Score als Ausgangspunkt, nicht als einziges Kriterium
- Risk-Based Priorisierung: vier Faktoren kombinieren, aktive Ausnutzung, Exponierung, Asset-Kritikalität, kompensierende Kontrollen
- CISA KEV als Goldstandard für aktiv ausgenutzte Schwachstellen
- EPSS als ergänzende Metrik, wahrscheinlichkeitsbasiert
- Ergebnis: Reparatur-Reihenfolge mit klaren Patch-SLAS

WERKZEUGE [CISA KEV](#) [EPSS](#) [Tenable Lumin](#) [Rapid7 InsightVM](#)

4 Remediation

Beheben, mitigieren oder akzeptieren?

Gemäß SLA

- Patchen: Software-Update, Konfigurationsänderung, unnötige Dienste deaktivieren
- Mitigieren: WAF-Regeln, Netzwerkisolation, erhöhtes Monitoring als Überbrückung
- Akzeptieren: bewusste, dokumentierte Risikoakzeptanz mit Kompensationsmaßnahmen
- Dokumentation: alle Entscheidungen schriftlich, Audit-Trail für BSI und BaFin
- Verifikation: erneuter Scan nach jedem Patch

WERKZEUGE Ansible Terraform WAF ModSecurity / OWASP CRS Jira / ServiceNow

5 Monitoring

Wie sichern wir dauerhafte Sichtbarkeit?

Täglich

- Kontinuierliches externes Scanning: neue Assets, neue Ports, neue Schwachstellen
- Score-Monitoring für eigene Infrastruktur und Lieferanten
- CVE-Feeds abonnieren, neue Schwachstellen automatisch einspeisen
- Alerting: erscheint ein neuer Dienst auf bekannten IPs, sofortige Benachrichtigung
- Erkenntnisse aus dem Monitoring starten die nächste Discovery-Runde

WERKZEUGE Shodan Monitor SecurityScorecard / BitSight OWASP Dependency-Track BSI-Sicherheitshinweise CISA KEV-Feed

PATCH-SLA-RICTWERTE AUS PHASE 3

Kritisch und aktiv ausgenutzt	CISA KEV + CVSS ≥ 9.0 + exponiert	24 bis 48 Stunden
Kritisch	CVSS ≥ 9.0 + aus dem Internet erreichbar	7 Tage
Hoch	CVSS 7.0 bis 8.9 + aus dem Internet erreichbar	30 Tage
Mittel	CVSS 4.0 bis 6.9	90 Tage
Niedrig	CVSS < 4.0	Nächstes Patch-Fenster

CISA KEV, der Known Exploited Vulnerabilities Catalog, ist kostenlos unter cisa.gov/known-exploited-vulnerabilities-catalog abrufbar. Er ist der Goldstandard für die Frage, ob eine Schwachstelle gerade aktiv ausgenutzt wird.
Eigene Darstellung. Stand: September 2026