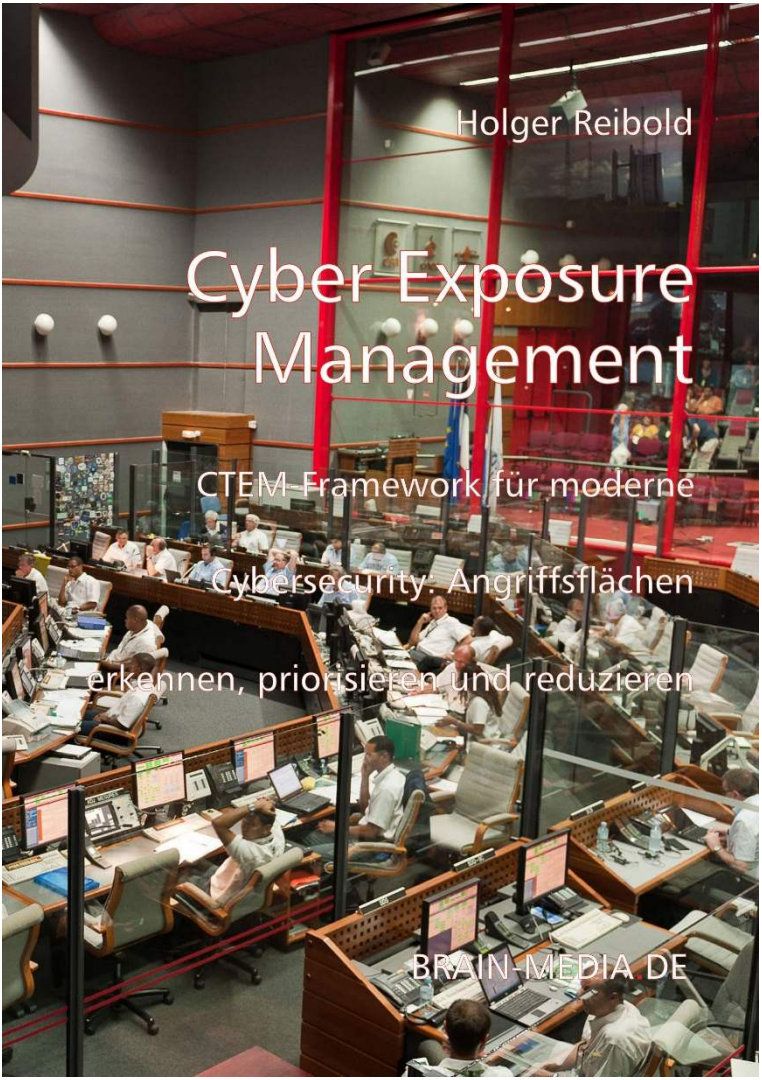

Checklisten für die fünf CTEM-Phasen

Die folgenden Checklisten unterstützen Organisationen dabei, die einzelnen Phasen des Continuous Threat Exposure Management strukturiert umzusetzen. Sie dienen als praktische Orientierung für Security-Teams, IT-Verantwortliche und Führungskräfte, um den Fortschritt ihres CTEM-Programms zu überprüfen.

1. Scoping – Fokus definieren

Ziel dieser Phase ist es, den Umfang der Analyse festzulegen und jene Systeme und Geschäftsbereiche zu identifizieren, die im CTEM-Prozess berücksichtigt werden sollen. Ein klar definierter Scope verhindert, dass Sicherheitsanalysen zu breit oder zu unstrukturiert durchgeführt werden.

☐ Kritische Geschäftsprozesse identifiziert

☐ Geschäftskritische Assets dokumentiert

☐ Relevante Cloud- und SaaS-Plattformen berücksichtigt

☐ Externe und interne Angriffsflächen definiert

☐ Business-Impact-Analyse durchgeführt

☐ Stakeholder und Verantwortlichkeiten festgelegt

☐ Scope der Analyse klar dokumentiert

2. Discovery – Angriffsflächen sichtbar machen

In dieser Phase wird die tatsächliche Angriffsfläche der Organisation analysiert. Ziel ist es, potenzielle Schwachstellen, Fehlkonfigurationen und Exposures zu identifizieren. Die Discovery-Phase bildet die Grundlage für alle weiteren CTEM-Schritte.

☐ Externe Angriffsfläche (EASM) analysiert

☐ Interne Infrastruktur gescannt und bewertet

☐ Cloud-Ressourcen und Container-Plattformen einbezogen

☐ Identitäten und Berechtigungsstrukturen überprüft

☐ Fehlkonfigurationen identifiziert

☐ Supply-Chain-Schnittstellen analysiert

☐ Sicherheitsdaten aus verschiedenen Quellen konsolidiert

3. Priorisierung – Risiken bewerten

Nicht jede identifizierte Schwachstelle stellt automatisch ein kritisches Risiko dar. In dieser Phase werden Sicherheitsprobleme im Kontext ihrer tatsächlichen Auswirkungen bewertet. Eine strukturierte Priorisierung hilft Security-Teams, ihre Ressourcen gezielt einzusetzen.

☐ Technische Schwachstellen kontextualisiert

☐ Asset-Kritikalität berücksichtigt

☐ Threat-Intelligence-Daten integriert

☐ Angriffspfade analysiert

☐ Business-Impact bewertet

☐ High-Risk-Exposures identifiziert

☐ Priorisierte Maßnahmenliste erstellt

4. Validierung – Sicherheitskontrollen überprüfen

In der Validierungsphase wird getestet, ob identifizierte Risiken tatsächlich ausnutzbar sind und ob vorhandene Sicherheitsmaßnahmen wirksam funktionieren. Diese Phase hilft Organisationen zu verstehen, welche Risiken tatsächlich ausnutzbar sind.

☐ Breach-and-Attack-Simulationen durchgeführt

☐ Sicherheitskontrollen getestet

☐ Automatisierte Validierungstools eingesetzt

☐ Red-Team- oder Purple-Team-Übungen durchgeführt

☐ Angriffspfade simuliert

☐ False Positives identifiziert und reduziert

5. Operationa sierung – Maßnahmen umsetzen

Die letzte Phase konzentriert sich darauf, identifizierte Risiken nachhaltig zu reduzieren und Sicherheitsmaßnahmen in operative Prozesse zu integrieren. Ziel dieser Phase ist es, aus Sicherheitsanalysen konkrete Verbesserungen der Infrastruktur abzuleiten.

☐ Remediation-Prozesse definiert

☐ Verantwortlichkeiten für Maßnahmen festgelegt

☐ Zusammenarbeit zwischen Security und IT-Operations etabliert

☐ Automatisierung von Workflows implementiert

☐ Ticketing- und Tracking-Systeme integriert

☐ Reporting für Management und Vorstand eingerichtet

Kontinuier cher Verbesserungszyk us

CTEM ist kein einmaliger Ablauf, sondern ein fortlaufender Zyklus. Nach der Umsetzung von Maßnahmen beginnt der Prozess erneut mit einer aktualisierten Analyse der Angriffsfläche. Durch diesen kontinuierlichen Prozess kann die Sicherheitsstrategie fortlaufend an neue Bedrohungen und Veränderungen innerhalb der Infrastruktur angepasst werden.

☐ Regelmäßige Neubewertung der Angriffsfläche

☐ Aktualisierung der Risikoanalyse

☐ Anpassung der Priorisierung

☐ Validierung neuer Sicherheitskontrollen

☐ Integration neuer Technologien und Systeme

Mehr zum Thema CTEM

Der vollständige Leitfaden „Cyber Exposure Management – CTEM-Framework für moderne Cybersecurity: Angriffsflächen erkennen, priorisieren und reduzieren“