LogRhythm
The Security Intelligence Company

Das Security Operations Maturity Model – Schnellübersicht

Optimieren Sie Ihre Sicherheitsabläufe

Unternehmen sollten ihre Sicherheitsabläufe als kritischen Geschäftsprozess betrachten. Schließlich sind effektive Sicherheitsabläufe die erste Verteidigungslinie gegen Cyberangriffe. Um diese Effektivität zu gewährleisten, brauchen Unternehmen ausgereifte Programme, die Menschen, Prozesse und Technologien gleichermaßen einbeziehen. Nur so können komplexe Angriffe schnell erkannt und abgewehrt werden.

Manchen Unternehmen fällt es jedoch schwer, ihre Sicherheitsabläufe effektiv zu gestalten. Auch fehlt ihnen die Grundlage, um die Effektivität zu messen und ihre Maßnahmen zu verbessern. Ein ausgereiftes Sicherheitsprogramm befähigt Unternehmen, Bedrohungen früher im Lebenszyklus eines Cyberangriffs zu erkennen – einem Prozess, der sich in mehreren Phasen aufbaut, bis der Angreifer sein Ziel schließlich erreicht hat.

Das Security Operations Maturity Model

LogRhythm hat das Security Operations Maturity Model (SOMM) entwickelt, ein Reifegradmodell, mit dem Unternehmen die derzeitige Reife ihrer Sicherheitsfunktionen bewerten können, um dann schrittweise Verbesserungen vorzunehmen. Unternehmen sollten dieses Modell als Grundlage nutzen, um eine Roadmap hin zu demjenigen Reifegrad zu entwickeln, der vor dem Hintergrund ihrer Ressourcen, ihres Budgets und ihrer Risikotoleranz angemessen ist.

Das Modell von LogRhythm beschreibt fünf Reifestufen für die Sicherheitsvorgänge. Jede Stufe baut auf der vorhergehenden auf und fügt zusätzliche Technologie- und Prozessoptimierungen hinzu, die bewirken, dass die Sicherheitsteams des Unternehmens die mittlere Erkennungszeit (MTTD) und die mittlere Reaktionszeit (MTTR) zunehmend verkürzen können. Diese Verkürzung können Unternehmen mithilfe des Threat Lifecycle Management (TLM) Frameworks von LogRhythm umsetzen. Das Framework umfasst eine Reihe wichtiger Funktionen, die Technologien, Menschen und Prozesse aufeinander abstimmen, um so die wichtigsten Programme des Security Operations Centers (SOC) zu unterstützen.

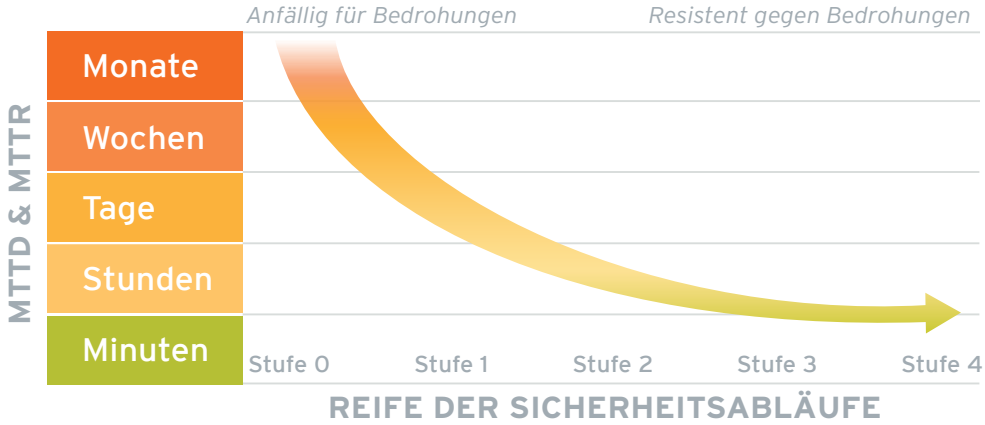

Abb. 1: Wie sehr sich die Zeit zur Erkennung und Bewältigung von Cyberbedrohungen verkürzen lässt, hängt eng mit der Reife der Sicherheitsabläufe zusammen

	TLM-Fähigkeiten	Unternehmensmerkmale	Risikomerkmale
STUFE 0 Blind	• Keine	• Fokus auf Prävention (Unternehmen setzt z. B. Firewalls, Virenschutz etc. ein) • Isoliertes Logging auf Basis technischer und funktionaler Silos, keine Sichtbarkeit durch zentrales Logging • Indikatoren für Bedrohungen und Kompromittierungen existieren, sind aber nicht sichtbar. Kein Threat Hunting, um sie aufzudecken • Kein formaler Prozess zur Reaktion auf Vorfälle; alles hängt von den „heroischen Bemühungen“ einzelner Mitarbeiter ab	• Vorschriften werden nicht eingehalten • Blind für interne Bedrohungen • Blind für externe Bedrohungen • Blind für Advanced Persistent Threats (APTs) • Potenzieller Diebstahl von geistigem Eigentum (wenn es für Staaten oder Cyberkriminelle von Interesse ist)
STUFE 1 Minimal regel-konform	• Zentralisierung der vorgeschriebenen Logdaten und Sicherheitsereignisse • Vorschriftsgemäße, Compliance-getriebene Serverforensik, z. B. File Integrity Monitoring und Endpoint Detection & Response (EDR) • Minimale, Compliance-getriebene Überwachung und Reaktion	• Compliance-getriebene Investitionen, oder das Unternehmen hat einen bestimmten Bereich in seiner Umgebung ermittelt, der geschützt werden muss • Compliance-Risiken werden durch Prüfung von Berichten ermittelt; Prozesse zur Verwaltung von Verstößen können existieren oder auch nicht • Bessere Sicht auf Bedrohungen für den geschützten Bereich wird angestrebt, doch fehlen Mitarbeiter und Prozesse für eine effektive Bewertung und Priorisierung der Bedrohungen • Kein formaler Incident-Response-Prozess; Reaktionen hängen von den „heroischen Bemühungen“ einzelner Mitarbeiter ab	• Deutlich reduziertes Compliance-Risiko (abhängig von der Audit-Tiefe) • Blind für die meisten internen Bedrohungen • Blind für die meisten externen Bedrohungen • Blind für APTs • Potenzieller Diebstahl von geistigem Eigentum (wenn es für Staaten oder Cyberkriminelle von Interesse ist)
STUFE 2 Regel-konform	• Gezielte Zentralisierung von Protokolldaten und Sicherheitsereignissen • Gezielte Server- und Endpunktforensik • Gezielte Charakterisierung von Risiken in der Umgebung • Reaktiver, manueller Vulnerability-Intelligence-Workflow • Reaktiver, manueller Threat-Intelligence-Workflow • Grundlegende maschinelle Analysen zur Korrelierung und Priorisierung von Alarmen • Grundlegende Monitoring- und Reaktionsprozesse vorhanden	• Das Unternehmen geht über den minimalen „Kontrollkästchen-Ansatz“ für Compliance hinaus und strebt nach Effizienz und mehr Zuverlässigkeit • Hat erkannt, dass es die meisten Bedrohungen praktisch nicht entdecken kann; strebt wesentliche Verbesserungen an, um potenzielle gravierende Bedrohungen erkennen und entschärfen zu können, mit Schwerpunkt auf den risikoreichsten Bereichen • Hat formale Prozesse eingerichtet und Verantwortlichkeiten für die Überwachung kritischer Alarme zugewiesen • Hat einen grundlegenden, aber formalen Incident-Response-Prozess eingerichtet	• Extrem belastbare und hocheffiziente Compliance-Aufstellung • Gute Sicht auf interne Bedrohungen, mit einigen blinden Flecken • Gute Sicht auf externe Bedrohungen, mit einigen blinden Flecken • Weitgehend blind für APTs, doch werden Anzeichen und Belege dafür leichter erkannt • Widerstandsfähiger gegen Cyberkriminelle, außer solchen, die APTs einsetzen oder auf Blind Spots abzielen • Stark anfällig für staatliche Angriffe

	TLM-Fähigkeiten	Unternehmensmerkmale	Risikomerkmale
STUFE 3 Wachsam	• Zentralisierung sämtlicher Logdaten und Sicherheitsereignisse • Ganzheitliche Server- und Endpunktforensik • Gezielte Netzwerkforensik • IOC-basierte Threat Intelligence, integriert in die Analysen und Workflows • Ganzheitliche Schwachstellenintegration mit grundlegender Korrelation und Workflow-Integration • Erweiterte maschinelle Analytik für IOC- und TTP-basierte Szenarioanalysen, um bekannte Bedrohungen zu erkennen • Gezielte maschinelle Analysen, um Anomalien zu erkennen (z. B. mithilfe von Verhaltensanalysen) • Formaler und ausgereifter Monitoring- und Reaktionsprozess mit Standard-Playbooks für die meisten häufigen Bedrohungen • Funktionsfähiges physisches oder virtuelles SOC • Fallmanagement für den Workflow zur Untersuchung von Bedrohungen • Gezielte Automatisierung des Untersuchungs- und Problembehebungs-Workflows • Grundlegende operative MTTD/ MTTR-Metriken	• Das Unternehmen hat erkannt, dass es für viele gravierende Angriffe blind ist • Hat in die nötigen organisatorischen Prozesse und Mitarbeiter investiert, um die Fähigkeit zur Erkennung und Reaktion auf Bedrohungen aller Art erheblich zu verbessern • Hat ein formales Security Operations & Incident Response Center (SOC) mit kompetentem Personal eingerichtet • Überwacht Alarme gut und geht allmählich zu proaktivem Threat Hunting über • Nutzt Automatisierung, um die Prozesse zur Untersuchung von Bedrohungen und Vorfallsreaktion zu verbessern und zu beschleunigen	• Extrem belastbare und hocheffektive Compliance-Aufstellung • Hervorragende Sicht auf interne Bedrohungen und schnelle Reaktion darauf • Hervorragende Sicht auf externe Bedrohungen und schnelle Reaktion darauf • Gute Sicht auf APTs, jedoch mit blinden Flecken • Sehr widerstandsfähig gegen Cyberkriminelle, außer solchen, die Angriffe mit APTs führen und dabei Blind Spots ins Visier nehmen • Weiter anfällig für staatliche Angriffe, doch viel größere Wahrscheinlichkeit, dass diese frühzeitig erkannt werden und schnell reagiert wird
STUFE 4 Resistent	• Zentralisierung sämtlicher Logdaten und Sicherheitsereignisse • Ganzheitliche Server- und Endpunktforensik • Ganzheitliche Netzwerkforensik • Branchenspezifische IOC- und TTP-basierte Threat Intelligence, integriert in die Analysen und Workflows • Ganzheitliche Vulnerability Intelligence mit fortschrittlicher Korrelation und automatischer Workflow-Integration • Erweiterte IOC- und TTP-basierte maschinelle Analysen zur Erkennung bekannter Bedrohungen • Erweiterte maschinelle Analysen zur ganzheitlichen Erkennung von Anomalien (z. B. mittels breitgefächerter AI/ML-basierter Verhaltensanalysen) • Etablierte, dokumentierte, ausgereifte Reaktionsprozesse mit Standard-Playbooks für fortgeschrittene Bedrohungen (z. B. APTs) • Etabliertes, funktionsfähiges physisches oder virtuelles 24/7 SOC • Bereichsübergreifende Fallmanagement-Kooperation und -Automatisierung • Weitgehende Automatisierung des Untersuchungs- und Problembehebungs-Workflows • Vollständig autonome Automatisierung für häufige Bedrohungen, von der Bewertung bis zur Eindämmung • Erweiterte operative MTTD/MTTR-Metriken und Verfolgung historischer Trends	• Das Unternehmen ist ein wertvolles Ziel für Staaten, Cyber-Terroristen und die organisierte Kriminalität • Wird kontinuierlich über die verschiedensten Vektoren angegriffen: physisch, logisch, sozial etc. • Dienstunterbrechungen oder Sicherheitsverletzungen sind inakzeptabel und kämen einem organisatorischen Versagen höchsten Grades gleich • Geht proaktiv an das Bedrohungsmanagement und die Sicherheit im Allgemeinen heran • Investiert in hochkarätige Mitarbeiter, Technologien und Prozesse • 24/7 Alarmüberwachung mit organisatorischen und betrieblichen Redundanzen • Verfügt über umfangreiche proaktive Fähigkeiten für Bedrohungsprognosen und Threat Hunting • Verfügt, wo immer möglich, über automatisierte Prozesse zur Bewertung, Untersuchung und Bewältigung von Bedrohungen	• Extrem belastbare und hocheffiziente Compliance-Aufstellung • Kann alle Arten von Bedrohungen schnell erkennen und auf sie reagieren • Erkennt Hinweise auf APTs in einem frühen Stadium des Lebenszyklus und ist fähig, deren Aktivitäten zu entschärfen • Extrem widerstandsfähig gegen Cyberkriminelle aller Art • Kann sich auch gegen die stärksten, staatlich unterstützten Gegner behaupten

7 wichtige Metriken, die Sie in Ihrem SOC erheben sollten

Um die operative Effizienz ihres TLMs zu bestimmen, sollten Unternehmen die folgenden Metriken erheben:

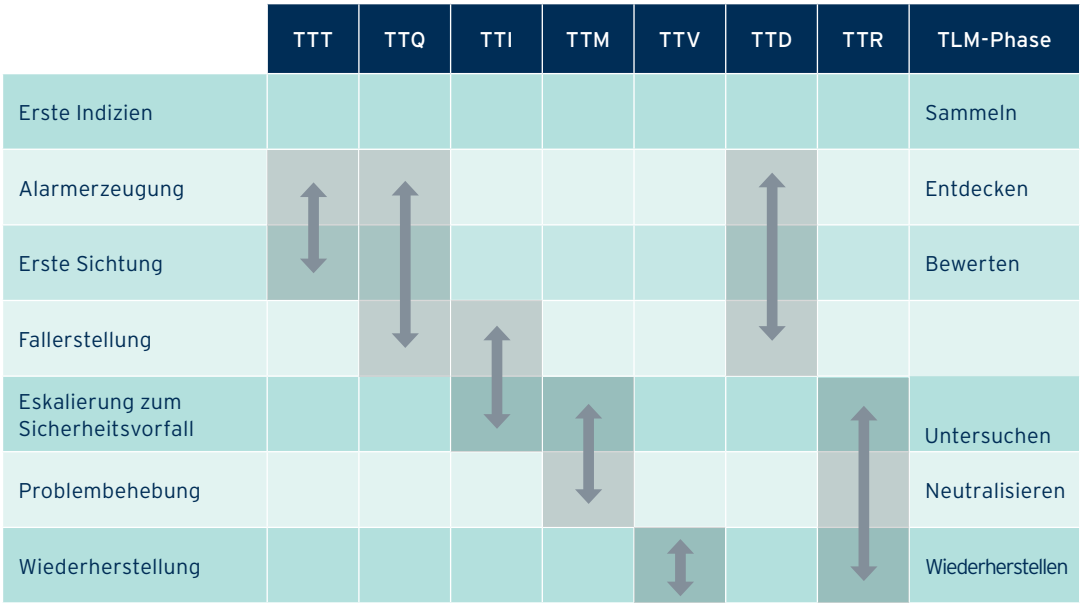

Abb. 2: Sieben Schlüsselmetriken zur Messung der Effektivität des TLMs

- **Zeit zwischen Alarm und Sichtung (Alarm Time to Triage, TTT):** Misst die Verzögerungszeiten bei der Überprüfung eines Alarms
- **Zeit zwischen Alarm und Bewertung (Alarm Time to Qualify, TTQ):** Misst, wie lange Ihr Team gebraucht hat, um einen Alarm vollständig zu prüfen und zu bewerten
- **Zeit zur Untersuchung (Threat Time to Investigate, TTI):** Misst, wie lange Ihr Team gebraucht hat, um eine bestätigte Bedrohung zu untersuchen
- **Zeit zur Problembehebung (Time to Mitigate, TTM):** Misst, wie lange Ihr Team gebraucht hat, um einen Sicherheitsvorfall zu entschärfen und das unmittelbare Risiko für Ihr Unternehmen auszuräumen
- **Zeit zur Wiederherstellung (Time to Recover, TTV):** Misst, wie lange Ihr Team gebraucht hat, um die Wiederherstellung nach einem Sicherheitsvorfall vollständig abzuschließen
- **Zeit zwischen Entdeckung und Bestätigung (Incident Time to Detect, TTD):** Misst, wie lange Ihr Team gebraucht hat, um einen Sicherheitsvorfall zu bestätigen
- **Zeit zwischen Bestätigung und Entschärfung (Incident Time to Response, TTR):** Misst, wie lange Ihr Team gebraucht hat, um einen bestätigten Sicherheitsvorfall zu untersuchen und zu entschärfen

Fazit

Um die Cyberrisiken zu verringern und das Sicherheitsniveau zu erhöhen, müssen Unternehmen ein ausgereifteres Threat Lifecycle Management anstreben – unternehmensweit und über ihre gesamte IT- und OT-Infrastruktur hinweg. Das Security Operations Maturity Model von LogRhythm bietet ihnen eine Roadmap zum Erfolg. Es hilft Unternehmen, die MTTD/MTTR wesentlich zu verkürzen, was das Risiko schwerwiegender Sicherheitsvorfälle erheblich reduziert.

Um mehr zu erfahren, lesen Sie bitte das Whitepaper *Das Security Operations Maturity Model:* www.logrhythm.com/somm.

+49 89 919292 - 200 // europe@logrhythm.com // Balanstraße 73 - Haus 7, 81541 München, Deutschland