Hand in Hand mit MDR gegen Cyber-Angreifer
indevis feat. Grant Thornton

Mittwoch, 26. Oktober 2022

Herzlichen Willkommen!

Ihre heutigen Referenten:

Johannes Potschies
Head of SOC & Service Support

- seit 10+ Jahren in der SIEM/SOC-Beratung & SOC-Leitung tätig
- Schwerpunkte:
  SOC, SIEM & SOAR

E-Mail: johannes.potschies@indevis.de
Tel.: +49 89 452424 215
www.indevis.de

Cengizhan Yücel
Senior Manager Risk Advisory

- seit 12+ Jahren in der Informationssicherheit
- Schwerpunkte:
  Cyber Incident Response

E-Mail: cengizhan.yuecel@de.gt.com
Tel.: +49 211 9524 8415
www.grantthornton.de

Grant Thornton indevis

Agenda

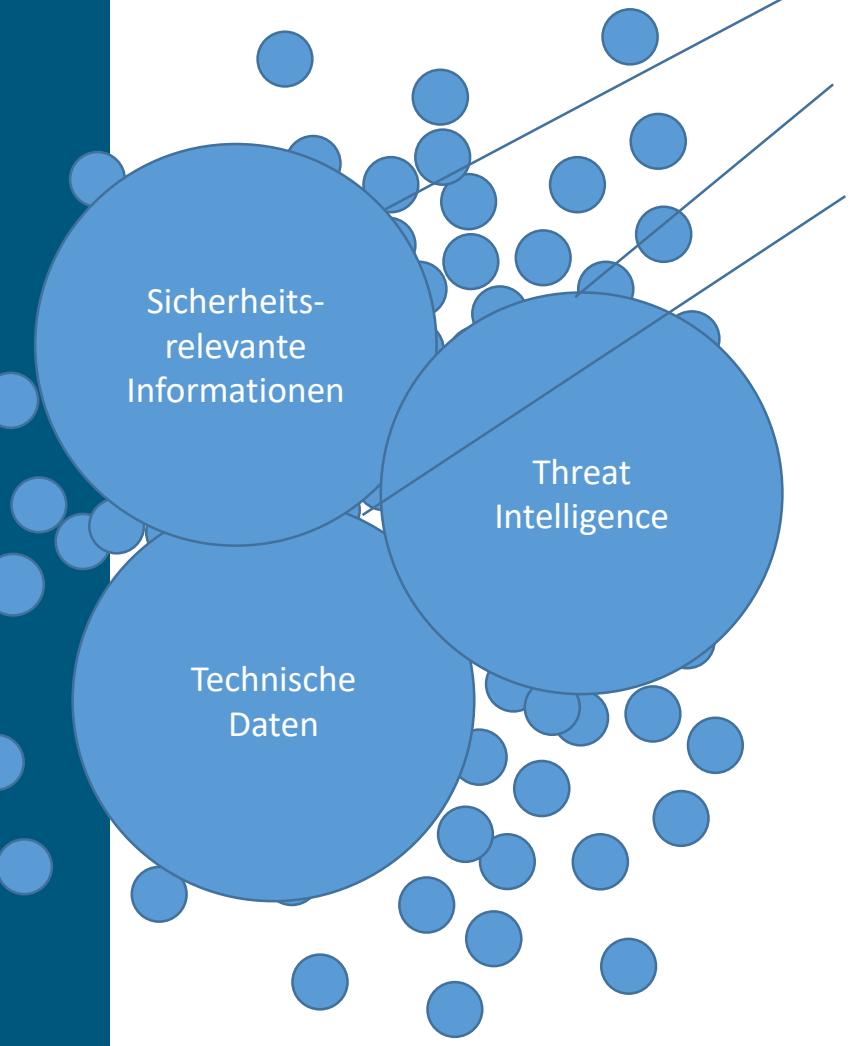
- MDR as a Service
- Reaktion auf Cyber-Vorfälle
- Prävention von Cyber-Vorfällen

MDR as a Service

Managed Detection and Response

Grant Thornton indevis

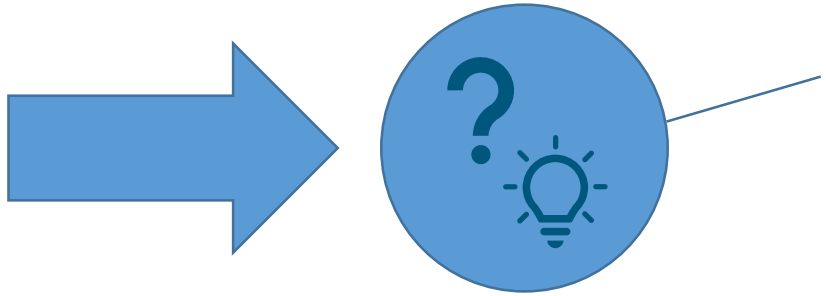
Detection & Response – die Herausforderung



z.B. Ergebnisse aus Schwachstellenscans, …

z.B. Informationen zu C&C-Servern, …

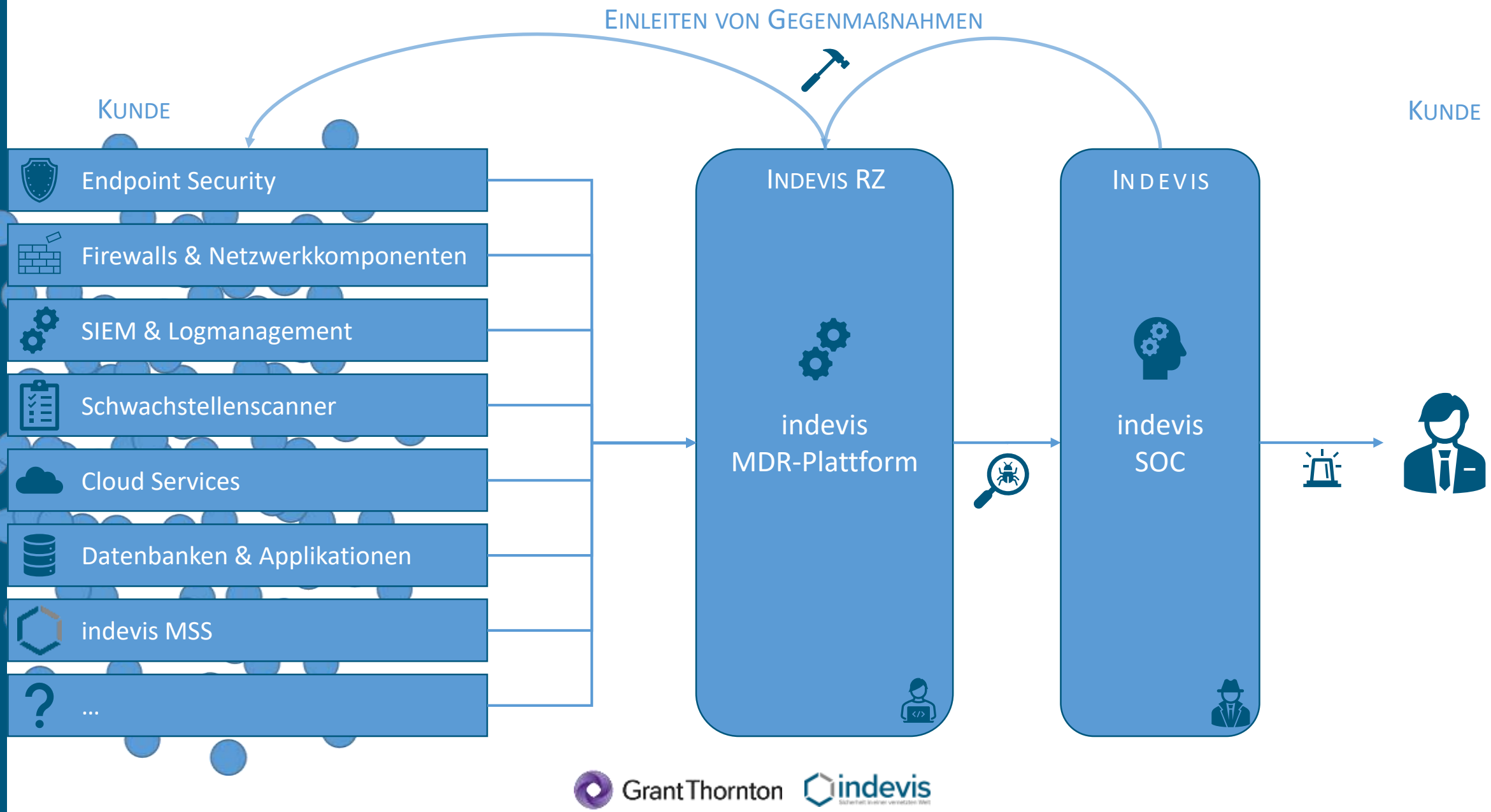
z.B. Logdaten aus dem Netzwerk und von Applikationen, …



Herausfiltern relevanter Informationen erfordert:

- Maschinelle Unterstützung, z.B. SIEM, SOAR, …
- Spezifisches Knowhow

indevis MDR – Datenfluss und Architektur



Grant Thornton indevis

Reaktion auf Cyber-Vorfälle

Unterstützungsdienstleistungen von Grant Thornton

Reaktion auf Cyber-Vorfälle

Cyber Incident Response

- Bei einem Zwischenfall betreuen Sie unsere IT-forensischen Experten und Incident Responder zu sämtlichen IT-Sicherheitsvorfällen wie Hackerangriffen, Datenverlusten etc. Die sofortige Schließung der Sicherheitslücken, Schadensermittlung und Rückverfolgung der Angriffe stehen hierbei neben der Daten- und Systemwiederherstellung im Vordergrund, um entstandene finanzielle und operative Schäden zu minimieren und weitere Negativauswirkungen und Verluste abzuwenden.
- Das Bundesamt für Sicherheit in der Informationstechnologie (BSI) hat uns geprüft und empfiehlt uns als „qualifizierten Dienstleister für APT-Response“.

Cyber Incident Response Rahmenvertrag

- Vorteil: Externe Unterstützung bei Bedarf schnell und unkompliziert abrufbar (z.B. Rahmenbedingungen geklärt, direkter Kontakt)
- Vorteil: Unsere Spezialisten lernen Ihre IT-Infrastruktur / IT-Prozesse vorher kennen und können effizienter auf einen Vorfall reagieren

Grant Thornton indevis

Reaktion auf Cyber-Vorfälle

Digital-forensische Untersuchungen

- Wirtschaftskriminalität kommt in allen Branchen vor. Heutzutage geht es bei der Aufklärung von Straftaten in Unternehmen immer häufiger auch um digitale Daten und ganze IT-Systeme.
- Beratung zu optimalem Vorgehen bei sensiblen IT-forensischen Sonderuntersuchungen und Begleitung bei den notwendigen Schritten – von der Erstaufnahme des Tathergangs über Ad-hoc-Maßnahmen zur Identifizierung und Abgrenzung des Schadensausmaßes bis hin zur Durchführung von gerichtsfesten forensischen Datensicherungen und Analyse der digitalen Beweismittel.
- Bei der Aufklärung von computergestützten Straftaten (Cybercrime) führen wir ebenfalls die IT-forensische Untersuchung des Vorfalls durch. Wir unterstützen Sie bei der Analyse des Angriffsverlaufs sowie bei der Ermittlung des Täters und des entstandenen Schadens.
- Alle Untersuchungsschritte werden von erfahrenen Rechtsanwälten oder Datenschutzbeauftragten unseres Teams einer datenschutzrechtlichen Würdigung unterzogen.

Grant Thornton indevis

Prävention von Cyber-Vorfällen

Beratungsdienstleistungen von Grant Thornton

Prävention von Cyber-Vorfällen

Beratung IT-Notfallmanagement

Erarbeitung von Notfallplänen für gängige Szenarien, beispielsweise:

- DDoS (Distributed Denial of Service): Absicherung durch Unterstützung von Internet Service Providern oder spezieller Anti-DDoS Serviceanbieter
- Ransomware (Erpressungstrojaner): Prüfung der Backup & Recovery Strategie in Bezug auf Schutz gegen unautorisierte Verschlüsselung. Hierbei werden insbesondere das Isolationslevel, die Möglichkeit zur Wiederherstellung großer Datenmengen und der Durchführung von Verifizierungen betrachtet
- Brand im Rechenzentrum: Strategien zur Sicherstellung eines Weiterbetriebs der Infrastruktur durch Verteilung auf verschiedene Standorte, Dienstleister etc.
- Pandemie: Absicherung bei plötzlichem Personalausfall, unter anderem durch Vertretungsregeln und eine aktuelle und vollständige Betriebsdokumentation zur Vereinfachung der Übernahme von Aufgaben

Prävention von Cyber-Vorfällen

Incident Response Readiness Assessment

- Prüfung von bereits vorhandenen Cyber Incident Response Plänen auf Angemessenheit und Vollständigkeit zur Behandlung von Sicherheitsvorfällen. Hierbei werden vor allem die Organisationsstruktur sowie Pläne und Richtlinien zu Kommunikation und vorbereitete Behandlungsmaßnahmen für Incidents betrachtet
- Erarbeitung von Möglichkeiten zur Verbesserung des Ist-Zustandes sowie diesbezügliche Umsetzungsempfehlungen
- Tests und Übungen zur Umsetzung von Cyber Incident Response Plänen anhand von Simulationen und Tabletop Exercises. Hierbei werden die Handlungsabläufe mit den beteiligten Personen trainiert, um Automatismen für den Ernstfall zu entwickeln und die bereichsübergreifende Kooperation zu erproben
- Prüfung von technischen Sicherungsmaßnahmen wie das Einspielen von Datensicherungen und Isolieren von Systemen

Prävention von Cyber-Vorfällen

Cyber Health Check

- Prüfung von technischen und organisatorischen Gegebenheiten mit Informationssicherheitsrelevanz
- Der Prüfungsumfang lässt sich durch einen modularen Aufbau flexibel definieren
- Bestandteil des Checks sind typischerweise folgende Module:
  - Erfassung von grundlegenden Informationen zu Organisation und technischen Maßnahmen mittels Fragebogen und Interviews
  - Prüfung von implementierten Maßnahmen der Sicherheitsorganisation und IT-Sicherheitsinfrastruktur
  - Testung der Infrastruktur mittels Schwachstellenanalysen und Penetrationstests von innen und außen
- Abschließend werden die innerhalb der Module erlangten Informationen bewertet und gemeinsam mit passenden Handlungsempfehlungen bereitgestellt

Grant Thornton indevis

Prävention von Cyber-Vorfällen

Cyber Security Awareness Training

- Zusammenstellung individueller Schulungsinhalte gemäß Mandantenwunsch bzw. aktueller IT-Sicherheitslage
- Konzeption von Schulungsmaßnahmen (bspw. mit Proofpoint)
- Erstellung, Durchführung und Auswertung von Phishing-Kampagnen
- Live-Hacking (Inhalte aus unserem Repertoire, aber auch zusätzliche Inhalte nach Wunsch möglich)
- Strategische Krisensimulation mit verschiedenen Szenarien

Die meisten Sicherheitsvorfälle beginnen mit Phishing. Daher sind wir davon überzeugt, dass eine starke Plattform zur Phishing-Prävention, aber auch für die Schulung Ihrer IT-Nutzer unerlässlich für Ihre Sicherheit ist.

Grant Thornton indevis

Ihre Ansprechpartner

Johannes Potschies
Head of SOC & Service Support

E-Mail: johannes.potschies@indevis.de
Tel.: +49 89 452424 215
www.indevis.de

Cengizhan Yücel
Senior Manager Risk Advisory

E-Mail: cengizhan.yuecel@de.gt.com
Tel.: +49 211 9524 8415
www.grantthornton.de

Grant Thornton indevis