

Managed Detection and Response Implementierung und Best Practice



Falls es irgendwelche Zweifel an der Notwendigkeit der Digitalisierung für den Aufbau von Business Resilience gab, haben die jüngsten Ereignisse diese eliminiert. Externe Kräfte, einschliesslich der globalen Pandemie, haben ein massives Umdenken in unserem täglichen Leben bewirkt. Dazu gehört auch die Verlagerung der Arbeit ins Homeoffice, welche die Dynamik der Belegschaft in den kommenden Jahren stark prägen wird. Unternehmen, die sich 2019 gegen eine dezentralisierte Belegschaft sträubten, fanden sich 2020 gezwungen ihre Digitalisierung zu beschleunigen, um Remotearbeit zu unterstützen. Für viele war dies die einzige Möglichkeit, das Geschäft am Leben zu erhalten.

Die Digitalisierung ist wohl schon seit einiger Zeit im Vormarsch. Der Druck, flexiblere Arbeit anzubieten, um Mitarbeiter zu binden, sowie eine grössere Rücksichtnahme auf den CO2-Footprint des Einzelnen, sind wichtige Faktoren für die beschleunigte Anpassung der Unternehmensrichtlinien. Allerdings fehlt es vielen Unternehmen immer noch an der nötigen Infrastruktur und den Ressourcen, um diese Veränderungen sicher durchführen zu können.

Datensicherheit erwies sich als Stolperstein für Remotearbeit – bis jetzt

Viele Unternehmen waren 2020 nicht darauf vorbereitet, Mitarbeiter, die mit sensiblen Kundendaten und internen Informationen arbeiten, ins Homeoffice zu schicken. Cyberkriminelle reagierten sofort und die Angriffe stiegen von März bis April 2020 um 34 %.¹ Phishing Angriffe verzeichneten einen starken Anstieg von 5'000 pro Woche im Februar auf mehr als 20'000 pro Woche Anfang April 2020.² Den meisten Unternehmen fehlten schlichtweg die Sicherheitstools, Ressourcen und das Know-how, um sich gegen die zahlreichen Angriffe zu schützen.

Obwohl Betriebssicherheit und Cybersecurity bereits oberste Priorität bei IT- und Unternehmensleitern hatte, haben die Ereignisse von 2020 deren dringliche Umsetzung noch stärker in den Fokus gerückt.

Fortschrittliche Organisationen haben sich mit Sicherheitsunternehmen zusammengetan, um ihre Sicherheitsbedürfnisse neu anzupacken, auch im Bereich der Security Operations. Um das erhöhte Risiko sowie Angriffe insgesamt anzugehen, bieten Partner mit Managed Detection and Response (MDR) eine skalierbare Lösung, welche Bedrohungen frühzeitig erkennt, den Schaden begrenzt und ernsthafte Attacken sofort stoppt. Darüber hinaus werden die Fähigkeiten der internen IT- und Sicherheitsteams mit Cybersecurity Experten und fortschrittlichen Technologien erweitert. Diese Kombination hilft Bedrohungen die Stirn zu bieten und ist mit bestehenden Sicherheitskontrollen und anderen relevanten Datenquellen integrierbar.

Dieser Leitfaden beschreibt Herausforderungen in der Post-COVID-Welt, präsentiert neue Perspektiven für die Risikobewertung und zeigt, was eine erfolgreiche MDR Partnerschaft bewirkt.

Sicherheitsexperten stehen vor drei grossen Herausforderungen

Wie auch immer die Mischung aus Büro- und Remotearbeit in Zukunft aussehen mag, Unternehmen müssen akzeptieren, dass Endgeräte sowohl privat als auch geschäftlich genutzt werden. Dazu kommt, dass Mitarbeiter und Auftragnehmer nur begrenzte Kontrolle über die Sicherheit ihres Heimnetzwerks haben.

Weiter wird die Cloud-Nutzung nicht weniger und die digitale Transformation somit weiter vorangetrieben. Dies kann die Nutzung von Software-as-a-Service (SaaS) Lösungen sowie massgeschneiderte cloudbasierte Infrastrukturen, wie etwa Container-Lösungen, beinhalten. Selbst Remote-Connectivity wird möglicherweise nicht mehr vom traditionellen «On Premises»-Rechenzentrum kommen, sondern in der Cloud angesiedelt sein. Für Sicherheitsexperten ergeben sich daraus Herausforderungen in drei Hauptbereichen:

- 1 Identity und Access Management
- 2 Datenschutz und Datensicherheit
- 3 Security Operations, inkl. Detection und Response Fähigkeiten

1 Identity und Access Management (IAM)

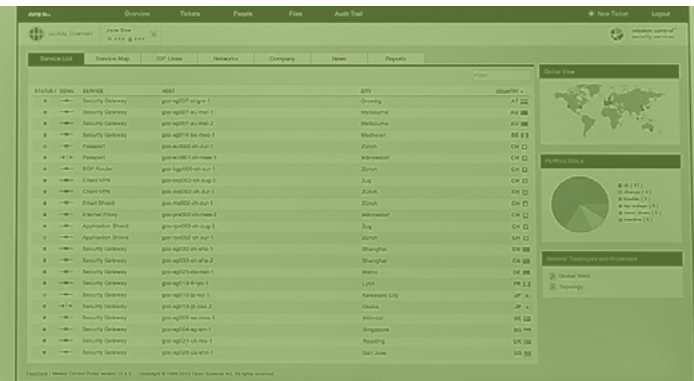
Wie Sie wissen, dienen kompromittierte Anmeldedaten oft als Pforte in das Netzwerk eines Unternehmens.

Anstelle der «Schutzmauer» in Form einer Firewall, ist die Personenidentität der neue Perimeter. Da viele Dienste über eine einzige Anmeldung im Internet verfügbar sind, muss dieser Zugang überwacht und verwaltet werden. Die Praxis des Identity und Access Managements (IAM) automatisiert und strukturiert die Identität einer Person und ermöglicht Überwachung und Schutz, was mit individuellem System Management nicht möglich wäre.

Da immer mehr Unternehmen zu einer neuen hybriden On-Demand/On-Premises-Konfiguration übergehen, wird die Zugangskontrolle immer schwieriger.

User-Password Fatigue, manuelle Bereitstellungsprozesse und die Zugriffsverwaltung über eine Vielzahl von Geräten und Browsern können eine ganze Reihe von Sicherheitslücken eröffnen und die Angriffsfläche einer Organisation somit vergrößern.

Wer, wo, wann und wieso hat eine gewisse Person Zugang? Zu verstehen, wie auf Anwendungen und Daten zugegriffen wird, stellt eine weitere Herausforderung dar, vor allem bei Public Cloud und Remote-Teams, die über die ganze Welt verteilt sind: Diese Identitäten (wann und wo sich jemand anmeldet oder es zumindest versucht) müssen für die Triage der Sicherheitssituation zugänglich sein. Identität ist die neue Firewall. Das macht nicht nur Compliance schwierig, es kann sich auch negativ auf den Datenschutz auswirken.



Source IP	Destination	Port	Protocol	Count	Direction
192.168.1.1	192.168.1.2	80	TCP	1	Out
192.168.1.2	192.168.1.1	80	TCP	1	In
192.168.1.1	192.168.1.2	443	TCP	1	Out
192.168.1.2	192.168.1.1	443	TCP	1	In
192.168.1.1	192.168.1.2	22	TCP	1	Out
192.168.1.2	192.168.1.1	22	TCP	1	In
192.168.1.1	192.168.1.2	3389	RDP	1	Out
192.168.1.2	192.168.1.1	3389	RDP	1	In
192.168.1.1	192.168.1.2	5900	VNC	1	Out
192.168.1.2	192.168.1.1	5900	VNC	1	In

2

Datenschutz und Datensicherheit

Der Datenschutz, der definiert wie Organisationen persönlich identifizierbare Informationen (PII) sammeln und weitergeben, wird immer schwieriger mit der Verlagerung der Unternehmensdaten in die Public Cloud und der Vorschriften-Flut, die diese mit sich bringt: von der General Data Protection Regulation (GDPR) - hierzulande auch als EU-Datenschutzgrundverordnung (DSGVO) bekannt - und dem kalifornischen Verbraucherschutzgesetz (CCPA) bis hin zum Payment Card Industry Data Security Standard (PCI DSS). Heute haben 93 % der Unternehmen eine Multi-Cloud-Strategie und 87 % eine Hybrid-Cloud-Strategie - Unternehmen nutzen durchschnittlich 2,2 Public Clouds und 2,2 Private Clouds.³

Remote-Arbeit erhöht weiter die Komplexität: Wenn ein Unternehmen beispielsweise per Fernzugriff verdächtige Aktivitäten untersucht, besteht auch die Möglichkeit den Endnutzer bei der Eingabe privater Daten (Benutzername und Passwort) zu beobachten.

Cloudbasierte Unternehmen mit Remote-Mitarbeitern müssen anerkennen, dass Cybersecurity eine besondere Herausforderung darstellt. Sie müssen transparent aufzeigen, wie sie gesetzlich geschützte Daten sammeln, sichern und handhaben, und wie sie unbefugte Zugriffsversuche überwachen.



3 Security Operations

Sicherheitsexperten sind mehr und mehr mit der Last 24x7 der Security Operations konfrontiert, einschliesslich der Erkennungs- und Reaktionsfähigkeiten. Die meisten Fachleute sind sich einig, dass die Bearbeitung von Sicherheitsvorfällen zu viel Zeit und Kosten in Anspruch nehmen. In der Tat sind die Gesamtbetriebskosten (TCO) ein wichtiger Faktor für viele CISOs, die hohe Summen in die Sicherheit stecken, ohne dabei viel zu erreichen. Oft liegt es an der Alarmflut: Die zahlreichen Alerts werden zeitintensiv vom Security Operations Team untersucht und Notfälle direkt bearbeitet. Strategie und Prozess-

verbesserungen kommen dabei zu kurz, was zu Burnouts und Fluktuation der Mitarbeiter führt. Andere Faktoren können zu viele manuelle Prozesse, schlecht abgestimmte Sicherheits- und IT-Betriebsteams, ein Mangel an geeigneten Tools und Fähigkeiten oder ein unzureichender Kontext für die Einordnung der Alerts sein. Kurz gesagt: Sicherheitsabläufe sind schwierig und zur Verbesserung reingepumptes Geld muss mit enorm hoher Wirksamkeit und Effizienz einhergehen.



Sicherheit mit Blick auf das grosse Ganze

Die organisatorische Sicherheit in Technologie-Silos zu behandeln, ist ein häufiger Fehler. Sicherheits- und IT-Verantwortliche müssen einen klaren Blick auf das grosse Ganze des Geschäftsrisikos haben, um ihre Investitionen effizient zu schützen. Geschäftsrisiken können auf viele Arten kategorisiert werden, einschliesslich Sicherheit, Finanzen, Technik und Reputation. Geschäftsrisiken können zwar nicht eliminiert werden, aber man kann sie einplanen. Wichtig dabei ist das Gleichgewicht zwischen Chancen und Risiken zu finden.

Das schwierigste bei der Beurteilung des Risikos, ist der Mangel an verwertbaren Informationen. Selbst Informationen über vergangene Ereignisse sind nie ganz vollständig, da Menschen oft unterschiedliche Aussagen über dieselben Vorfälle machen. Um dem entgegenzuwirken, kann die Modellierung von Chancen und Bedrohungen helfen einen Rahmen zu schaffen, der das Risiko sowohl aus der Perspektive der Gefahr als auch der Chance beurteilt. Einige Fragen, die von der **Electronic Frontier Foundation**⁴ für die Risikomodellierung empfohlen werden, sind folgende:

- Was wollen Sie schützen?
- Wovor wollen Sie es schützen?
- Wie wahrscheinlich ist es, dass Sie es schützen müssen?
- Wie schlimm sind die Konsequenzen, wenn Sie versagen?
- Wie viel Mühe sind Sie bereit auf sich zu nehmen, um einen Angriff zu verhindern?

Aber das ist nur die Hälfte der Gleichung. Microsofts EMEA Chief Security Advisor weist in einem einschlägigen Blog über

«Managing Cybersecurity Like a Business Risk» darauf hin, dass das Risiko einer verpassten Chance nicht in der Bedrohungsmodellierung erfasst ist.⁵ Er schlägt vor, folgende Fragen zu berücksichtigen, um die Chancen effektiv zu modellieren:

- Wie hoch ist der Vermögenswert, den Sie schützen möchten?
- Wie hoch ist der potenzielle Gewinn der Chance?
- Wie wahrscheinlich ist es, dass die Opportunity realisiert wird?
- Wie wahrscheinlich ist es, dass eine Stärke ausgenutzt wird?



Mit diesem Rahmen im Hinterkopf müssen Sicherheits- und IT-Verantwortliche ihre Investitionen unter dem Gesichtspunkt der Fähigkeiten versus der Insel-Lösung betrachten. Die Frage lautet also: *Zielen die Investitionen auf den Erwerb von Fähigkeiten ab, die Menschen, Prozesse und Tools nutzen für die Reduzierung der Geschäftsrisiken, oder beschaffen Sie einfach Tools, die ein bestimmtes Kästchen abhaken?*

Diese Frage ist sehr wichtig, da Beschaffungsprozesse und eine schlechte Abstimmung zwischen den Abteilungen Technologien ins Haus bringen, die anstelle Resultate zu liefern, zu erhöhter Komplexität und somit zu verschlechterter Effizienz und Wirksamkeit führen.

In Bezug auf die Erkennung von Vorfällen und die darauffolgende Reaktion bedeutet dies, dass die Vorstellung von Best-of-Breed-Technologien als Allheilmittel für Sicherheits- und Compliance-Herausforderungen aufgegeben werden muss. Ein Business Risk Framework sollte sich stattdessen auf eine fortschrittliche Automatisierung konzentrieren, welche menschliches Know-how einschließt und gut definierte operative Prozesse kombiniert. Unternehmen ermöglicht dies eine schnelle und sichere Bewältigung ihrer Security Anforderungen.

Detection and Response: Einordnung auf der Cyber Kill Chain

Der richtige Partner für effektive Security Operations und Minimierung von Risiken führt schnell zu einem hohen ROI. Managed Detection and Response (MDR) ist eine schlagkräftige Lösung, die Sie in Betracht ziehen sollten. MDR ist speziell darauf ausgelegt, fortschrittliche Bedrohungen zu erkennen, die bestehende Sicherheitskontrollen umgehen. Diese Bedrohungen sind komplexer Natur und die richtige Identifizierung erfordert oft die Korrelation verdächtiger Verhaltensweisen aus vielen verschiedenen Blickwinkeln.

Eine effektive MDR-Lösung sollte die Geschäftsauswirkungen berücksichtigen sowie auf Risiken und Vermögenswerte fokussieren. Die Lösung sollte darüber hinaus den Stand der Unternehmenssicherheit rapportieren, nachverfolgen und die Widerstandsfähigkeit kontinuierlich verbessern – statt «laute» Security-Events und Produkte hervorzubringen.

Die Zuordnung von MDR in dem Framework, die sogenannte «Cyber Kill Chain», hilft dabei, den Lärm zu destillieren, den Incident-Response-Prozess zu strukturieren und einen Rahmen für die Bewertung der Wirksamkeit der MDR-Lösung zu bieten.

Die ursprünglich von Lockheed Martin etablierte und von Organisationen wie MITRE weiterentwickelte Cyber Kill Chain (siehe Abbildung 1), zeigt die Vorgehensweise der Eindringlinge auf. Die Kill Chain umfasst mehrere Phasen und eröffnet Transparenz auf Taktiken, Techniken und Verfahren der Gegner.

Eine wirksame MDR-Lösung bietet Transparenz auf der Cyber Kill Chain. Bedrohungen werden z.B. in der Delivery- oder Exploitation-Phase erkannt mittels E-Mail-Überwachung auf Binärdateien an Endnutzer.



Abbildung 1: Die Cyber Kill Chain, beginnend mit der Erkundung und der Etablierung im Netzwerk, endend mit der Exfiltration oder anderem. Eine gute MDR-Lösung bietet Erkennung an mehreren Stationen.

Letztendlich wird eine wirksame MDR-Lösung über Fähigkeiten verfügen, die sowohl passiv (z. B. Identifizierung von Informationen, die von IP-Adressen, Domänen, sozialen Netzwerken usw. gesammelt werden) als auch aktiv sind (z. B. offensive Massnahmen, die in einem Angriffsprozess eingesetzt werden). Die Lösung sollte auch in der Lage sein, Protokolle aus mehreren Datenquellen zu verarbeiten, die mit bestimmten Ereignissen in der Kill Chain korreliert werden können.

Wenn Sie einen potenziellen MDR-Partner in Betracht ziehen, sollten Sie sich fragen, wie effektiv die Lösung wirklich ist und wie die Erkennung von Bedrohungen in der Kill Chain stattfindet. Die Reaktionsfähigkeit und wie der Anbieter bei Vorfällen mit Ihnen zusammenarbeitet, ist matchentscheidend. Mit anderen Worten: Wie hilft der Anbieter Ihnen, das Risiko zu minimieren?

Die richtige Implementierung einer MDR-Lösung

Der Implementierung einer MDR-Lösung sollte eine ordnungsgemäße Analyse der Geschäftsrisiken vorausgehen. Dies beinhaltet auch die Untersuchung auf die Fähigkeit der Risikominderung der Organisation durch interne Mitarbeiter oder mit Hilfe eines Anbieters. Wir haben sechs Schritte skizziert, die jedes Unternehmen berücksichtigen sollte, bevor es sich für einen Partner entscheidet und eine Lösung implementiert:

1 Schritt 1: Einschätzen

- Untersuchen Sie die aktuellen Incident Response Prozesse Ihres Unternehmens, die Netzwerkarchitektur und Standorte mit kritischen Gütern und Mitarbeitern.
- Bewerten Sie das aktuelle Geschäftsrisiko Ihres Unternehmens anhand des Gefahren- und Chancenmodells, das weiter oben in diesem Leitfaden vorgestellt wurde (oder eines ähnlichen Frameworks).
- Berücksichtigen Sie die verfügbaren internen Ressourcen und das Budget, das für Incident Response in Ihrem Unternehmen benötigt wird.

2 Schritt 2: Identifizieren

- Identifizieren Sie die Schwachstellen in der Cybersecurity Ihres Unternehmens.
- Achten Sie besonders auf Bereiche, die Ihre Angriffsfläche exponentiell vergrößern können, wie z. B. Endpunkte und Konfigurationen in virtuellen und remoten Infrastrukturen sowie Richtlinien und Verfahren in Bezug auf IAM, Datenschutz und -sicherheit und Sicherheitsabläufe.



3 Schritt 3: Bestimmen

- Prüfen Sie, ob Ihr Unternehmen in der Lage ist, selbständig auf Vorfälle zu reagieren.
- Berücksichtigen Sie internes Fachwissen und den TCO im Zuge des Aufbaus Ihres Sicherheitsteams.
- Verwenden Sie KPIs wie *Time-to-Detect* und *Time-to-Respond*, um zu bestimmen, wie effektiv Ihre Sicherheitsabläufe sein werden.
- Berücksichtigen Sie praktische Überlegungen, wie z. B. das Schichtmanagement für eine 24x7-Überwachung (was in der Regel ein Team von 8 bis 10 Personen erfordert) und die Verwaltung der kritischen Anlagen Ihres Unternehmens.

4 Schritt 4: Evaluieren

- Bewerten Sie die Fähigkeiten des Partners mit Schwerpunkt auf PPT (Personen, Prozesse, Tools), einschliesslich der Qualität der Mitarbeiter des Anbieters, der Sicherheitstechnologien, des Trainings, des Schichtmanagements, der Prozesse und Verfahren für Eskalation, Forensik und Analysen.
- Vergewissern Sie sich, dass Ihr ausgewählter Anbieter 24x7 Managed Detection and Response mit kollaborativem Operations anbietet und gut mit Ihrem bestehenden Team zusammenarbeitet.
- Entscheiden Sie sich für cloudbasierte Plattformen, die Automatisierung mit menschlichem Fachwissen kombinieren sowie Reporting und Alerts auf Basis von Playbooks, Use Cases und kontinuierlicher Überwachung verbinden.
- Berücksichtigen Sie die Fähigkeit des Anbieters, sich in Ihr bestehendes Sicherheitssystem zu integrieren.



5 Schritt 5: Planen

- Entwickeln Sie gemeinsam mit Ihrem Anbieter eine Roadmap, die Governance und Best Practices für die Einhaltung gesetzlicher Vorschriften beinhaltet.
- Entwickeln Sie Prozesse und Verfahren, die empfohlene Reaktionsmassnahmen beinhalten, um die Isolierung von echten Vorfällen sicherzustellen. Ihr MDR-Partner sollte flexibel sein, damit Sie den Umfang des Vorfall-Supports, resp. der Incident-Bearbeitung, definieren können.
- Legen Sie die Ansprechpartner für das Schichtmanagement fest und definieren Sie gemeinsame Aktionen zwischen den Teams.

6 Schritt 6: Implementieren

Arbeiten Sie mit Ihrem neuen MDR-Partner für folgendes zusammen:

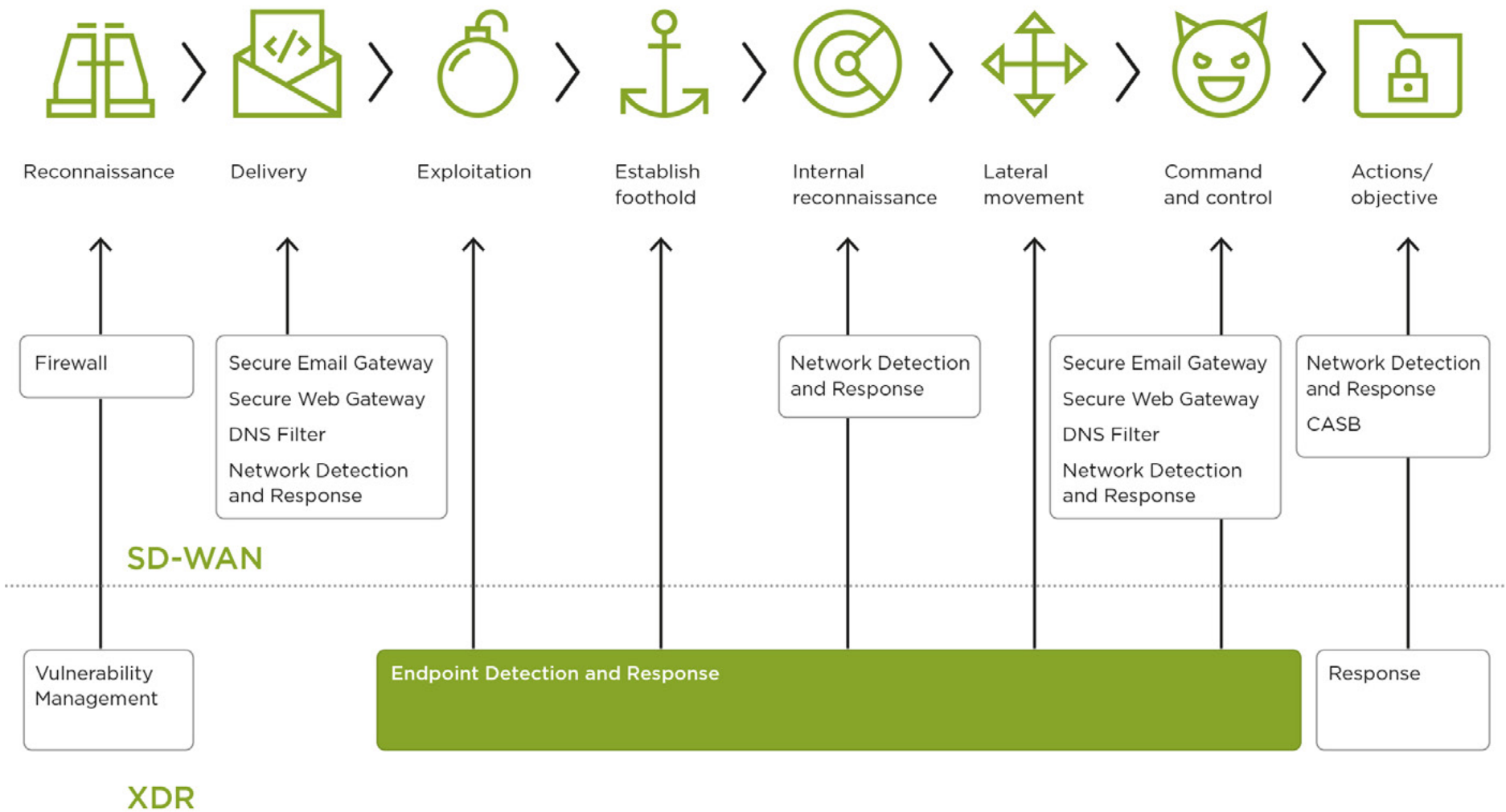
- Erstellen Sie eine Baseline Ihrer Umgebung und beheben Sie alle kritischen Mängel.
- Erfassen Sie kritische Anlagen und definieren Sie einen Plan für die Reaktion auf Vorfälle.
- Bestimmen Sie sicherheitsrelevante Felder in Log- und Datenquellen und definieren Sie Standardwarnungen.
- Integrieren Sie verschiedene Security-Stack-Technologien (falls zutreffend).
- Messen Sie die Response und sorgen Sie für eine kontinuierliche Verbesserung.

Fazit

Unternehmen müssen leider damit rechnen, dass Cybersecurity-Angriffe von Jahr zu Jahr weiter zunehmen. Neue Bedrohungen wie ML/AI-Poisoning-Angriffe, immer raffiniertere Ransomware und Zero-Day-Exploits sowie anhaltende Insider-Threats werden die IT- und Sicherheitsverantwortlichen weiterhin vor neue und gewaltige Herausforderungen stellen.

MDR-Lösungen können Ihrem Unternehmen dabei helfen, diese wachsenden Bedrohungen zu bewältigen und interne Hindernisse zu adressieren, wie z. B. hohe Kosten für Sicherheitstechnologien und zu wenig Zeit und engagierte Mitarbeiter, um sie zu bedienen. Erstklassige MDR-Lösungen kombinieren fortschrittliche Technologien auf der Präventionsschicht mit kontinuierlicher Überwachung und Erkennung. Dies ermöglicht die Beschaffung von Präventionsinformationen sowie fundierte Analysen und Reaktionen für Unternehmensnetzwerke, Endpunkte und die Cloud.

Bei Open Systems geht die **MDR-Lösung** einen Schritt weiter und bietet eine optionale Integration mit unserer Secure Access Service Edge (SASE)-Lösung. Diese Komplettlösung ermöglicht es uns, Bedrohungen präzise zu erkennen und Vorfälle über mehrere Punkte einzudämmen, die Netzwerk, Infrastruktur und cloudbasierte Technologien und Kontrollen umfassen.



Unsere MDR-Lösung ist an das MITRE ATT&CK®-Framework gebunden und lässt sich nahtlos in das cloudbasierte, KI-fähige Azure Sentinel SIEM von Microsoft integrieren, damit Unternehmen von dessen Skalierbarkeit, Erkennungsfunktionen und Community-Vorteilen profitieren können.

open
systems

Es ist an der Zeit, sich mit MDR zu befassen. Oder anders ausgedrückt: Hoffnung ist keine Strategie, Vorbereitung hingegen schon.

Wenn Sie mehr über die MDR-Lösungen von Open Systems erfahren möchten, [kontaktieren Sie uns noch heute.](#)

¹SC Media, "**COVID-19 accounts for most 2020 cyberattacks**," 22. Juli 2020

²Ibid.

³Flexera, **2020 State of the Cloud Report**

⁴Electronic Frontier Foundation (EFF), "**Surveillance Self-Defense/Your Security Plan**," Zugriffen am 24. Oktober 2020

⁵Microsoft, "**Managing cybersecurity like a business risk: 1. Teil – Modeling opportunities and threats**," 28. Mai 2020



Open Systems ist Pionier im Bereich Secure Access Service Edge (SASE), der Unternehmen eine flexible Skalierung mittels sicheren, cloudbasierten und vollumfänglich betriebenen Verbindungen ermöglicht. Open Systems kombiniert Netzwerk und Sicherheit und stellt Secure SD-WAN und MDR Services bereit, für Ihr zukunftsfähiges Unternehmen.

Weitere Informationen unter open-systems.com.