baseVISION

Entlastung interner Ressourcen mit baseVISIONs Managed Extended Detection and Response Service

Case Study MCH Group

Wer ist MCH Group?

Die MCH Group mit Sitz in Basel ist ein international tätiges Event-Marketing-Unternehmen mit einem umfassenden Dienstleistungsnetzwerk. Sie veranstaltet rund 30 Community-Plattformen im In- und Ausland, darunter die Art Basel, die Swissbau und die Giardina. Das Geschäftsfeld Live Marketing Solutions mit den Marken MCH Global, MC2 und Expomobilia bietet umfassende Erlebnismarketing-Lösungen von der Strategie über die Kreation bis zur Umsetzung. Die MCH Group betreibt zudem das Messe- und Kongresszentrum Basel und die Messe Zürich.

Die Vision

- 24/7 Security Monitoring
- Erhöhung der Erkennung von Gefahren
- Konzentrierte Sicherheitsexpertise nutzen

Ausgangslage

Die MCH Group hat einen strategischen Plan zur Verbesserung ihrer internen Überwachungs-, Erkennungs- und Reaktionsfähigkeit bei Sicherheitsvorfällen umgesetzt. Dazu gehörte die Integration eines professionellen Security Operation Centers, welches rund um die Uhr externe Unterstützung bietet und eine robuste und reaktionsfähige Sicherheitsinfrastruktur gewährleistet. Darüber hinaus musste die Sicherheitsabdeckung auf zusätzliche Cloud- und On-Premise-Ressourcen ausgeweitet werden. Diese Herausforderungen verdeutlichten, wie wichtig es ist, Ressourcenbeschränkungen zu beseitigen und die Sicherheitsmassnahmen zu verbessern, um den sich entwickelnden Bedrohungen zu begegnen.

«Da wir die IT-Sicherheit der MCH Group laufend weiterentwickeln und verbessern müssen, sahen wir uns mit der Notwendigkeit konfrontiert, unsere Infrastruktur in der Cloud und on-premise rund um die Uhr zu überwachen und bei Vorfällen schnell reagieren zu können. Die hohe Professionalität und Expertise von baseVISION sowie unser Wunsch, in der Microsoft Produktlinie zu bleiben, haben uns überzeugt, uns für baseVISION zu entscheiden.»

Rachid Dahjaoui
Head of Information Security – MCH Group AG

Über baseVISION AG

baseVISION ist ISO27001 zertifiziert und ist Mitglied der Microsoft Intelligent Security Association.

ISO/IEC 27001:2013
BUREAU VERITAS
Certification
UKAS MANAGEMENT SYSTEMS 0008

Microsoft Intelligent Security Association

Microsoft Security

Microsoft Verified Managed XDR Solution

Einfacher baseVISION MXDR Premium Onboarding-Prozess

baseVISION nutzt einen einfachen Onboarding-Prozess, um Security Operations Services innerhalb weniger Wochen starten zu können.

1. Vorbereitung: Der erste Schritt des SOC-Onboardings ist eine gründliche Vorbereitung. Sie umfasst die Bereitstellung von Ressourcen und die Planung der anstehenden Sicherheitsmassnahmen. Ein wichtiger Teil dieser Phase ist das Kick-off-Meeting, in dem Rollen, Erwartungen und Zeitpläne besprochen und geklärt werden. Mit Hilfe des Kundenfragebogens werden wichtige Informationen über die spezifischen Sicherheitsanforderungen des Unternehmens gesammelt. Darüber hinaus wird durch eine Überprüfung der Voraussetzungen sichergestellt, dass die Umgebung des Kunden für den Onboarding-Prozess bereit ist.

2. Onboarding: In der Onboarding-Phase liegt der Schwerpunkt auf technischen Aspekten. Das SOC-Team und der Kunde koordinieren die technischen Konfigurationsanforderungen. Die technische Implementierung des Onboardings umfasst den Einsatz von Sicherheitstools und -konfigurationen, die auf den wirksamen Schutz der Kundenumgebung zugeschnitten sind.

3. Kommunikation: Effektive Kommunikation ist für eine erfolgreiche Partnerschaft von grundlegender Bedeutung. In dieser Phase werden sichere Kommunikationskanäle und die Anforderungen an die Berichterstattung festgelegt. Regelmässige Statusberichte werden erstellt, um beide Parteien über den Fortschritt des Integrationsprozesses auf dem Laufenden zu halten. Darüber hinaus finden in dieser Phase Diskussionen und Abstimmungen über identifizierte Optimierungsmöglichkeiten statt.

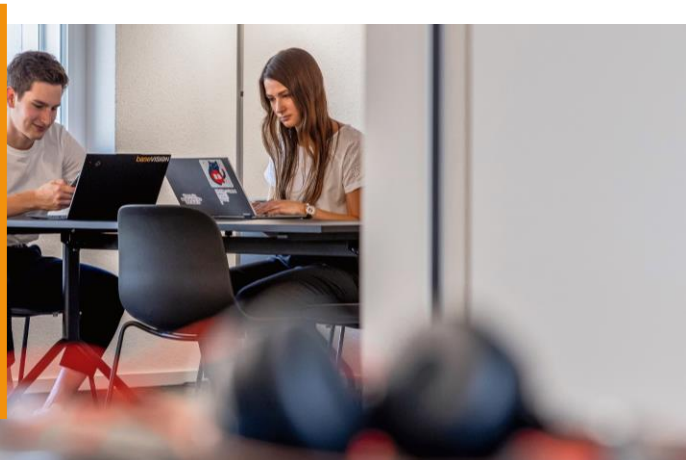
4. Optimierung: Optimierungsbemühungen zielen auf die Feinabstimmung von Sicherheitsprozessen ab, um deren Effizienz zu erhöhen. Der Schwerpunkt liegt dabei auf der Beseitigung bekannter falsch positiver und negativer Ergebnisse. Validierte Optimierungs- und Automatisierungsmassnahmen werden implementiert, um die Erkennung von Bedrohungen und die Reaktionsfähigkeit zu verbessern. Spezifische Reaktionsmassnahmen werden in Übereinstimmung mit den Präferenzen des Kunden und den validierten Optimierungsmassnahmen eingerichtet.

5. Betrieb: Mit dem Übergang in die Live-Betriebsphase des SOC werden die Sicherheitsdienste offiziell aufgenommen und die Service Level Agreements (SLAs) treten in Kraft. Regelmässige SOC-Berichte und Besprechungen zu Sicherheitsvorfällen werden organisiert, um Transparenz und Koordination zwischen beiden Parteien zu gewährleisten. Kontinuierliche Verbesserungsmassnahmen werden eingeleitet, um sich an die sich ändernden Bedrohungen und Herausforderungen anzupassen und eine kontinuierliche Sicherheitseffektivität zu gewährleisten.

Diese fünf Schritte bilden zusammen einen strukturierten SOC-Onboarding-Prozess und haben dazu beigetragen, die Sicherheitslage der MCH Group zu verbessern.

«Wir sind von der Lösung überzeugt! Die Zusammenarbeit mit den Ansprechpartnern von baseVISION verlief reibungslos und hat unsere Erwartungen übertroffen. Besonders beeindruckt hat uns die hervorragende Qualität und das hohe Engagement während des Onboarding-Prozesses und im laufenden Betrieb. Die Zusammenarbeit mit baseVISION war zweifellos ein Gewinn für uns.»

Christian Boos
Head Corporate IT – MCH Group AG



Effizienter 24/7 Schutz

Ein 24/7-Betrieb ist unabdingbar, da Angriffe jederzeit erfolgen können und in den meisten Fällen eine schnelle Reaktion erforderlich ist. Unser MXDR Premium Service entlastet das Sicherheitsteam der MCH Group und überwacht die Umgebung kontinuierlich. Das baseVISION Team kann bis zu 99% der Vorfälle selbständig und ohne Kundeninteraktion analysieren, bearbeiten und abschliessen.

«Die offene und transparente Kommunikation während des Onboarding-Prozesses hat eine effiziente Zusammenarbeit ermöglicht und zu einer besseren Sichtbarkeit von Sicherheitsvorfällen geführt. Es ist inspirierend, das starke Engagement aller Experten zu sehen, die ständig an der Verbesserung der Erkennung, des Schutzes und der Reaktion auf aktuelle und neue Bedrohungen arbeiten.»

Jürg Meier
Lead SOC at baseVISION AG

Eines der Ziele der MCH Group war es, die Erkennungsabdeckung durch die Nutzung der umfassenden Fähigkeiten der Microsoft 365 Defender Plattform zu verbessern, mit der zusätzlichen Flexibilität, die Datenquellen in Zukunft zu erweitern. Das baseVISION MXDR Premium Paket bietet darüber hinaus Zugriff auf das baseVISION Detection Repository, das über 100 zusätzliche Erkennungen in die Kundenumgebung integriert. Dieses Repository wird von den baseVISION Sicherheitsexperten gepflegt und kontinuierlich um aktuelle Bedrohungen erweitert.

Neben der Erweiterung der Erkennungsfunktionen ist es wichtig, die Aufgaben des Sicherheitsbetriebs kontinuierlich zu optimieren und zu automatisieren. Dies ist im baseVISION-Angebot vollständig enthalten und wir überprüfen kontinuierlich die Automatisierung von Sicherheitsvorfällen, um die Effizienz der Bearbeitung durch Automatisierung und Anreicherung zu erhöhen. Auf diese Weise werden mehr als 60 % der erkannten Vorfälle innerhalb weniger Minuten automatisch bearbeitet.

Die meistgenutzten Microsoft Technologien

- ✓ Microsoft 365 Defender
- ✓ Microsoft Entra ID Protection
- ✓ Microsoft Sentinel

«Wir sind mit dem effizienten Integrationsprozess der baseVISION AG sehr zufrieden. Die Integration hat uns erheblich entlastet, so dass wir uns auf andere Aktivitäten konzentrieren können, mit der Gewissheit, dass unsere Erkennungsfunktionen robust sind und unsere Sicherheitsprozesse kontinuierlich optimiert werden. Die professionelle und schnelle Arbeitsweise von baseVISION hat unsere Fähigkeit, mit aktuellen Bedrohungen umzugehen, deutlich verbessert, so dass wir uns gut unterstützt und sicher fühlen. Es ist beruhigend zu wissen, dass ein Grossteil der Vorfälle dank der fortschrittlichen Automatisierungs- und Anreicherungsprozesse nun schnell und automatisch bearbeitet wird.»

Rachid Dahjaoui
Head of Information Security – MCH Group AG

Zusammenfassung

Der SOC Onboarding Prozess für die MCH Group wurde von den Zielen der MCH Group getrieben, eine 24/7 Sicherheitsüberwachung zu erreichen, die Detektionsabdeckung zu verbessern und von spezialisierter Sicherheitsexpertise zu profitieren. Diese Ziele wurden durch die Implementierung des Managed Service "baseVISION MXDR Premium", der eine Sicherheitsüberwachung rund um die Uhr gewährleistet, erfolgreich umgesetzt. Die Erkennungsabdeckung wurde durch die Einführung zusätzlicher Signale in Microsoft Sentinel und die Bereitstellung von Erkennungen aus dem baseVISION Detection Repository deutlich verbessert. Darüber hinaus profitiert die MCH Group nun von der Expertise der baseVISION-Sicherheitsexperten, die Vorfälle aktiv analysieren, was den Bedarf an Kundeninteraktion reduziert und die allgemeine Sicherheitseffektivität erhöht.

baseVISION AG
Unterführungsstrasse 25
4600 Olten

info@basevision.ch

+41 62 291 30 00

Kontaktieren Sie uns

baseVISION
SECURE & MODERN ENDPOINT MANAGEMENT

Wir machen Ihren IT-Arbeitsplatz fit für die Zukunft - modern, flexibel und sicher.

Durch unsere fokussierte Unternehmensstrategie verbinden wir Expertenwissen mit praktischer Erfahrung. Auf dem Weg zu modernen IT-Arbeitsplätzen und dem einfachen und sicheren Betrieb Ihrer Endgeräte können Sie sich auf unsere Kompetenz als Berater, Integrator und Coach verlassen. Als junges Unternehmen sind wir stolz darauf, dass wir für unsere innovativen und erfolgreichen Projekte bereits viermal mit dem Microsoft Partner of the Year Award ausgezeichnet wurden.