Ontinue

CUSTOMER STORY

Ontinue stärkt die Sicherheits-DNA von Metrohm

Präzision ist seit jeher eine Schweizer Tugend. So ist es nicht verwunderlich, dass sich die Metrohm AG in ihrer 80-jährigen Firmengeschichte zu einem der weltweit größten Hersteller von Hochpräzisionsinstrumenten für die chemische Analytik entwickelt hat. Neben, also Geräten für die quantitative, entwickelt, produziert und vertreibt der Messtechnikexperte zahlreiche weitere Laborinstrumente und -technologien, darunter Ionenchromatographen sowie Raman- und Nahinfrarot- Spektrometer. Zum Produktportfolio gehört zudem die Software „OMNIS“ für die, mit der Labore ihre Produktivität und Effizienz steigern können. Das 1943 in Herisau gegründete Traditionsunternehmen beschäftigt heute rund 3.300 Mitarbeiter und betreibt über 100 eigene Standorte in 45 Ländern. Durch sein umfangreiches Partnernetzwerk ist die Metrohm AG somit in insgesamt mehr als 80 Ländern vertreten.

Das stete Wachstum des Unternehmens machte auch vor der technologischen Infrastruktur nicht Halt: Die Anzahl an Workplace Clients stieg und das interne Netzwerk vergrößerte sich mit jedem neuen Entwicklungs-, Produktions- und Vertriebsstandort. Mittlerweile betreuen die über 30 IT-Experten der Metrohm AG rund 3.300 Work-place Clients und drei Datenzentren in Eigenregie. Hinzu kommen georedundante Rechenzentren von Partnern sowie

Metrohm

Motivators

- Ausbau des Security-First-Ansatzes
- Proaktiveres und automatisiertes Ergreifen von Maßnahmen gegen Cyberbedrohungen
- Stärkung der Sicherheits DNA über die gesamte IT-Infrastruktur hinweg
- 24/7 Monitoring sämtlicher Endpunkte und Assets
- Aufbau eines Security Operations Center für First Response, Threat Intelligence und Threat Hunting
- Rationalisiertes Reporting, um aus Security Incidents zu lernen und Mitarbeiter für Sicherheitsthemen zu sensibilisieren

Lösung

- Zusammenarbeit im Bereich klassicher SOC Tätigkeiten mit Ontinue, inklusive Threat Intelligence, Threat Hunting, Data Science, Detection Engineering und automatisierter Threat Detection
- Implementierung von Microsoft Defender als EDR-Lösung für Clients und Server
- Inbetriebnahme von Microsoft Sentinel als SIEM-Plattform

Ergebnis

- Rund um die Uhr Monitoring der IT-Infrastruktur
- Voll funktionsfähiges SOC
- Visibilität über sämtliche Assets, von den Clients über die Rechenzentren bis hin zur Multi-Cloud-Umgebung
- Deutliche Entlastung des unternehmensinternen IT Teams
- Niedrigere Anzahl schwerer und kritischer Security Incidents
- Präventive und proaktive Verteidigung gegen Cyberthreats
- Nur wenige von über 1.000.000 Alerts erreichen das Sicherheitsteam der Metrohm AG

Über die Metrohm AG

Die Metrohm AG ist einer der weltweit Hersteller von Hochpräzisionsinstrumenten für die chemische Analytik und wurde 1943 Ingenieur Bertold Suhner im Schweizerischen Herisau gegründet. Heute hat das Unternehmen über 100 eigene Standorte in 45 Ländern und ist in 80 Ländern mit Tochtergesellschaften bezie-hungsweise Vertriebspartnern präsent.

der Bezug von Public-Multi-Cloud-Services. Die internationale Bedrohungslage durch Hackerattacken und die enge Personaldecke hatte das Unternehmen schon vor einiger Zeit dazu bewegt, den Betrieb und Schutz des SD-WAN zu externalisieren.

„Unser Credo heißt: Security First", erklärt Zeno Stämmer, Chief Information Officer bei der Metrohm AG. „Die Sicherheits-DNA der Metrohm AG fußt auf dem festen Vorsatz, überall und an jeder Stelle der IT-Infrastruktur und -Services entsprechende Maßnahmen zu bedenken und zu ergreifen. Dazu ist es nicht nur notwendig, das Netzwerk, die Rechenzentren und die Clients rund um die Uhr im Auge zu behalten, sondern auch ein möglichst umfassendes Bild der Bedrohungslandschaft zu haben. Unsere unternehmensinternen Mitarbeiterressourcen und Experten Know-how reichten dafür nicht aus. Was uns effektiv fehlte, war ein Security Operations Center, das uns helfen würde, unsere Lücken im Bereich Detection and Response zu schließen und die dringend notwendige Visibilität über alle IT-Bereiche herzustellen."

Ein eigenes Security Operations Center (SOC) aufzubauen, kam nicht in Frage: Die ohnehin knappen Mitarbeiterressourcen noch weiter zu strecken, hätte massive Einschränkungen im IT-Betrieb und entsprechenden Projekten bedeutet. Zudem ist teamintern zu wenig Erfahrung im Aufgabenspektrum von Security Advisors und Threat Huntern vorhanden. Aus diesem Grund entschied sich die Metrohm AG, wie schon beim Aufbau, Betrieb und Schutz des SD-WAN, für die Zusammenarbeit mit einem vertrauenswürdigen Partner. Zeno Stämmer fasst diesen Entschluss wie folgt zusammen: „Neben einem dedizierten Security Team sind Systeme zur Erkennung von Cyberthreats und zur Automatisierung von Abwehrmaßnahmen der absolute Vorteil von SOCs. Unternehmen benötigen zudem entsprechende Software, die sie betreiben müssen, wir bei Metrohm sind dafür allerdings leider nicht geeignet aufgestellt."

> **„ Wir haben mehrere Anbieter auf Herz und Nieren überprüft und ihre spezifischen Offerings mit unserem Anforderungsprofil abgeglichen. Ontinue konnte sich im Wettbewerb behaupten"**
>
> Zeno Stämmer
> **Chief Information Officer**
> Metrohm AG

Eine einfache Entscheidung

Das Anforderungsprofil für einen geeigneten MXDR (Managed Extended Detection and Response) Serviceanbieter war schnell erstellt. Zum einen war es ein Vorteil, wenn der Anbieter auf Microsoft Technologien spezialisiert ist, da die Metrohm AG in grossen Stücken auf Microsoft Technologie aufsetzt. Da der Microsoft Defender bereits an den Endpunkten eingesetzt wurde, lag es nahe, diese Software für die Endpoint Detection and Response (EDR) zu verwenden und einen Wechsel bei den Servern vorzunehmen. Gleichwohl überzeugte Zeno Stämmer, den CISO der Metrohm AG, und die IT-Architekten des Unternehmens gleichermaßen, Microsoft Sentinel als SIEM (Security Information and Event Management) -Lösung zum Tool Stack hinzufügen, um eine ganzheitliche Sicherheitsinfrastruktur aus einem Guss aufzubauen.

Der potenzielle MXDR Anbieter musste zudem über genügend Kapazitäten verfügen, um die große IT-Infrastruktur der Metrohm AG rund um die Uhr zu überwachen, sowie Threat Intelligence und Automatisierungsmechanismen als Teil des Servicepakets. Wie es von einem Unternehmen, für das Präzision an erster Stelle steht, nicht anders zu erwarten ist, gab es eine klar definierte Roadmap für die Evaluierung eines geeigneten SOC Anbieters. „Wir haben mehrere Anbieter auf Herz und Nieren überprüft und ihre spezifischen Offerings mit unserem Anforderungsprofil abgeglichen. Ontinue konnte sich im Wettbewerb behaupten", betont Zeno Stämmer. „Nach unseren guten Erfahrungen mit Open Systems, dem Unternehmen aus dem Ontinue hervorging, waren wir in dieser Hinsicht nicht überascht."

Nachdem die Entscheidung für den MXDR Service ION von Ontinue getroffen war, legte die Metrohm AG das nötige Software Fundament mit der Anschaffung von Microsoft E5 Security-Lizenzen und damit

des Microsoft Defender für sämtliche Endpunkte und Server des Unternehmens. Zudem nahmen Zeno Stämmer und sein Team Microsoft Sentinel in Betrieb. Ein Microsoft Teams Channel wurde als Kommunikationskanal für Absprachen zwischen dem SOC von Ontinue und dem IT-Team der Metrohm AG eingerichtet. Die Cyber Advisor des MXDR Experten übernehmen dabei die strategische Ausrichtung der Sicherheitsinfrastruktur und die Beratung, während die Cyber Defender operativ die Sicherheitslage checken und in akuten Gefahrensituationen als direkter Ansprechpartner rund um die Uhr in Sekundenschnelle Eingriffe vornehmen und erreichbar sind.

Security First in Aktion

Bereits sieben Tage nach Beginn der Zusammenarbeit erhöhte sich das Sicherheitsniveau deutlich. Erste Analysen durch das SOC von Ontinue ergaben ein viel deutlicheres Bild über die Bedrohungslandschaft und ermöglichten die ersten proaktiven Gegenmaßnahmen. Gleichzeitig konnte der MXDR Profi bereits einen großen Teil der zahlreichen nichtkritischen Sicherheitsvorfälle lösen, sodass das IT Team der Metrohm AG nun wieder genug Ressourcen hat, um sich selbst um schwerere Vorfälle zu kümmern. In Zahlen bedeutet das, dass Ontinue nur vier Events von mehr als einer Million an das Security Team von Zeno Stämmer weiterleiten muss. Mit Hilfe der EDR- und SIEM- Lösung von Microsoft kann Ontinue ein 24/7 Monitoring der IT-Infrastruktur gewährleisten, das ist besonders wichtig, da sich Cyberkriminelle selten an Geschäftszeiten halten, wie die Zahlen belegen: Mehr als ein Viertel der Angriffe auf die Metrohm AG fanden im letzten halben Jahr an Wochenenden statt. Die Sicherheitsinfrastruktur kommt aber auch Ontinue selbst zugute, denn weniger als ein Drittel der einlaufenden Incidents wird überhaupt erst zu einem Ticket.

„Vor unserer Zusammenarbeit mit Ontinue waren wir vor allem eines: reaktiv. Weder hatten wir die Mittel, noch die Ressourcen, um sämtliche Angriffstypen zu kennen und ihnen präventiv entgegenzuwirken. Das hat sich nun komplett geändert“, fasst Zeno Stämmer die positive Entwicklung zusammen. Ontinue hilft der Metrohm AG nicht nur bei der First Response und der Triage der Vorfälle. Insbesondere auch die Bereiche Threat Hunting und Threat Intelligence werden vom Service des MXDR Profis abgedeckt: Die Experten von Ontinue suchen gemeinsam mit Zeno Stämmers Team nach möglichen Schwachpunkten und helfen ihm dabei, sie zu schließen. Gleichzeitig teilt das SOC seine Erkenntnisse aus ihren Threat-Intelligence Bemühungen, um die Sicherheits DNA der Metrohm gegen potenzielle und zukünftige Bedrohungen zu impfen.

„Ich bin mir nicht sicher, was uns ohne Managed SOC alles hätte passieren können. Während der ersten drei Monate hatten wir mehrere Dutzend High Severity Security Incidents, die wir abwehren konnten, bereits einer dieser Vorfälle hätte bei Erfolg Kosten in Höhe mehrerer Hundertausend Franken verursachen können“, berichtet Zeno Stämmer.

> **„ Seit der Zusammenarbeit mit Ontinue konnten wir mehrere Dutzend High Severity Incidents rechtzeitig erkennen. Wäre nur ein einziger erfolgreich gewesen, hätte er Kosten in Höhe mehrerer Hundertausend Franken verursachen können. Kritische Vorfälle gibt es seit mehreren Monaten keine mehr, was uns in unserer Entscheidung, Ontinue als SOC- und MXDR- Provider zu engagieren, mehr als bestätigt.“**
>
> Zeno Stämmer
> **Chief Information Officer**
> Metrohm AG

Ontinue

Über Ontinue

Ontinue, der Experte für KI-gestützte Managed Extended Detection and Response (MXDR), ist ein rund um die Uhr verfügbarer Sicherheitspartner mit Hauptsitz in Zürich. Um die IT-Umgebungen seiner Kunden durchgehend zu schützen, ihren Sicherheitsstatus zu bewerten und kontinuierlich zu verbessern, kombiniert Ontinue KI-gesteuerte Automatisierung und menschliches Fachwissen mit dem Microsoft-Sicherheits-Produktportfolio. Durch die intelligente, Cloud-basierte Nonstop SecOps-Plattform reicht Ontinues Schutz vor Cyberattacken weit über die grundlegenden Detection- und Response-Services hinaus.

Weitere Informationen gibt es unter www.ontinue.com