

Curaden schützt sich mit MDR von Netcloud.

- MDR – Managed Detection and Response Service
- Security Operations Center SOC
- Vulnerability Management IP-Scan mit Rapid7

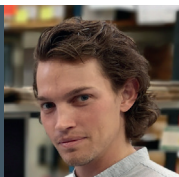
Vorreiterin in der Mundgesundheit

Die Curaden AG ist ein Schweizer Traditionsunternehmen im Bereich Mundhygiene, das auf 70 Jahre Erfahrungsschatz zurückblickt und ihre Produkte auf der ganzen Welt verkauft. In Zusammenarbeit mit Fachleuten aus Forschung, Lehre und Praxis entwickelt Curaden Mundhygieneprodukte, die möglichst wirksam und schonend sind. Das Unternehmen setzt sich seit je für eine ganzheitliche Mundgesundheit ein. So verkaufen Sie nicht nur physische Produkte, sondern bieten ebenfalls Weiterbildungen für Fachleute und Zahnärzte an. Im Fokus steht dabei immer die Prävention in der oralen Gesundheit.

Mit Netcloud Cyberbedrohungen abwehren

Prävention ist jedoch nicht nur in der Mundgesundheit ein Muss: Auch in der IT-Sicherheit soll vorgesorgt sein. Um ihre Security-Maturität zu erhöhen, führte die Curaden NIST-Assessments durch und identifizierte dabei mehrere Schwachstellen. Auf dieser Grundlage entwickelte Curaden eine IT-Security-Strategie und fragte im Rahmen dessen Netcloud für eine Zusammenarbeit im Cyber Defence Bereich an.

Für eine hochprofessionelle Verteidigung der Kunden IT-Infrastruktur offerierte Netcloud ihren Managed Detection & Response Service (MDR), welcher auf Cortex XDR Pro von Palo Alto Networks basiert. Der Aufbau auf dieser Plattform lässt sich nahtlos ins Cyber Defence Center (CDC) der Netcloud integrieren und garantiert somit einen höchstmöglichen Schutz der Kunden-Assets sowie volle Visibilität. Das CDC der Netcloud fungiert als Security Operations Center (SOC) und überwacht die Bedrohungsmeldungen von Cortex XDR Pro. Alle Meldungen der Endpoints werden registriert, automatisch analysiert und bei Bedarf von einem Netcloud Security Analyst manuell bearbeitet. Die Zusammenarbeit von Technologie und Mensch ermöglicht es, auch grosse Datenmengen effizient und bei höchsten Sicherheitsstandards zu analysieren.



Thomas Husi
Head of IT

«Mit Netcloud haben wir einen Partner gefunden, der unsere Bedürfnisse kennt und uns im Bereich IT-Security voranbringt. Ihr umfassendes Know-how hat es uns ermöglicht, unsere Security-Maturität erheblich zu verbessern. Cyber Security ist ein kontinuierlicher Prozess, da sich Bedrohungen stetig weiterentwickeln. Mit Netcloud an unserer Seite blicke ich zuversichtlich in die Zukunft und freue mich auf die weitere erfolgreiche Zusammenarbeit.»

Vorteile des Managed Detection & Response Service von Netcloud

- *Threat Management und Vulnerability Management decken proaktiv Bedrohungen und Schwachstellen auf, bevor ein Schaden entsteht.*
- *Curaden ist durch die monatlichen Security Reports und Service Meetings stets auf dem aktuellen Stand und kann bei Bedarf einfach und effizient Verbesserungen einleiten.*
- *Die Integration des MDR Services in bestehende Sicherheitssysteme steigert die Effizienz der Sicherheitsoperationen erheblich.*
- *Die Mitarbeitenden des Unternehmens werden entlastet und können sich auf die für sie relevanten Geschäfte konzentrieren.*

Die technische Umsetzung

Für die Implementierung des MDR-Services mit Cortex XDR Pro von Palo Alto Networks wurde zuerst eine Bestandsaufnahme der IT-Infrastruktur gemacht und die Integration in die bestehenden Systeme geplant. Danach wurden Pilotgruppen definiert und die XDR-Agents auf diesen Endpunkten und Servern ausgerollt. Es folgte der Rollout auf alle restlichen Endpunkte und Server. Die XDR-Agents wurden auf allen gängigen Betriebssystemen installiert: Windows, macOS, Linux und iOS. Anschliessend wurde eine umfassende Schulung des IT-Sicherheitspersonals durchgeführt. Das Netcloud CDC überwacht die Events aus dem Cortex XDR 24/7. Über eine API-Schnittstelle werden die Events ins zentrale SOAR (Cortex XSOAR) der Netcloud übertragen. Um die Effizienz und Reaktionsgeschwindigkeit zu erhöhen, werden im XSOAR Automatisierungs-Playbooks eingesetzt und stetig an die Kundenbedürfnisse angepasst. Im Betrieb werden die Daten aus den Events systematisch analysiert, um wiederkehrende False Positives zu identifizieren.

Hauptziel des MDR Services ist es, die Erkennungszeit von Bedrohungen zu verringern und Gefahren möglichst frühzeitig zu identifizieren, um einen Cyber Incident zu verhindern. Mit Erfolg: Seit der Implementierung konnte die Curaden AG eine massive Verbesserung der Bedrohungserkennungsrate und eine Reduzierung der Reaktionszeiten auf Sicherheitsvorfälle verzeichnen.

Schwachstellen beheben

Im Zuge dessen erkannte man nicht nur die Wichtigkeit von Cyberabwehr, sondern auch die Bedeutung der Erkennung und Behebung von Schwachstellen. Die Basis einer effektiven Sicherheitslösung ist Visibilität. Mit Cortex XDR Pro weiss Curaden stets, was in ihrer IT-Umgebung vor sich geht und wo Bedrohungen auftreten. Um ihre Security-Maturität auf den «next level» zu bringen, setzt Curaden zusätzlich auf ein Vulnerability Management, welches mit den Services der Netcloud Security Consultants flankiert wird. Damit werden Schwachstellen identifiziert und behoben, bevor sie ausgenutzt werden können. Die Netcloud-Experten beraten Curaden bei der Priorisierung und Behebung der Schwachstellen, sodass stets klar ist, wo und wie zuerst angesetzt werden muss. Thomas Husi, Head of IT, resümiert: «Die Netcloud hat uns im ganzen Prozess hervorragend unterstützt. Nicht nur die Expertise ist auf einem sehr hohen Niveau, auch kulturell passt Netcloud perfekt zu uns. Wir haben uns als Kunde stets sehr geschätzt gefühlt und tun es immer noch.»

Mehr über unsere Success Stories erfahren Sie

unter +41 58 344 12 12, sales@netcloud.ch oder auf unserer Website

www.netcloud.ch

Winterthur: Wülflingerstrasse 5, 8472 Seuzach

Bern: Carba Center, Waldeggstrasse 37, 3097 Liebefeld

Basel: Schützengraben 21, 4051 Basel