



Mehr Sicherheit durch ein KI-gestütztes SOC

Waldaschaff Automotive stärkt seine Cyberresilienz mit Arctic Wolf. enthus hat die Einführung der neuen Security Operations-Plattform vorbereitet und begleitet.

Die Challenge

- Steigende Anforderungen an IT-Sicherheit und Compliance (u. a. TISAX)
- Verarbeitung hochsensibler Entwicklungs- und Produktionsdaten
- Wachsende Bedrohung durch Cyberrisiken
- Begrenzte personelle Ressourcen für Security-Themen

Unser Job

- Beratung zur Sicherheitsstrategie inkl. TISAX-Einordnung
- Empfehlung eines KI-gestützten Security-Operations-Modells
- Vorstellung des Managed Detection & Response Service von Arctic Wolf
- Begleitung von Umsetzung und Integration (technisch & organisatorisch)

Der Businessvorsprung

- 24/7-Überwachung der IT durch ein externes SOC
- Frühzeitige Erkennung verdächtiger Aktivitäten
- Detaillierte forensische Analyse von Sicherheitsvorfällen
- Kontinuierliche Weiterentwicklung der Security-Architektur
- Planbares und flexibel skalierbares Kostenmodell



Waldaschaff Automotive

Waldaschaff Automotive ist ein international tätiger Automobilzulieferer mit Schwerpunkt auf Leichtbaukomponenten aus Aluminium. Das Unternehmen entwickelt und produziert unter anderem Batteriegehäuse für Elektrofahrzeuge, Crash-Management-Systeme, Strukturbauteile und Türkomponenten für namhafte OEMs der Automobilindustrie. Waldaschaff Automotive steht für hohe Fertigungstiefe, technologische Kompetenz und langjährige Erfahrung in der Zusammenarbeit mit anspruchsvollen Kunden. Seit dem Jahr 2015 gehört das Unternehmen zur chinesischen Lingyun Industrial Group und ist damit zukunftssicher für eine weitere globale Expansion aufgestellt.

Weitere Informationen finden Sie unter:
www.waldaschaff.com

Bildquellen: Waldaschaff Automotive, Adobe Stock

Sicherheit auf Enterprise-Niveau – mit einem Kostenmodell, das für den Mittelstand bezahlbar ist: Das bietet die Security Operations-Plattform von Arctic Wolf dem Automobilzulieferer Waldaschaff Automotive. Ein externes Expertenteam überwacht heute rund um die Uhr die gesamte IT und unterstützt bei der Weiterentwicklung der Sicherheitsarchitektur. Das ist auch für Compliance-Themen wie TISAX hilfreich.

Steigende Sicherheitsanforderungen in der Automobilindustrie

Als Automobilzulieferer verarbeitet Waldaschaff Automotive täglich sensible Informationen – von Entwicklungs- und Konstruktionsdaten bis zu den Daten der digital gesteuerten Produktion. Entsprechend hoch sind mittlerweile die Anforderungen an die Informationssicherheit. Großkunden aus der Automobilindustrie erwarten heute, dass die Waldaschaff über die entsprechenden Technologien und Prozesse verfügt, um Datenzugriffe umfassend zu überwachen und bei Sicherheitsvorfällen sofort reagieren zu können.

Eine Schlüsselrolle spielt dabei der Branchenstandard TISAX (Trusted Information Security Assessment Exchange). Mit einer TISAX-Zertifizierung weisen Unternehmen der Automobilindustrie nach, dass sie Informationssicherheit systematisch umsetzen und Sicherheitsereignisse strukturiert erkennen, bewerten und dokumentieren können.

Gleichzeitig erhöhen regulatorische Vorgaben wie die EU-Richtlinie NIS2 den Druck auf Unternehmen, ein wirksames und dauerhaft überwacht Sicherheitsniveau sicherzustellen.

„Um die Anforderungen von TISAX vollumfänglich zu erfüllen, brauchen wir ein SIEM-System (Security Information & Event Management), das alle Ereignisdaten unserer IT-Umgebung sammelt und analysiert“, sagt Nils Becker, Head of IT bei Waldaschaff Automotive.

„Noch besser wäre es, ein eigenes Security Operations Center mit 24/7-Verfügbarkeit zu betreiben. Für uns als mittelständisches Unternehmen mit begrenzten IT-Ressourcen ist das aber überhaupt nicht darstellbar.“ Die Verantwortlichen machten sich daher auf die Suche nach einer alternativen Lösung.



Der Weg zum Managed Detection and Response Service

Gemeinsam mit dem langjährigen IT-Partner enthus erarbeitete das IT-Team von Waldaschaff Automotive ein Konzept für einen Managed Security Service. Die Grundidee war, die IT-Umgebung rund um die Uhr von einem externen Partner überwachen zu lassen. Durch die Echtzeit-Auswertung unterschiedlicher Logquellen sollten Anomalien und verdächtige Aktivitäten möglichst schnell erkannt werden. „Wir wollten in der Lage sein, bei allen kritischen Ereignissen sofort die notwendigen Maßnahmen zu ergreifen“, sagt Nils Becker.

Als Lösungspartner für dieses Konzept empfahl enthus schließlich Arctic Wolf, einen weltweit führenden Anbieter von Security Operations. Die Plattform von Arctic Wolf bietet Kunden nicht nur SIEM-Funktionen für eine umfassende Transparenz über ihre Netzwerke, Endgeräte und Cloud-Umgebungen, sondern auch 24/7-Bedrohungserkennung durch ein lokales Security Operations Center (SOC) in Frankfurt am Main. Arctic Wolf kombiniert dabei die KI-gestützte Analyse aller sicherheitsrelevanten Telemetriedaten mit der Expertise hochqualifizierter Security-Teams.

„Arctic Wolf kann mit seinem SOC die Überwachung unserer gesamten Umgebung übernehmen – auch während der Nacht oder am Wochenende“, erklärt Nils Becker. „Zudem stellt uns Arctic Wolf ein dediziertes Concierge Security Team an die Seite, das uns strategisch berät und gemeinsam mit uns die Sicherheit der IT-Infrastruktur verbessert. Wir waren daher sehr schnell überzeugt, dass wir genau den richtigen Partner gefunden haben.“

Die Einführung des neuen Managed Detection and Response (MDR) Services erfolgte in enger Abstimmung zwischen Waldaschaff Automotive, enthus und Arctic Wolf. Zu Beginn stand eine strukturierte Bestandsaufnahme der gesamten IT-Landschaft: von der On-Premises-Infrastruktur über Microsoft

365 bis hin zu Firewalls und bestehenden Endpoint-Security-Lösungen. Auf dieser Basis definierte Arctic Wolf, welche Systeme angebunden werden sollten, um eine möglichst vollständige Sicht auf sicherheitsrelevante Ereignisse zu erhalten.

Technisch umfasst die Lösung unter anderem eine zentrale Appliance zur Analyse des Nord-Süd-Traffics im Rechenzentrum sowie verteilte Agenten auf Servern und Endgeräten. Die Installation und Anpassung der Netzwerk- und Infrastrukturkomponenten übernahm enthus gemeinsam mit dem IT-Team von Waldaschaff Automotive. Nach dem Rollout schloss sich eine mehrwöchige Lernphase an, in der Arctic Wolf das Normalverhalten der Systeme analysierte und schrittweise die Überwachung auf relevante Sicherheitsereignisse aktivierte.

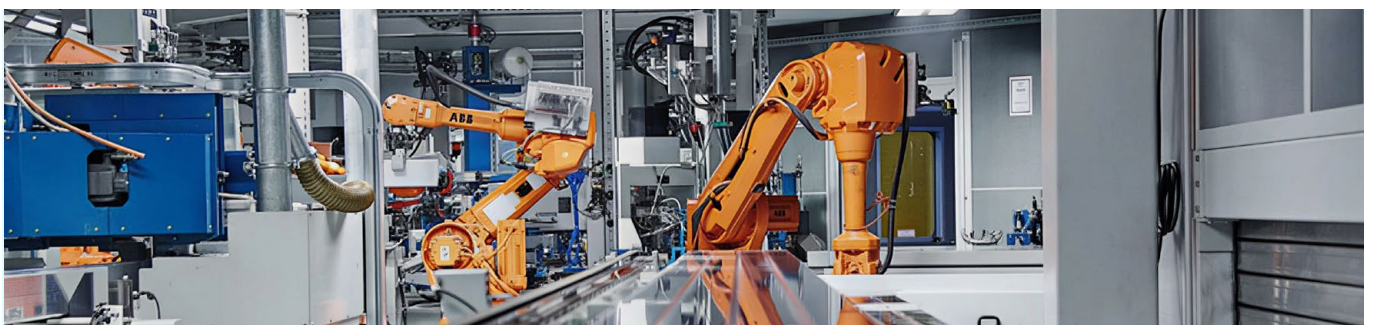
Bedrohungen schnell erkennen und sofort reagieren

Im laufenden Betrieb zeigten sich schnell die Mehrwerte des MDR-Services. Die Spezialisten von Arctic Wolf überprüfen heute alle eingehenden Warnmeldungen auf mögliche Risiken und Bedrohungen. Sobald sie auffällige Aktivitäten registrieren, informieren sie das IT-Team von Waldaschaff Automotive umgehend. Von der Erkennung bis zur Benachrichtigung vergehen dabei in der Regel nur wenige Minuten.

„Einmal klingelte beispielsweise an einem Feiertag plötzlich mein Telefon“, erinnert sich Nils Becker. „Arctic Wolf hatte einen ungewöhnlichen Microsoft Teams-Chat mit einem Teilnehmer in Asien erkannt und als kritisch eingestuft. Auch wenn sich der Vorfall schnell aufklären ließ, zeigt genau das den Wert der 24/7-Überwachung.“

Bei akuten Bedrohungen können die Security-Spezialisten von Arctic Wolf auch selbst aktiv werden. Sie sind beispielsweise in der Lage, einen Client von Netzwerk zu trennen, wenn auf dem Gerät auffällige Aktivitäten festgestellt wurden. Die Überwachung beschränkt sich dabei nicht alleine auf die interne IT-Umgebung von Waldaschaff Automotive. Im Rahmen des sogenannten Dark Web Monitorings prüft Arctic Wolf regelmäßig, ob Zugangsdaten von Mitarbeitern oder mögliche Angriffspunkte in öffentlichen Darknet-Foren auftauchen.

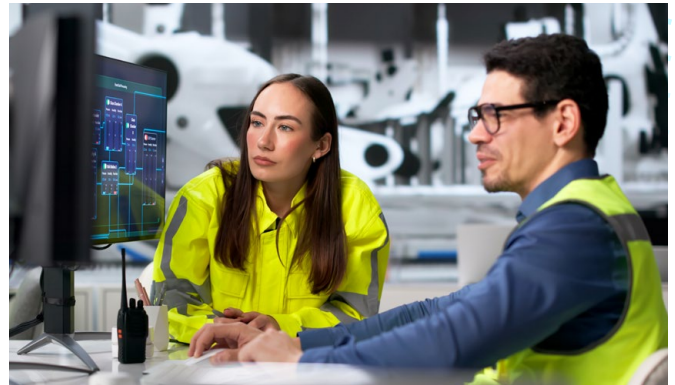
Sehr hilfreich ist für Waldaschaff Automotive zudem die forensische Aufarbeitung realer Sicherheitsvorfälle. So konnte Arctic Wolf etwa im Nachgang eines Phishing-Incidents detailliert rekonstruieren, auf welchem Weg die Zugangsdaten eines Mitarbeiters kompromittiert wurden und welche Aktivitäten anschließend über diesen Account erfolgten. „Arctic Wolf hat uns in dieser Situation geholfen, den Vorfall sauber zu bewerten und umfassend darauf zu reagieren“, so Nils Becker.



Security Journey: Sicherheit als kontinuierlicher Prozess

Über die laufende Überwachung hinaus unterstützt Arctic Wolf auch bei der kontinuierlichen Weiterentwicklung der Sicherheitsarchitektur. In regelmäßigen Terminen tauscht sich das Concierge Security Team dazu mit den IT-Spezialisten von Waldaschaff Automotive aus. Dabei werden gezielt einzelne Themen adressiert, beispielsweise Active Directory, Microsoft 365, Berechtigungsmodelle oder Notfall- und Disaster Recovery-Pläne. Ziel ist es, Schwachstellen und Fehlkonfigurationen systematisch aufzudecken und konkrete Maßnahmen zur Härtung der Systeme abzuleiten.

„Diese regelmäßigen Calls sind für uns extrem wertvoll“, sagt Nils Becker. „Das Concierge Team kennt unsere Umgebung mittlerweile sehr genau und geht Schritt für Schritt mit uns durch die einzelnen Themen. Dabei werden auch Dinge angesprochen, die man im Tagesgeschäft leicht übersieht. Wir priorisieren dann die jeweiligen Maßnahmen und setzen diese gemeinsam mit der enthus um.“



Arctic Wolf hat diese „Security Journey“ bewusst als fortlaufenden Prozess angelegt, um die Sicherheitsmaßnahmen immer wieder zu überprüfen und auch neuartige Cyberrisiken frühzeitig einzudämmen. So entsteht mit der Zeit eine Sicherheitsarchitektur, die sich stets an die aktuelle Bedrohungslage anpasst. Gleichzeitig profitiert Waldaschaff Automotive von Best Practices und konkreten Hilfestellungen, ohne dass das IT-Team dafür erst eigenes Know-how aufbauen muss.



Eine Lösung, die auch für den Mittelstand bezahlbar ist

Neben der hohen fachlichen Qualität spielte für Waldaschaff Automotive auch die wirtschaftliche Perspektive eine zentrale Rolle. Der Managed Security Service von Arctic Wolf wird auf monatlicher Basis abgerechnet. Die Kosten orientieren sich dabei an der Größe und Komplexität der angebundenen IT-Umgebung. „Stark vereinfacht gesagt bewegt sich das auf dem Niveau eines einzelnen IT-Spezialisten“, sagt Nils Becker. „Wir erhalten dafür aber 24/7-Verfügbarkeit und die Expertise eines kompletten Teams. Um das intern abzubilden, bräuchte ich mehrere hochspezialisierte Fachkräfte plus Infrastruktur und Software. Das ist weder realistisch noch wirtschaftlich.“

Ein wichtiger Aspekt für die Verantwortlichen bei Waldaschaff Automotive ist zudem die stufenlose Skalierbarkeit des Modells. Der Serviceumfang passt sich automatisch an alle Veränderungen der IT-Umgebung an. Wenn beispielsweise Systeme konsolidiert oder IT-Standorte zusammengeführt werden, sinken auch die Kosten für den Managed Security Service. Umgekehrt lässt sich die Lösung problemlos erweitern, wenn neue Systeme oder Services hinzukommen. „Diese flexible Skalierbarkeit schätzen wir sehr, da die anfallenden Kosten dadurch für uns verlässlich planbar sind“, sagt Nils Becker.

„Wir haben die Entscheidung für Arctic Wolf noch keine Sekunde bereut. Für mich ist der größte Mehrwert, dass wir jederzeit auf hochspezialisierte Security-Expertise zugreifen können, ohne sie selbst vorhalten zu müssen. Dadurch erreichen wir ein höheres Sicherheitsniveau und bessere Transparenz zu wirtschaftlich sinnvollen Konditionen. enthus hat uns mit seiner Beratung und Unterstützung den Weg dorthin geebnet.“

Nils Becker, Head of IT, Waldaschaff Automotive GmbH

Fazit und Ausblick

Mit der Security Operations-Plattform und dem Concierge Team von Arctic Wolf hat Waldaschaff Automotive seine IT-Sicherheit auf eine neue Stufe gebracht. Der Automobilzulieferer überwacht die gesamte Umgebung kontinuierlich auf mögliche Risiken und kann jederzeit nachweisen, dass er seine Security-Prozesse im Griff hat. „Bei Audits können wir beispielsweise sehr einfach darlegen, wie wir Security Incidents erkennen, bewerten und bearbeiten“, erklärt Nils Becker. „Das hilft uns natürlich auch bei Compliance-Themen wie der TISAX-Zertifizierung.“

Aktuell arbeitet Waldaschaff Automotive gemeinsam mit enthus bereits an einer Erweiterung der Sicherheitsarchitektur. Künftig will das Unternehmen auch den Aurora™ Endpoint Security Service nutzen, um alle Endgeräte vor modernen Cyberbedrohungen zu schützen. Sicherheitsspezialisten von enthus werden das IT-Team bei der Implementierung begleiten.



enthus

Über 500 Enthusiast:innen an mehreren Standorten in Deutschland, Österreich und der Schweiz sind bei über 200 Millionen Euro Jahresumsatz leidenschaftliche **#erfolgreichmacher** für IT und Digitalisierung. Mit innovativen IT-Lösungen, Managed Services & XaaS sowie unseren smarten Lösungen für digitale Geschäftsprozesse wollen wir **#yourfirstchoice** auf dem Weg ins digitale Zeitalter sein.

Denn Herausforderungen löst man am besten im Schulter-schluss – partnerschaftlich und auf Augenhöhe.

Weitere Informationen finden Sie unter: www.enthus.de



Interessiert?

Wolfgang Hahl

Mitglied der Geschäftsführung

E-Mail: hallo@enthus.de