infopulse
Part of Tietoevry Create

GOODVALLEY
Since 1994

Proaktive Sicherheit mit einem SOC und Cloud SIEM für Goodvalley_

Ein SOC zur proaktiven Sicherung der hybriden Infrastruktur eines multinationalen Agrar- und Lebensmittelherstellers

Branche: **Landwirtschaft und Lebensmittel** **Standort:** **Dänemark, Polen, Ukraine**

Mitarbeitende: **Über 1.700**

Über den Kunden

Website:
https: www.goodvalley.com

Goodvalley ist ein internationaler Lebensmittelhersteller, der sich zu verantwortungsbewussten landwirtschaftlichen Praktiken und der Lieferung von qualitativ hochwertigen Schweinefleischprodukten verpflichtet hat. Der Ansatz des Unternehmens beinhaltet eine vollständige Qualitätskontrolle des Produktionsprozesses vom Feld bis zur Gabel am Tisch. Zum Produktionsnetzwerk von Goodvalley gehören insgesamt 37 Bauernhöfe in Polen und der Ukraine, 33.500 Hektar Ackerland und 9 Biogasanlagen, die den Produktionskreislauf schließen und zur Verringerung von Emissionen und Auswirkungen auf das Klima beitragen. Goodvalleys Geschäftstätigkeit ist in hohem Maße von IT-Systemen abhängig, um den Betrieb zu steuern und zu kontrollieren. Daher sind Stabilität und Sicherheit entscheidend, um Geschäftsunterbrechungen und finanzielle Risiken zu vermeiden.

Zusammenfassung_

Ziele

Bereitstellung eines SOC mit einem effizienten SIEM-System zur Überwachung von Datensicherheitsbedrohungen innerhalb der gesamten IT-Infrastruktur. Entwicklung und Pflege einer effizienten Cybersicherheitsstrategie und Bereitstellung von mehrstufigem Support für die Sicherheitsüberwachung und das Management von Zwischenfällen.

Lösung

Die Sicherheitsexperten von Infopulse entwickelten ein verwaltetes SOC auf der Basis von Microsoft Sentinel und sorgten für eine dedizierte Sicherheitswartung, die die gesamte IT-Infrastruktur des Kunden an mehreren Standorten, einschließlich der Cloud, abdeckt.

Vorteile

Mehr Cybersicherheit, proaktives Sicherheitsrisikomanagement, umfassender Schutz der gesamten IT-Infrastruktur, einschließlich Cloud-Ressourcen, Automatisierung der Bearbeitung wiederkehrender Probleme, Senkung der Kosten für den Sicherheitsbetrieb und kontinuierliche Verbesserung der Sicherheitssysteme, um den sich entwickelnden Bedrohungen einen Schritt voraus zu sein.

Gelieferte Dienstleistungen

Cybersecurity, Security Operations Center (SOC), SIEM & SOAR, Sicherheitsbewertung, Microsoft Sentinel

Anforderung_

Bereits 2021 begann Goodvalley mit der Prüfung von Optionen für die Einführung von SOC. Ende 2023 war Goodvalley auf der Suche nach einem zuverlässigen Sicherheitsdienstleister, der das Unternehmen bei der Verwirklichung der folgenden Ziele unterstützen würde:

- Implementierung eines SOC mit SIEM-Lösung zur Abdeckung der gesamten hybriden IT-Infrastruktur
- Ermöglichung einer effizienten Überwachung der Cybersicherheit
- Automatisierung der Verarbeitung von Sicherheitsvorfällen
- Gewährleistung einer speziellen Unterstützung und Wartung der Datensicherheit

Die folgenden Aspekte waren für das Unternehmen von größerer Bedeutung:

- Eignung der vorgeschlagenen Technologien und Instrumente
- Gesamtkosten des Projekts
- Unser strategischer Ansatz und unsere proaktive Haltung bei der Implementierung von Sicherheitsverbesserungen.

Goodvalley entschied sich für Infopulse als vertrauenswürdigen Sicherheitspartner mit branchenspezifischer Erfahrung und einem tiefen Verständnis der spezifischen Infrastruktur des Unternehmens. Wir empfahlen eine auf Microsoft Defender basierende Lösung, die den Anforderungen des Kunden entsprach und perfekt in sein aktuelles Sicherheits-Ökosystem passte.

Lösung und Geschäftswert_

Infopulse hat eine leistungsstarke, auf Microsoft Sentinel basierende Managed SOC-Lösung implementiert, die IT-Infrastrukturkomponenten von Goodvalley zur kontinuierlichen Sicherheitsüberwachung mit SIEM verbindet.

Neben der mehrschichtigen Sicherheitswartung und -unterstützung wird unser Kunde von folgenden Vorteilen profitieren:

- Deutlich verbessertes Risikomanagement und Stabilität der Cybersicherheit
- Kontinuierliche strategische Verbesserungen der Cybersicherheitslage des Unternehmens
- Proaktiver Ansatz zur Bearbeitung von Cybersicherheitsvorfällen
- Geringere Kosten für IT-Infrastruktur und Sicherheitsmaßnahmen

Dank der gemeinsamen Anstrengungen der Sicherheitsexperten von Infopulse und der IT-Abteilung von Goodvalley erreichte das Agrar- und Lebensmittelunternehmen ein stabiles, hohes Niveau an Cybersicherheitseffizienz und konnte kritische Sicherheitsvorfälle vermeiden.

Technische Informationen

Nach eingehender Untersuchung der Kundenbedürfnisse schlug Infopulse den Einsatz von **Microsoft Sentinel** vor – eine strategische Entscheidung, da die IT-Infrastruktur von Goodvalley hauptsächlich auf dem Microsoft-Ökosystem basiert.

Wir haben ein Pilotprojekt initiiert, um die Möglichkeiten von Microsoft Sentinel zu demonstrieren, damit der Kunde alle Vorteile der vorgeschlagenen Lösung in Aktion sehen konnte. Für das Pilotprojekt stellte unser Partner Microsoft alle erforderlichen Lizenzen kostenlos zur Verfügung, sodass Goodvalley die Funktionsfähigkeit der Lösung ohne jegliche Kosten prüfen konnte.

Nach dem erfolgreichen Pilotprojekt haben wir das Projekt in vollem Umfang umgesetzt, das folgende Punkte umfasst:

1. **Durchführung der SIEM-Systemintegration** durch Verbindung aller lokalen und Cloud-Ressourcen. Auf der Grundlage der Ergebnisse des Pilotprojekts berechneten wir das erforderliche Budget und schlugen spezifische Netzoptimierungen vor, um wettbewerbsfähige Preise anbieten zu können.
2. Wir **implementierten die Microsoft Sentinel-Lösung und stellten Cloud-Dienste** wie Azure, Microsoft 365, verschiedene SaaS-Tools usw. bereit. Anschließend haben wir die Cortex XDR- und Fortinet-Firewalls sowie die übrige Infrastruktur mit dem SOC verbunden.
3. **Aufstellung von Analyseregeln** zur Erkennung von Sicherheitsvorfällen und Aktivierung geeigneter Verarbeitungsmechanismen. Dies ermöglichte es, echte Vorfälle aus allen empfangenen Systemwarnungen herauszufiltern und sie korrekt zu entschärfen, was eine effiziente SOC-Leistung sicherstellt.
4. Die SIEM-Überwachung ergab unsachgemäße Netzwerkeinstellungen. Deshalb gaben wir **Empfehlungen zur Netzwerkoptimierung**, die es Goodvalley ermöglichten, die Arbeitslast der Infrastruktur zu verringern und somit Ressourcen und Kosten zu sparen.
5. **Reduzierung der übermäßigen Datenprotokolle.** Um die Datenmengen zu reduzieren, die keinen praktischen Wert für die Sicherheit haben, haben wir unnötige Daten herausgefiltert und Daten aus allen analysierten Quellen aggregiert. So konnten wir die Menge der in der Cloud gespeicherten Daten deutlich verringern, ohne ihre Aussagekraft zu beeinträchtigen.

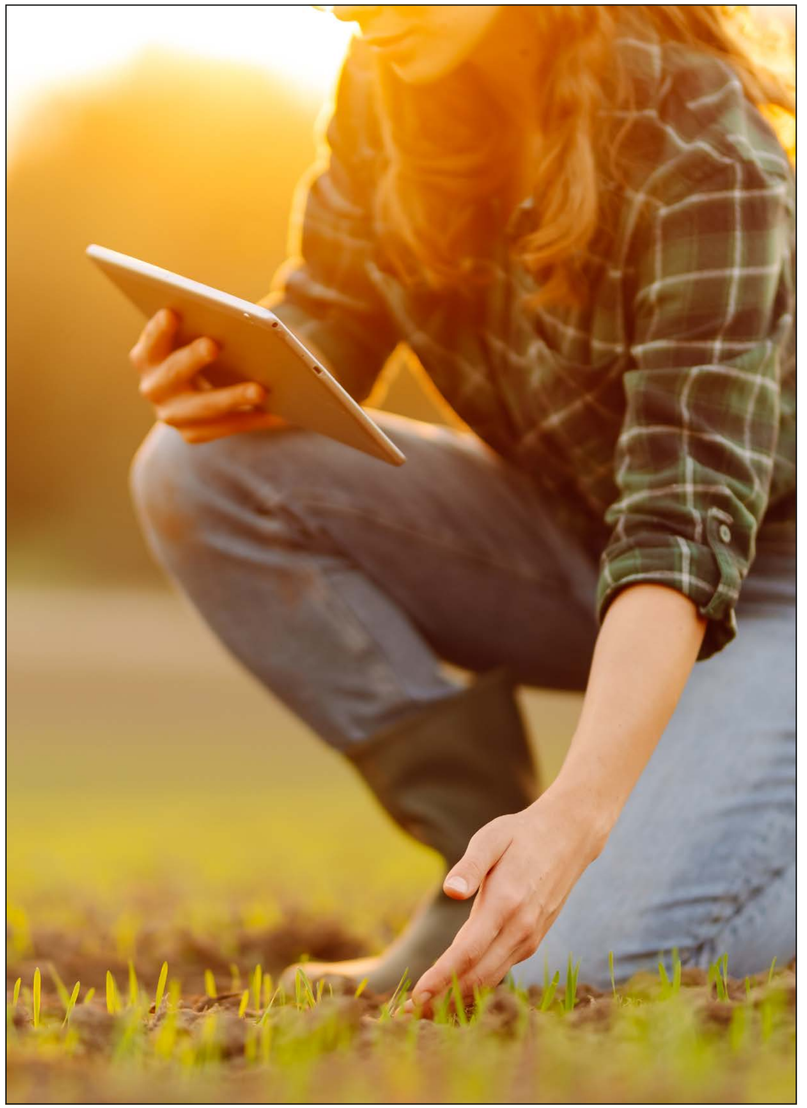
Die Ersteinrichtung und Bereitstellung des SOC dauerte ca. 3 Monate. Sobald wir die ersten Überwachungsprotokolle erhalten hatten, begannen wir mit der Umsetzung von Verbesserungen der Sicherheit und der IT-Infrastruktur. Wir haben proaktiv potenzielle Schwachstellen identifiziert und behoben und einen nahtlosen Übergang von der vorherigen Lösung ohne Unterbrechungen sichergestellt.

Nach der anfänglichen Implementierungsphase begann unser engagiertes SOC-Team mit der umfassenden „Security-as-a-Service“-Wartung und Unterstützung auf mehreren Ebenen:

- **Ebene 0** umfasst die automatische Verarbeitung von Vorfällen zur Entschärfung wiederkehrender Sicherheitsfälle mit geringer Auswirkung.
- **Ebene 1:** Die erste Alarmanalyse wird von zuvor erstellten Playbooks durchgeführt. Der Dienst wird von einem Team von Sicherheitsspezialisten in der Ukraine und der EU erbracht.
- **Ebene 2/3:** Bearbeitung untypischer und komplexer Vorfälle. Diese wird von zwei eigens eingesetzten Spezialisten durchgeführt. Nach der Bearbeitung jedes solchen Vorfalls werden Anweisungen für L1-Spezialisten erstellt, um ähnliche Alarme in Zukunft zu bearbeiten, wenn solche Alarme auftreten.
- **Forensischer Scan:** Detaillierte Untersuchung und Dokumentation komplizierter Vorfälle mit den größten möglichen Auswirkungen. Glücklicherweise hatte der Kunde während unserer Zusammenarbeit keine derartigen Sicherheitsvorfälle.

Wir haben das SOC-Alarmsystem auch in das interne Ticketing-System des Kunden integriert, so dass die IT-Spezialisten des Kunden vollen Überblick haben und die Sicherheitsaufgaben problemlos verwalten können.

Das Projekt ist noch nicht abgeschlossen. In wöchentlichen Sitzungen wird Goodvalley über die Leistung des SOC informiert, es werden Verbesserungsvorschläge gemacht und alle anderen Aspekte der Datensicherheit besprochen.



Technologien und Tools_

- Microsoft Azure
- Microsoft Sentinel
- Kortex XDR
- Fortinet-Firewall

Über Infopulse

Infopulse gehört zum führenden nordischen Unternehmen für digitale Dienstleistungen Tietoevry Create und ist ein internationaler Anbieter von Dienstleistungen in den Bereichen Cybersicherheit, Schutz der IT-Infrastruktur, SIEM/SOAR und Bereitstellung von SOC-Lösungen. Mit unseren Dienstleistungen decken wir alle Cybersecurity-Bedürfnisse moderner Unternehmen ab. Wir berücksichtigen dabei branchenspezifische Anforderungen, um betriebliche Widerstandsfähigkeit und robusten Schutz vor Cyberbedrohungen zu erreichen. Viele namhafte Unternehmen vertrauen auf Infopulse, darunter Corteva Agriscience, Delta Wilmar, EarthDaily Agro, Goodvalley, Kernel, MHP, RAGT Semences Ukraine, Zeppelin, BICS, Bosch, LMT, Microsoft, Metinvest, Offshore Norge, OLX, SAP, VEON, Vodafone und andere.

Für weitere Informationen besuchen Sie bitte **www.infopulse.com/de**

Kontaktieren sie uns

PL +48 (221) 032-442

DE +49 (69) 505-060-4719

US +1 (888) 339-75-56

UA +38 (044) 585-25-00

BG +359 (876) 92-30-90

NL +31 (70) 89-10-8534

BR +55 (21) 99298-3389

info@infopulse.com