UnderDefense
CYBERSECURITY

UnderDefense Helps Retail Software Leader Make the Most of Existing Security Tools and Ensure 24×7 Monitoring

About the client

The client is a big, innovative US-based company that provides retailers with integration and management software, including POS, OMS, and other equipment. Their cloud-based solutions are used for retail analytics, inventory control, and shipment. The client owns over 15,000 live terminals in 5,000 stores globally and keeps growing.

Headquarters:	**Florida, USA**
Industry:	**IT**
Client Since:	**October 2022**
Technologies and Tools:	**CrowdStrike XDR**
Internal IT Security Team:	**Yes**
Infrastructure:	**Hybrid**

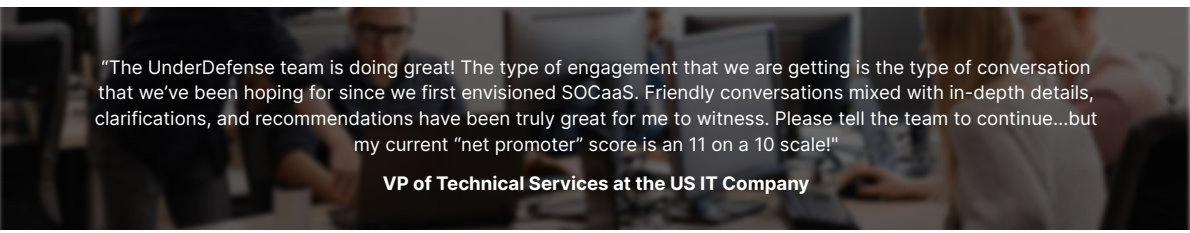
Data-Driven Outcomes

30min
MTTR ensuring attack containment at the earliest stage

40
High-risk alerts addressed within the last 5 months

817
Covered endpoints

70+
Insecure XDR exclusions fixed enabling advanced malware analysis functionality



"The UnderDefense team is doing great! The type of engagement that we are getting is the type of conversation that we've been hoping for since we first envisioned SOCaaS. Friendly conversations mixed with in-depth details, clarifications, and recommendations have been truly great for me to witness. Please tell the team to continue...but my current "net promoter" score is an 11 on a 10 scale!"

VP of Technical Services at the US IT Company

CHALLENGES

- Tool-centered approach, relying only on out-of-the-box product features
- Lack of competence to properly assess and configure system functionality
- MTTR was unspecified due to zero alerts received by the customer
- Lack of software fine-tuning, leading to a wrong impression that everything was in order
- Misconfiguration of XDR, causing monitoring blind spots and decreasing protection
- Lack of dedicated professionals with expertise in cybersecurity

RESULTS

- Thorough assessment of settings and introduction of an appropriate incident response workflow
- Close communication via 24/7 hotline and operational chat to address abnormal activities immediately
- Security monitoring 24/7 with an average of 30 minutes MTTR
- 40 high-risk alerts processed and 1 incident addressed within the last 5 months
- Over 70 insecure XDR exclusions fixed to improve the protection policies and enable advanced malware analysis features
- Providing expert recommendations on identity protection, cloud, and on-prem infrastructure security

RESULTS

UnderDefense
CYBERSECURITY

UnderDefense is a CyberSecurity as a Service Platform to easily solve Security Operations, Automation & Compliance challenge with 24×7 MDR. We are ISO27001 certified in cybersecurity, privacy and data protection. Our mission is to assure greater Cyber Resiliency and business continuity for small and medium-sized enterprises. Worldwide.

Address: suite 420, 111 John St New York, NY 10038, USA
Tel: +1 929 999 5101
email: help@underdefense.com
Website: underdefense.com