UnderDefense
CYBERSECURITY

Enhancing US Government Organization Security with MDR

About the client

The client is one of the 10 largest government organizations in the US financial sector.

Headquarters:	Texas, USA
Industry:	Government/Finance
Client Since:	December 2021
Technologies and Tools:	-QRadar -Office365 + AD -Windows Servers -Palo Alto Firewall -CortexXDR
Internal IT Security Team:	Yes
Infrastructure:	Hybrid

Data-Driven Outcomes

$700,000+
Saved after entrusting security tasks to UnderDefense

32%
Of threats resolved outside usual work hours by remote SOC

9min
Is the average time to detect and remediate a threat

1200+
Covered endpoints and servers

547
Automated rules enabled

1500
Critical/high risk alerts addressed during the first 11 months of cooperation

CHALLENGES

- A limited internal IT team of 4 people without the necessary expertise to efficiently process all alerts promptly
- IT team was overwhelmed by alert fatigue, preventing them from concentrating on their primary tasks
- The inability to detect suspicious behavior from logs resulting from data fragmentation
- Alerts couldn't be processed outside of standard business hours
- The inability to identify, assess, and respond to risks rapidly and effectively
- The inability to expand the team due to a lack of funding

SOLUTION AND RESULTS

- During the first 11 months, 12,500 alerts were identified, analyzed, and resolved, with 1,500 being of high or critical risk
- Around 1000 working hours were saved due to the reduction in the number of false positives
- A custom SIEM was created with automated rules to collect data from all security software
- 32% of threats occurring outside of the typical working hours were promptly addressed due to 24/7 monitoring
- The average time it took to identify, analyze, and deal with high and critical alerts was 9 minutes
- An estimated $700,000 was saved by entrusting monitoring responsibilities to UnderDefense

RESULTS

UnderDefense

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