deepwatch

Financial Services **Case Study**

Bank Collaborates with deepwatch to Establish Security Operations Center and Mature Security Capabilities

The Customer

Industry: Financial Services

Security Team Size: 15

Assets Under Management: $1 Trillion

Endpoints: 24,000

The Challenges

- Compliance Regulations
- Security Talent
- 24x7x365 Alert Monitoring
- Security Maturity
- Highly Targeted Industry Segment

The Goal

The customer operates in the financial services industry and as such is a highly desirable target for threat actors. In 2017 the customer had suffered a security incident that cost the business millions of dollars to repair. At the time the customer did not have a Security Operations Center (SOC) or 24x7x365 security monitoring in place. After the incident, a Chief Information Security Officer (CISO) was hired by the Chief Executive Officer (CEO) and the Board to mature their security operations to reduce the risk of future security breaches.

The CISO evaluated his security team, their technologies, and their capabilities. In order to meet stringent compliance regulations and quickly establish 24x7x365 monitoring capabilities, the CISO collaborated with the CEO and the Board to set a budget and hire a Managed Security Service Provider (MSSP).

The goal for establishing a relationship with an MSSP was to:

- Quickly and cost effectively stand up a SOC
- Fully outsource a SOC to establish 24x7x365 security monitoring capabilities
- Ensure SOC monitoring, validation, vetting and triaging of alerts aligned with internal team priorities
- Grow their understanding of their industry threat landscape
- Enable the internal security team to focus on meeting compliance regulations, while the MSSP manages security
- Collaborate with the MSSP to improve overall security posture and enhance security capabilities over time

The Criteria

The CISO and his leadership team evaluated 8 different MSSP's as part of their selection process. The team believed that they would be well served by an MSSP that met the following criteria:

- Responsive team of analysts with specific knowledge and focus on their particular industry
- Delivery of a fully enabled 24x7x365 SOC
- A customer focused, long-term partner
- Strong technical acumen and innovation to stay ahead of the ever changing threat landscape
- Data portability in the event that the Board, CEO, and CISO determined that they would like to establish an in-house SOC
- A detailed roadmap and a trusted partner to work with to enhance security maturity over time
- Expertise, API integrations and strong working relationships with industry leading technology vendors

The Outcome

The CISO and his team selected deepwatch's Managed Detection & Response Services as the best match for their needs. deepwatch ranked highest for its technology platform, innovative roadmap, and its high-touch delivery model. The CISO needed deepwatch to ramp quickly in 2018 and pressed for full deployment in under 60 days. In 42 days deepwatch had deployed its capabilities and was delivering value to the business.

The deepwatch Squad Delivery Model allowed the CISO and his team to build strong relationships with named deepwatch analysts to grow communal understanding of the Bank's business, threat landscape, and operating model. Together, the deepwatch Squad and the CISO's team are able to improve alert fidelity by over 82% in less than 6 months. In addition, the deepwatch team improved the Bank's maturity index by 57% in the first year.

Now armed with the deepwatch sourced Maturity Model score, the CISO has secured a twofold increase in budget to enhance their security program. deepwatch, as a close partner, continues to collaborate with the CISO to recommend additional log sources to manage and monitor, which security technologies to jettison and which ones to acquire to enhance their ability to identify and resolve security incidents quickly.

ABOUT DEEPWATCH

deepwatch delivers data-driven managed security services while extending customers' cybersecurity teams and proactively advancing their SecOps maturity. Powered by our innovative cloud-native platform, deepwatch is trusted by leading global organizations to provide 24/7/365 managed security services.

CONTACT US

sales@deepwatch.com
7800 E Union Ave, Suite 900 Denver, CO 80237
855.303.3033

deepwatch.com