imc

Unlocking Secure Environments in Endpoint Protection

Background:

The leading financial investment company sought to fortify endpoint security within their environment by adhering to Palo Alto Networks Cortex XDR security guidelines. IMC undertook the development, provisioning, building, configuration, and deployment of a robust security architecture.

This initiative spanned across various environments, networks, infrastructure, software, and tools, ensuring compliance with the client's security policies and standards for a modernized and secure environment.

Key Challenges:

Lack of Endpoint Security Tools

The absence of tools to safeguard endpoints from behavior-based, signature-based, ML-based threats, and exploits.

Real-time Verdict Update Mechanism

Inability to maintain a real-time verdict update mechanism and integrate with cloud-based malware analysis services.

Identifying Malicious Activities

Challenges in identifying malicious activities within the client's environment due to the absence of threat detection engine updates.

The Solution:

Successfully implemented a comprehensive solution leveraging Cortex XDR to address the identified challenges:

1. **Cortex XDR Agent Deployment**

   Deployed the Cortex XDR agent to meet rigorous endpoint security needs, covering EDR, next-generation AV, and legacy AV replacement.

2. **Endpoint Data Lake Integration**

   Natively integrated the Cortex XDR endpoint data lake within the client's environment.

3. **Behavioral Analytics and Custom Rules**

   Analyzed data using machine learning-based behavioral analytics and custom rules to generate high-signal alerts.

4. **Secure Connection and Endpoint Routing**

   Established a secure connection with XDR, routed endpoints from the Airgap Subnet, and collected/forwarded logs and files for analysis.

5. **Integration with Wildfire**

   Integrated the Cortex XDR solution with Palo Alto Networks Wildfire to automatically prevent threats discovered on the network/ endpoint globally.

6. **Comprehensive Security Coverage**

   Deployed Cortex XDR agent as part of the Cortex XDR suite to detect and respond to security threats across networks, endpoints, and the cloud.

Benefits:

The implementation resulted in several tangible benefits for the financial investment company:

1. **Preventive Measures**

   Prevented malware, exploits, and suspicious activities across multiple systems.

2. **Attack Detection**

   Uncovered attacks by implementing Palo Alto Networks Cortex XDR, enhancing the overall threat detection capabilities.

3. **Lifecycle Protection**

   Protected critical stages of the attack lifecycle for both online and offline users, ensuring a comprehensive security posture.