Brian Sowers

12/04/2023

DevSecOps and SASE

1. Explain the three security layers that must be part of a DevSecOps and effective API security design.

DevSecOps is a philosophy that “strives to automate core security tasks that are essential to operations by embedding security controls and processes into the DevOps workflow" (Secure Business Modules, 7). In a DevSecOps approach for Application Programming Interface (API) security, there are three necessary security layers for its design. The first layer is application security, which targets the security of the API and application during development. Here, the focus is on practices like secure coding, regular security assessments, and code analysis to prevent vulnerabilities. This layer aims to shield the application from common threats like Structured Query Language (SQL) injection and cross-site scripting. The second layer is system security. This layer's focus is on safeguarding the systems where APIs and applications are hosted. It involves implementing robust authentication protocols, maintaining the security of servers and databases, and ensuring timely application of security patches. This layer is crucial for controlling access to system resources. The third layer is network security. It is about protecting the network channels used by APIs. Techniques include using transport layer security (TLS) for encryption, implementing network monitoring solutions, and deploying firewalls. This layer aims to secure data in transit, preventing unauthorized interceptions and tampering. Together, these layers ensure that APIs are developed, deployed, and operated with comprehensive security, covering each aspect from the code to the system and network level.

This multi-layered approach is fundamental in a DevSecOps strategy, ensuring protection against a variety of security threats such as information leakage, dependency vulnerabilities, and man-in-the-middle attacks (API Security in the Enterprise, 5).

2. Explain how you would reimagine security and networking infrastructure with a cloud-first and unified SASE architecture for your industry sector.

In the technologically evolving landscape of the financial sector, where banks are transitioning from a traditional banking-as-a-product approach to a more integrated banking-as-a-lifestyle model, the application of Zero Trust Network Architecture (ZTNA), Palo Alto's Prisma Cloud, Secure Access Service Edge (SASE), and Cortex XSOAR becomes increasingly relevant. With financial institutions expanding their offerings across various channels, including digital wallets, Peer-to-Peer (P2P) platforms, and Artificial Intelligence (AI)-driven services, securing these necessary and interconnected systems is paramount (Building the Digital Bank of the Future, 8).

Palo Alto's Prisma Cloud can fulfill a critical role in monitoring and securing these financial cloud-based services, from digital payment solutions to AI-driven wealth management tools, ensuring compliance with stringent financial regulations and safeguarding sensitive data (Palo Alto Networks, "Prisma Cloud"). SASE's unified architecture becomes instrumental in managing the complex network of digital channels and third-party partnerships, offering a streamlined yet secure access point for various financial services, enhancing customer experience without compromising security (Palo Alto Networks, “SASE”). Cortex XSOAR complements this architecture by providing security orchestration, automation, and response (SOAR)

technology across the varied services. Cortex XSOAR ensures rapid threat detection and mitigation in the quickly developing technological infrastructure of digital financial transactions and wealth management (Palo Alto Networks, "Cortex XSOAR"). ZTNA's principle of "never trust, always verify" is vital in this context, ensuring secure customer interactions by "eliminating implicit trust and continuously validating every stage of a digital interaction" (Palo Alto Networks, “Zero Trust”). It provides the necessary foundation for securing transactions and customer data, crucial in P2P payments and wealth management services that increasingly rely on digital communications. This comprehensive approach, tailored to the unique requirements of the financial sector's evolving business models and digital adoption, ensures a robust, agile, and secure infrastructure that aligns with the dynamic nature of emerging financial services.

Works Cited

42Crunch, Apidays, and Platformable. "API Security in the Enterprise." 2017, https://panacademy.net/CourseFiles/sbo/DevSecOps_API_Security.pdf. Accessed 4 Dec. 2023.

"Building the Digital Bank of the Future: The Emerging Role of Quality Assurance." Everest Global, 2018, https://panacademy.net/CourseFiles/sbo/Everest_Group_Quality_Orchestration.pdf. Accessed 4 Dec. 2023.

Palo Alto Networks. "Cortex XSOAR." Palo Alto Networks, n.d., www.paloaltonetworks.com/cortex/cortex-xsoar. Accessed 4 Dec. 2023.

Palo Alto Networks. "Prisma Cloud." Palo Alto Networks, n.d., www.paloaltonetworks.com/prisma/cloud. Accessed 4 Dec. 2023.

Palo Alto Networks. "Secure Access Service Edge (SASE)." Palo Alto Networks, n.d., www.paloaltonetworks.com/sase. Accessed 4 Dec. 2023.

Palo Alto Networks. "Zero Trust." Palo Alto Networks, n.d., www.paloaltonetworks.com/zero-trust. Accessed 4 Dec. 2023.

“Secure Business Operations Module 4”, *Palo Alto Networks.* https://s3.amazonaws.com/assets.paloaltonetworksacademy.net/sbo/Business_Operations_Module_4.pdf. Accessed: 4 Dec. 2023.