Managed Device to Cloud Security Operations

Container level cybersecurity for Docker images and Kubernetes containers in AWS EKS

Code based Vulnerability Assessment for applications and firmware across products

Case Study

Executive Summary

The client is a US-based provider of smart home products. They have a large smart home camera network being supported using an AWS based cloud application platform. In a span of 4 years, eInfochips team has helped in optimizing their cloud TCO for a 5x growth journey in deployed connected devices. With a growing number of products and variants in deployment, the firmware and application software codebase has grown increasingly complex across edge and cloud. Vulnerabilities across the technology architecture were seen to be emerging in deployed applications resulting in increased attack surface for the connected device network.

eInfochips IoT cybersecurity team conducted a thorough security assessment, spanning VAPT, SCA, and Application Security Testing as well as enabled adoption of DevSecOps practices.

Client Profile

The client is a US-based smart home camera company.

Challenge

- Lack of security scanning
  - At code level for different products in connected home devices segment
  - At container level for hundreds of unique images, thousands of running containers
- Manual process for code review, ticket assignment, management, and closures reducing productivity and throughput

Solution

eInfochips managed end-to-end security assessment and security operations enhancement using market leading commercial and open-source tool stacks.

The engagement included:

- Code vulnerability scanners integrated with Jenkins CI/CD Pipeline - scanning in every release cycle
- Policy based security assessment of builds
- Leveraged tool based automated ticket assignment to developers, Git based code repository
- Vulnerability management, checks for PCI, File Integrity Monitoring, Asset Inventory – agent installed in every asset (DC and Cloud)
- Automated ticket generation and resolution, security monitoring
- Manual pen-testing is done annually for overall infrastructure, for key vulnerabilities identified
- Resolved configuration issues in code analysis and testing tools (network configuration whitelisting, API key renewal) to streamline the pipeline

Benefits

- 25% reduction in false positive tickets in cybersecurity operations
- Transformed DevOps to DevSecOps by integrating cybersecurity tools into CICD pipeline
  - Re-initiated security scanning, addressed CICD pipeline backlog of 500+ tickets
- Complete automation of vulnerability ticket management process

USA HQ 2025 Gateway Place, Suite #270, San Jose, CA 95110.

INDIA HQ 11 A/B Chandra Colony, CG Road, Ellisbridge, Ahmedabad 380 006.

www.einfochips.com | marketing@einfochips.com