Proposal: Revisiting Application Categorization for Accurate Security Compliance

Background

Wells Fargo's Enterprise Application Security Platform (EASP) monitors and ensures the security health of applications and their components. Applications are categorized into security types such as EASP-Other, EASP-Cloud, and EASP-PAA based on parameters like technology and deployment platform. These categories influence how vulnerabilities are managed, with varying deadlines and priorities.

For example, a Severity-4 vulnerability is optional to fix under EASP-Other but must be addressed within 180 days under EASP-Cloud.

Lending Grid NDM (LGNDM) is a critical capability within Lending Grid, supporting file integrations. Initially categorized as EASP-Other, LGNDM partially migrated three UI components to the cloud while retaining the majority of its infrastructure on-premise due to legacy system dependencies.

Incident

Following the migration of a few UI components to the cloud, the entire LGNDM application was reclassified as EASP-Cloud. This reclassification was retroactive, meaning existing non-critical vulnerabilities became critical & overdue overnight.

Upon investigation, it was clarified that EASP categorization rules treat the entire application as cloud-based if even a single component is deployed in the cloud. This "all-or-nothing" approach triggered a firefighting situation, as the team had to resolve numerous non-critical vulnerabilities urgently.

The issue arises because this rule does not account for hybrid application footprints, leading to inaccurate categorizations and unnecessary operational strain.

Key Issues with the Current Rule

1. **Discourages Cloud Migration:** Teams may hesitate to migrate components incrementally due to disproportionate compliance burdens.
2. **Increased Workload with Limited ROI:** Teams face additional technical and administrative overhead without meaningful benefits.
3. **False Alarms:** Reports and escalations become inaccurate, creating unnecessary panic and urgency.

Proposed Solution

Introduce Component-Level Categorization:

Instead of applying security categorization at the application level, consider each component individually:

- Cloud-deployed components should be categorized as EASP-Cloud.
- Legacy on-premise components should remain categorized as EASP-Other.

Benefits of the Proposed Solution

1. **Encourages Incremental Cloud Migration:** Teams can adopt hybrid strategies, such as the Strangler Fig pattern, without undue penalties.
2. **Accurate Categorization:** Components are represented based on their actual deployment environments, improving compliance accuracy.
3. **Reduced Workload:** Developers focus on meaningful work, boosting productivity.
4. **Fewer False Alarms:** Leadership avoids being overwhelmed by unnecessary escalations.
5. **Improved Efficiency:** Saves time across all levels, from technical teams to approval processes.

Conclusion

Adopting component-level categorization aligns security compliance with actual deployment environments. This change not only ensures fairness but also promotes cloud adoption, reduces unnecessary workloads, and fosters a more efficient and accurate reporting system. We urge leadership to consider this proposal to optimize our application security processes and encourage innovation without compromising compliance.