opus

Checklist

Tracking Down Key Stakeholders for Effective Security Remediation

1 Understanding Your Key Players

- [ ] **Practitioners:** Those responsible for actually executing remediation, such as developers and system engineers.
- [ ] **Resource Allocators:** Decision-makers responsible for determining where resources should go, such as team leaders and project managers.
- [ ] **End-Users:** This typically refers to customers.

2 Determining the Right Stakeholder

- [ ] **In advance:** Map out your organization by Business Unit (BU) with pre-assign stakeholders for streamlined management.
- [ ] **As you go:** Assign remediation tasks to resource creators using tools like git blame or log tracking in cloud environments.

3 Combine and Automate

- [ ] **Blend:** Combining the approaches of organizational mapping and creator tracking can enable more comprehensive stakeholder identification.
- [ ] **Automate:** Eliminate manual track downs by leveraging tools for automated stakeholder identification and ticket allocation.
- [ ] **Remember to verify:** Ensure the identified stakeholder is still part of the organization.

4 Tackle Cloud Environment Challenges

- [ ] **Enforce EC2 tagging:** Implement system owner tags for AWS EC2 instances.
- [ ] **Retrieve CloudTrail logs:** Check creation events in CloudTrail logs for AWS resources.
- [ ] **Trace back to IaC tools:** In cases where deployment tools like Jenkins are used, refer back to IaC for clarity.

5 Optimize Remediation with the Right Tools

- [ ] **Embrace a technical approach:** Utilize technical queries and integrated tools to streamline your stakeholder identification process.

If you want to dive in and learn,
read our quick guide

Learn more