Evidence as a Service for NIST-Based Audits in Government Agencies

"Simplify NIST audit response with “Evidence as a Service” integrating audit documentation and response and continuous monitoring throughout the software delivery lifecycle."

For organizations like the Department of Defense (DOD), the ability to produce evidence on demand during cybersecurity audits such as FISCAM, CCRI, or NIST-based audits is crucial. Evidence as a Service (EaaS) ensures compliance with regulatory standards and significantly boosts efficiency and understanding of an organization's security posture. Let's delve into why this is so critical.

Evidence as a Service (EaaS) from CloudBees

CloudBees provides the first-of-its-kind Evidence as a Service (EaaS) to provide audit-ready evidence on demand. EaaS works seamlessly with our existing control frameworks. Each framework is a collection of OPA (Open Policy Agent) policies that can be customized based on the organization's risk preference. EaaS automates internal controls and business processes, streamlines audit response, and generates and delivers control evidence with one click.

At the heart of our EaaS solution are Best-in-breed plugin-based integrations to source code management tools, Artifact repositories, CI/CD pipelines, security tools (SAST, DAST, SCA, etc.), and ITSM platforms to detect changes across your SDLC, orchestrate the required security scans in response to these changes, gather the OPA assessments for every change that is detected and provide a near-real-time view of control effectiveness. This continuous assessment process generates audit-ready evidence on demand for each control at the click of a button. This gives you a top-down view of the control effectiveness across every organization and the evidence to substantiate the assessments.

1. Automated DevSecOps

- OOTB best practice cyber control frameworks
- Best in breed integrations across the SDLC
- 90% of effort saved in building IT controls within the pipeline across the enterprise

2. Security Control Assessment (SCA)

- Single pane view of security issues, risk scored based on the application context
- Built-in triage workflow
- Dashboard to manage supply chain risks

3. Continuous Controls Monitoring

- -90% Reduction in time spent in ensuring that teams are adhering to cyber controls set within the organization
- Every team empowered with real time view of control conformity metrics

4. Evidence as a Service

- Audit ready evidence at the click of a button
- Based on near-time data, no more point in tick-boxing

Evidence: The Backbone of Cybersecurity

Government agencies are bound by stringent regulatory and security standards, primarily guided by NIST guidelines. These standards mandate robust cybersecurity practices and require organizations to provide evidence of their adherence to them. Many organizations have implemented various Governance, Risk & Compliance (GRC) tools with the hopes of solving all their compliance woes. The bottom line is that tools can provide compliance indicators but not guarantee them. The only way to ensure and prove compliance is by having the capability to generate and make readily available auditable evidence.

Lack of auditable evidence can lead to severe consequences, including financial penalties and reputational damage. Real-time monitoring of evidence can provide a better understanding of at-risk areas and ultimately prevent a scenario where an overlooked aspect of security leads to a security breach, highlighting the importance of strict adherence to these guidelines.

The Impact of Manual Evidence Collection

The time and resources involved in manual evidence collection during audits can vary greatly. Factors influencing this include the complexity and scope of the audit, the organization's size, the maturity of its cybersecurity processes, and resource availability. In large organizations like the DOD, this can be a daunting task.
For instance, a comprehensive audit covering extensive systems and controls demands significant time and effort. The volume of documentation and the challenge of retrieving specific evidence adds complexity to the process. Furthermore, the need for thorough verification and validation of the evidence prolongs the audit.

In contrast, automated solutions streamline this process. They not only maintain and monitor evidence more efficiently but also minimize disruptions to regular operations by making it simpler to produce for an audit. The use of such tools can transform a week-long documentation marathon into a swift, routine check.

Risk Mitigation: Safeguarding Sensitive Information

The DOD handles highly sensitive and classified information, making the security of this data vital to national security. Continuous monitoring and immediate evidence production enable the quick identification of vulnerabilities and potential security breaches. Prompt action can be taken to mitigate risks before they escalate, much like a well-coordinated response to a breach in a secure facility.

Effective Incident Response: Staying Ahead of Threats

Cybersecurity incidents can occur unexpectedly. With continuous monitoring and the ability to produce evidence swiftly, the DOD can rapidly respond to incidents, investigate their root causes, and implement corrective measures. This quick response minimizes the impact of breaches and aids in preventing future occurrences.

Accountability, Transparency, and Traceability

In any organization, particularly in government agencies, accountability and traceability are key. Providing evidence as a service demonstrates a commitment to transparent and accountable cybersecurity practices that also provide providence and lineage of assets and evidence in your SDLC. It allows auditors and stakeholders to assess the organization's adherence to standards and policies, akin to an open-book examination.

Driving Continuous Improvement

Continuous monitoring and evidence production encourage ongoing enhancement of cybersecurity measures. Regular assessments enable organizations to prioritize and pinpoint improvement areas, fostering informed decisions to bolster security over time.

Conclusion: Embracing Automation in Cybersecurity

In conclusion, the ability to provide evidence as a service during cybersecurity audits is essential for organizations like the DOD. It ensures the evidence is readily available to prove regulatory compliance, enhances security and risk management, and maintains accountability. Implementing a solution like CloudBees EaaS for continuous monitoring and evidence production is a strategic move in today's digital landscape, reducing operational impacts and fostering a robust cybersecurity strategy.

CloudBees, Inc.
4 North Second Street | Suite 1270
San Jose, CA 95113
United States
www.cloudbees.com
info@cloudbees.com