Navigating the FFIEC CAT Sunset and Industry-wide Retirements

The cybersecurity landscape is undergoing significant transformations, marked by the retirement of key assessment tools and the evolution of industry standards. These changes necessitate proactive adaptation by organizations to maintain robust security postures.

FFIEC's Cybersecurity Assessment Tool (CAT) Retirement

The Federal Financial Institutions Examination Council (FFIEC) has announced the retirement of its Cybersecurity Assessment Tool (CAT) effective August 31, 2025. Introduced in 2015, the CAT was designed to help financial institutions assess their cybersecurity risks and preparedness. However, with the advent of more comprehensive frameworks, the FFIEC has decided to discontinue the CAT in favor of these newer resources.

Implications for Financial Institutions

The retirement of the CAT signifies a shift towards more dynamic and adaptable cybersecurity frameworks. Financial institutions are encouraged to transition to alternative tools such as:

- **NIST Cybersecurity Framework 2.0:** Offers a comprehensive approach to managing cybersecurity risks.
- **CISA's Cybersecurity Performance Goals:** Provides a set of practices to enhance cybersecurity across sectors.
- **Cyber Risk Institute’s Cyber Profile:** Tailored for the financial sector, aligning with various regulatory expectations.
- **Center for Internet Security Critical Security Controls:** A set of best practices designed to mitigate prevalent cyber threats.

Transitioning to these frameworks will require institutions to reassess their current cybersecurity strategies, ensure staff are trained on new protocols, and update internal policies to align with the selected framework.

Other Industry Tools Being Retired

Beyond the FFIEC CAT, other notable tools are also being phased out:

- **OSSIM (Open Source Security Information Management):** In December 2024, LevelBlue announced the retirement of OSSIM, an open-source security information and event management system. Organizations relying on OSSIM should seek alternative SIEM solutions to maintain effective security monitoring.
- **SentinelOne's 'Deception' Product Line:** In March 2025, SentinelOne announced the discontinuation of its 'Deception' products, originally acquired from Attivo Networks in 2022. This decision impacts organizations utilizing these products for threat detection and response, necessitating the exploration of alternative deception technologies or compensatory security measures.

Strategic Recommendations for Security & Risk Leaders

1. **Map Your Toolchain to Risk & Business Outcomes**
   Don't just replace a retired tool—re-evaluate its purpose. For each assessment or detection solution you're sunsetting, map its core function to your current risk register and business impact areas. Ask: *Did this tool enable visibility, compliance, detection, or response?* Then match alternatives not just to functionality, but to strategic outcomes—efficiency, audit-readiness, user experience, and incident recovery time.
2. **Build a Sunset-to-Activation Transition Playbook**
   Develop a structured playbook that includes vendor phase-out dates, internal decommissioning timelines, stakeholder impact assessments, and activation windows for the replacement tool or framework. Incorporate cross-functional input—GRC, SecOps, DevOps, Legal, and Procurement—to ensure continuity and avoid dead zones in coverage.
3. **Upskill Beyond the Interface**
   Tools change, but your people stay. Go beyond platform training. Upskill teams on the underlying concepts the tools were built to support—risk-based cybersecurity, zero trust enforcement, behavior analytics, control testing, etc. This makes your team adaptive, not tool-dependent.
4. **Establish Framework Interoperability**
   As you move from the FFIEC CAT to alternatives like the NIST CSF 2.0 or CRI Cyber Profile, create mapping matrices that show how control objectives, metrics, and

maturity levels align. This ensures consistency in reporting to regulators and executive leadership—and avoids the perception that you're "starting from scratch."

5. **Conduct Post-Retirement Reviews**
   Once a tool is retired and replaced, conduct a 90-day post-mortem. Was visibility lost or gained? Are incident response metrics affected? Did user experience improve or degrade? Use these insights to adjust your roadmap, budget justifications, and staffing plans.

6. **Stay Ahead of the Next Wave**
   Monitor CISA, NIST, sector-specific ISACs, and vendor roadmaps for upcoming retirements or consolidations. Proactively set a quarterly "Sunset Watch" session internally to forecast the potential impact of deprecations across your stack—and position security not just as reactive but as operationally foresightful.

Cyber Alchemist's Final Word

In cybersecurity, stagnation is vulnerability. The retirement of legacy tools like the FFIEC CAT and the sunsetting of trusted technologies remind us that resilience isn't about clinging to what worked yesterday—it's about preparing for what's coming tomorrow. The Cyber Alchemist's final word is this: *embrace the change, master the transition, and let obsolescence be the forge that tempers your security posture into something future-ready.* Our tools may change, but our mission—to protect, adapt, and endure—never will.