

Identity security: The must-have checklist for higher education institution attack readiness

14 questions to help protect your institution from identity-based cyber attacks.

Universities manage a massive, decentralized attack surface. Every semester, IT teams must securely onboard tens of thousands of users while navigating siloed directories and legacy systems. The adversary doesn't care about your firewall. They care about faculty credentials and student session tokens. Attackers exploit these tokens, bypass legacy MFA via AiTM proxies, and weaponize dormant service accounts to pivot undetected through research labs and the SIS.

Use this checklist to audit your defense capabilities against the modern threat landscape.

Please note that this checklist is intended only as a component of your overall security program.

PRE-ATTACK

Proactive posture management

This section focuses on resolving misconfigurations and reducing the identity attack surface across decentralized campus departments before an incident occurs.

- Do you continuously validate the identity security posture for both human users, such as students, faculty, and alumni, and non-human identities (service accounts, LMS API keys)?
- **Can you automatically enforce least privilege and validate that there are no MFA bypasses across your legacy campus infrastructure?**
- Do you have a process to identify stale accounts from alumni or partially off-boarded teaching assistants (TAs) who still retain active access to campus resources?
- Is there a system to prioritize and remediate identity misconfigurations and excessive permissions to minimize the blast radius if a student or faculty account is breached?
- **Do you use an identity lens to see exactly which researchers and staff have access to valuable institutional IP and how they authenticate, covering gaps left by CSPM and SSPM tools?**

[Identity Security Posture Management](#)

Continuously discover and remediate identity risks and misconfigurations.

DURING ATTACK

Continuous threat detection and response

This section covers the capabilities needed to detect and respond to threats across the digital campus in real time.

- Have you implemented phishing-resistant authentication (e.g., Okta FastPass) to protect high-value targets like university staff and research labs from credential harvesting?
- Do you continuously monitor session activity and user behavior across the digital campus after initial authentication to detect anomalies and lateral movement?
- **Can you automate inline responses to contain incidents, such as triggering a universal logout across the LMS and student portals, enforcing step-up MFA, or executing custom workflows?**
- **Do you have AI-driven bot protection that mitigates automated credential stuffing against student accounts without adding friction via CAPTCHA?**
- **Does your system continuously assess risk levels from unmanaged devices and off-campus locations to dynamically enforce access policies throughout a session?**

[Identity Threat Protection](#)
Automatically detect and respond to identity-based threats in real time.

[Okta Device Access](#)
Secure device login that hardens protection and simplifies resource access.

[Okta FastPass](#)
Gain Zero Trust security with phishing-resistant, passwordless authentication.

POST-ATTACK

Strengthen identity resilience

This section focuses on improving security posture and incident response after a campus breach has occurred.

- Do you have incident observability tools that can uncover the complete identity attack path across disparate college departments and siloed directories?
- **Is there a system to improve incident handling by correlating identity events and sharing intelligence across your university's security tools?**
- Can you provide compliance assurance by mapping identity controls to FERPA requirements and common frameworks like NIST?
- **Do you have a continuous feedback loop to analyze campus security events and fine-tune responses over time?**

Okta Recognized as an Overall Leader in the 2025 KuppingerCole Leadership Compass for ITDR. [Read more here.](#)

Okta makes it possible

Regardless of your institution's attack readiness, Okta provides the visibility and real-time response capabilities necessary to secure your campus before, during, and after an incident. With visibility into 10 billion global logins and 2 billion blocked threats monthly, Okta sees the tactics, techniques, and procedures others miss. By unifying signals across your SIS, LMS, and legacy IT, Okta enables you to move from reactive defense to proactive resilience. You can eliminate misconfigurations, stop student-targeted phishing, and automate inline responses to contain threats instantly. Learn how to turn your identity layer into your strongest security asset.

About Okta

Okta, Inc. is The World's Identity Company™. We secure Identity, so everyone is free to safely use any technology. Our customer and workforce solutions empower businesses and developers to use the power of Identity to drive security, efficiencies, and success — all while protecting their users, employees, and partners. Learn why the world's leading brands trust Okta for authentication, authorization, and more at okta.com.