Onboarding to Offboarding

The end-to-end secrets scanner checklist

entro

The cybersecurity field has become increasingly complex over the years. This has led us to the point where effective secrets management is not just a matter of following protocol but the backbone that supports the security of all your digital assets.

In this guide, we'll discuss in depth the intricacies of managing employee lifecycles within your organization, highlighting the critical importance of meticulous secrets management and how the two are related. We aim to provide a strategic blueprint for weaving secure practices into every stage of an employee's tenure. We'll dissect the onboarding and offboarding processes, uncovering latent risks and offering solutions to fortify your defenses.

As you read on, you'll gain not just a checklist but a deeper understanding of the principles and practices that make for effective secrets management.

Onboarding: laying the foundation for secure operations

Onboarding is the first step in integrating a culture of security into the fabric of your organization. It's where new hires are equipped with the tools, knowledge, and access they need, set against the backdrop of your security expectations and culture. Making this process comprehensive will not only ensure employees understand their role in safeguarding the organization's assets but also establish a baseline for their ongoing security behavior and awarenes.

To capture the essence of this phase, we've distilled the onboarding process into three focused checklists. Together, they provide a structured and thorough approach to welcoming and securing new members into your organization.

ACCOUNT PROVISIONING AND ACCESS CONTROL

Initiating robust account provisioning and access control are fundamental during the onboarding process. It sets the stage for secure operations and access management throughout an employee's tenure.

ACTION ITEM	DESCRIPTION	TOOLS/ TECHNOLOGY	BEST PRACTICES
Automate user account creation	Utilize automated provisioning tools to minimize errors and ensure consistent permission assignments. Incorporate a secrets management solution to track and manage sensitive access from the start. Entro ensures each account is monitored from the get-go, particularly in environments like GitHub or Slack where secrets might be shared.	Automated provisioning software	Schedule regular audits to ensure accuracy. Update automation rules as roles evolve.
Implement Role-Based Access Control (RBAC)	Assign roles within your provisioning solution and link them to appropriate users.	Access management software	Regularly review and update roles. Ensure roles reflect current job functions and data access needs.
Regularly review user permissions	Monitor user access to ensure permissions remain appropriate, adapting as roles or responsibilities change. Use secrets management insights to identify and address any excessive permissions or risks.	User access review tools	Conduct reviews after any major organizational changes. Use automated alerts for unusual access patterns.

ACTION ITEM	DESCRIPTION	TOOLS/ TECHNOLOGY	BEST PRACTICES
Establish clear policies	Develop definitive policies detailing user account creation, management, and access request processes.	Policy management platform	Clearly communicate policies to all employees. Update policies regularly to reflect changing security landscapes.
Ongoing monitoring and adjustment	Continuously monitor accounts and access patterns, particularly for high-privilege roles or sensitive areas. Adjust access as needed based on behavior, role changes, or emerging risks.	Monitoring tools Behavioral analytics	Implement real-time monitoring for critical roles. Regularly review access logs and patterns.

SECURITY AWARENESS TRAINING

Delivering in-depth security education is vital in preparing employees with the expertise and competencies required to defend themselves and the organization from cyber threats. This training cultivates a security-first mindset, making every employee an active participant in the organization's defense strategy.

ACTION ITEM	DESCRIPTION	TOOLS/ TECHNOLOGY	BEST PRACTICES
Develop training program	Develop a tailored security training curriculum that addresses possible dangers and safe protocols, customized to align with the organization's unique requirements and vulnerabilities.	E-learning platforms Interactive modules	Keep content updated with the latest security trends. Ensure the program is engaging and interactive.
Regular cybersecurity updates	Provide regular updates on new threats and security updates to keep security awareness front and center.	News feeds Email alerts	Schedule routine updates. Use real-world examples to illustrate threats.
Simulated phishing tests	Conduct simulated phishing and social engineering tests to gauge employee response and provide targeted training based on the outcomes.	Phishing simulation tools	Analyze and discuss test results with employees. Provide additional training where necessary.
Review and improve	Regularly review the effectiveness of the training program and make improvements based on feedback and changing security landscapes.	Feedback surveys Training analytics	Conduct post-training assessments. Be open to suggestions and new ideas.

ACTION ITEM	DESCRIPTION	TOOLS/ TECHNOLOGY	BEST PRACTICES
Ongoing monitoring and adjustment	Continuously monitor accounts and access patterns, particularly for high-privilege roles or sensitive areas. Adjust access as needed based on behavior, role changes, or emerging risks.	Monitoring tools Behavioral analytics	Implement real-time monitoring for critical roles. Regularly review access logs and patterns.

DEVICE AND NETWORK SECURITY PROTOCOLS

Ensuring that every device and network interaction is secure is paramount for maintaining the integrity of your organization's data and secrets. This checklist focuses on the necessary protocols and measures to secure hardware and network access effectively.

ACTION ITEM	DESCRIPTION	TOOLS/ TECHNOLOGY	BEST PRACTICES
Secure device configuration	Configure all devices with necessary security settings, including encryption and password protection. Regularly update with the latest security patches.	Device management software Encryption tools	Schedule regular device audits and update sessions.
Install protective software	Equip devices with protective software, including antivirus programs and firewalls, and consistently maintain updated and active software status.	Antivirus software Firewalls	Monitor software status and perform regular scans.
Enable remote management	Set up capabilities for remote tracking, locking, and wiping to protect data in case of device loss or theft.	Remote device management tools Tracking software	Conduct periodic tests of remote capabilities.
Network access control	Implement strict access controls and segmentation to manage who and what can connect to the network.	Access control systems VLANs Firewalls	Regularly review access logs and adjust controls as needed.
Secure wireless communications	Ensure that all wireless communications are encrypted and access is secured, especially for remote work scenarios.	VPNs Secure Wi-Fi protocols	Regularly update VPN and Wi-Fi security settings.

Now that you've got your onboarding down to a fine art, it's time to look at the other side of the coin. Offboarding might not get the spotlight, but it's where you ensure everything wraps up neatly.

Offboarding: protecting assets beyond tenure

Offboarding is as critical as onboarding when it comes to maintaining the security integrity of your organization. It's the process of systematically revoking access, retrieving company assets, and ensuring that no organizational secrets leave with the departing employee.

A meticulously organized offboarding procedure not only safeguards against possible security incidents but also guarantees adherence to legal and regulatory obligations. To comprehensively cover this vital process, we've divided it into three detailed checklists as follows:

ACCOUNT DEACTIVATION AND DATA RETRIEVAL

Ensuring a secure departure means diligently deactivating accounts and retrieving all company assets. A meticulous approach prevents unauthorized access post-departure and protects organizational secrets.

TASK	DESCRIPTION	RESPONSIBILITY	VERIFICATION METHOD
Account deactivation	Systematically deactivate all user accounts across all platforms, including email, intranet, CRM, and any other software with access to sensitive data. Utilize a secrets management solution to identify and address associated secrets and credentials. Schedule these deactivations to occur immediately upon official departure to prevent unauthorized access.	IT & Security team	Confirmation from IT, along with audit logs and a report from the secrets management platform verifying all associated accounts and secrets have been addressed.
Retrieve company assets	Collect all physical company property, such as ID badges, keys, and devices. For digital assets, ensure the return or secure deletion of any company data from the employee's personal devices, cloud storage, and email accounts. This includes documents, contacts, notes, and any downloaded company applications.	HR & IT	A comprehensive checklist of all items to be returned, signed off by the employee, and verification of data deletion or transfer from devices and accounts.

TASK	DESCRIPTION	RESPONSIBILITY	VERIFICATION METHOD
Secrets and credentials audit	Conduct a thorough review of all the secrets and credentials the employee had access to, including API keys, access tokens, and passwords. Determine the sensitivity and exposure risk of these secrets. For critical secrets, especially those in production environments or with access to sensitive data, initiate a rotation or revocation process.	Security team	A detailed audit report listing all accessed secrets, with notes on actions taken (revoked or rotated) and confirmation from the secrets management system.
Data retrieval & secure erase	Ensure that any company data remaining on the departing employee's devices or accounts is either securely transferred back to the company or irretrievably erased. Use data wiping tools that comply with industry standards for secure data deletion. For cloud-stored data, change passwords and revoke access permissions.	IT & Data Protection Officer	Data retrieval confirmations, secure erase verification logs, and updated access lists for cloud storage demonstrating the removal of the departing employee's permissions.

ACCESS REVIEW AND CREDENTIAL MANAGEMENT

As employees depart, it's crucial to ensure that their access to company secrets and systems is thoroughly revoked and managed. This checklist focuses on reviewing and managing credentials and access rights to maintain security and prevent unauthorized use of company resources.

TASK	DESCRIPTION	RESPONSIBILITY	VERIFICATION METHOD
Comprehensive access review	Conduct a detailed review of all the access rights the employee had, including system logins, file permissions, and access to sensitive areas. Utilize a secrets management tool to identify any overlooked access points or credentials related to critical systems.	IT & Security team	Access review report detailing revoked permissions and any changes made.
Revocation of access rights	Systematically revoke all access rights, including remote access, VPN permissions, and access to physical and digital workspaces. Ensure that all forms of access, even those that might be overlooked, like API access or third-party services, are included.	HR & IT	Checklist of all access points with sign-off as each is revoked.

TASK	DESCRIPTION	RESPONSIBILITY	VERIFICATION METHOD
Secrets and key management	Identify and manage all cryptographic keys and secrets the employee had access to. Rotate or revoke keys, especially those providing access to highly sensitive data. A secrets management solution can provide insights into which secrets are most critical and require immediate action.	Security team	A report from the secrets management system detailing key rotations, revocations, and the current status of each.

DATA TRANSFER AND LEGAL COMPLIANCE CHECKLIST

Securely managing the transfer and deletion of company data is essential during offboarding. This checklist ensures compliance with legal standards and protects against data breaches.

TASK	DESCRIPTION	RESPONSIBILITY	VERIFICATION METHOD
Data handover and deletion	Securely transfer or delete all company data from the departing employee's devices and accounts. Use encryption for transfers and certified tools for deletion. Ensure personal data is also handled appropriately.	IT & Data Protection Officer	Confirmation of transfer/deletion and a signed data handover agreement.
Legal and regulatory compliance	Review all actions for compliance with legal agreements and data protection laws. Confirm adherence to confidentiality, non-disclosure, and intellectual property agreements.	HR & Legal Department	Compliance checklist and legal sign-off.
Notification and monitoring	Notify internal and external parties of the employee's departure and new data responsibility. Post-offboarding, monitor for any unauthorized attempts to access or use company data. You can expect Entro to alert you on matters such as that, or any signs of suspicious privilege escalation, ensuring proactive security management at every step.	HR & Security Team	Communication logs and ongoing monitoring reports.

Final thoughts

Onboarding and offboarding? Big deal. Mastering these is less about ticking boxes and more about weaving a tapestry of security that's as intricate as it is invisible.

Maintaining a focus on detailed strategies for secrets management will enhance your security posture and proactively address cybersecurity threats. It's about being not just reactive but strategic, ensuring long-term protection and peace of mind.