IdentitySecurity.net

Top 20 Things Happy Security Admins

Implement Just-in-Time Access (JIT)

Why it makes admins happy:

No more “always-on” admin accounts means fewer attack vectors and a better night’s sleep.

When to use:

When reducing long-standing privileges and ensuring access is only granted on demand.

For more content like and follow me: @bertblevins

Enforce Least Privilege

Why it makes admins happy:
Reduces insider threats and accidental misconfigurations—less cleanup later!

When to use:
RWhen defining role-based access controls (RBAC) and minimizing excessive permissions.

Centralize Privileged Access

Why it makes admins happy:
No more hunting for passwords across multiple systems—everything is in one place.

When to use:
When consolidating access to privileged credentials across IT environments.

Monitor Session Activities

Why it makes admins happy:
If something goes wrong, they have the receipts to prove what happened!

When to use:
When tracking privileged user activities and ensuring compliance with audit requirements.

For more content like and follow me: @bertblevins

Use Multi-Factor Authentication

Why it makes admins happy:
Even if a password is stolen, attackers still can't get in—less worry about breaches.

When to use:
When securing high-risk accounts and mitigating credential compromise risks.

Automate Credential Rotation

Why it makes admins happy:
No more manually changing passwords or worrying about static credentials getting leaked.

When to use:
When managing shared credentials and ensuring password freshness.

Eliminate Hardcoded Credentials

Why it makes admins happy:
Fewer security vulnerabilities and no more developers asking for a spreadsheet of passwords.

When to use:
When securing credentials used in automation, DevOps, and applications.

For more content like and follow me: @bertblevins

Enable Self-Service Access Requests

Why it makes admins happy:
No more being the bottleneck—users get what they need without constant admin intervention.

When to use:
When users require temporary or emergency privileged access.

Integrate PAM with ITSM & SIEM Tools

Why it makes admins happy:
Fewer separate tools to check, easier incident detection, and smoother workflows.

When to use:
When ensuring privileged access events are logged and monitored for anomalies.

Set Up Auto-Revocation for Accounts

Why it makes admins happy:
No more lingering accounts that attackers love to exploit—less manual cleanup too.

When to use:
When enforcing automated lifecycle management for privileged accounts.

For more content like and follow me: @bertblevins

Enforce Zero Standing Privileges

Why it makes admins happy:
Attackers can't compromise what doesn't exist—big win for security!

When to use:
When moving to an on-demand privilege access model.

Run Continuous Access Reviews

Why it makes admins happy:
Avoids privilege creep and awkward compliance audit surprises.

When to use:
When conducting security audits and access governance reviews.

Detect & Respond to Anomalies

Why it makes admins happy:
Faster threat detection means fewer data breaches on their watch.

When to use:
When identifying unusual behavior in privileged accounts.

For more content like and follow me: @bertblevins

Ensure Compliance with Regulations

Why it makes admins happy:
Avoids regulatory fines and impresses auditors—career bonus points!

When to use:
When aligning security controls with industry and regulatory standards.

Use Secure Remote Access

Why it makes admins happy:
No more worrying about external contractors leaving with permanent access

When to use:
When managing third-party privileged access without VPNs or direct credentials.

Educate Users on PAM

Why it makes admins happy:
Fewer “Oops, I clicked on that” incidents—less headache for the security team.

When to use:
When onboarding new employees and reinforcing security culture.

For more content like and follow me: @bertblevins

Gamify Security Awareness

Why it makes admins happy:
Makes security training fun and engaging instead of a chore—users actually pay attention!

When to use:
When fostering a proactive security mindset within the organization.

Leverage AI & Machine Learning

Why it makes admins happy:
AI does the heavy lifting, reducing workload and improving security decisions.

When to use:
When adopting advanced analytics for detecting access anomalies.

Regularly Test Incident Response

Why it makes admins happy:
When a real attack happens, they're ready—not panicked.

When to use:
When preparing for security incidents and breach response exercises.

For more content like and follow me: @bertblevins

IdentitySecurity.net

Share your thoughts in comments below

For more content like and follow me: @bertblevins