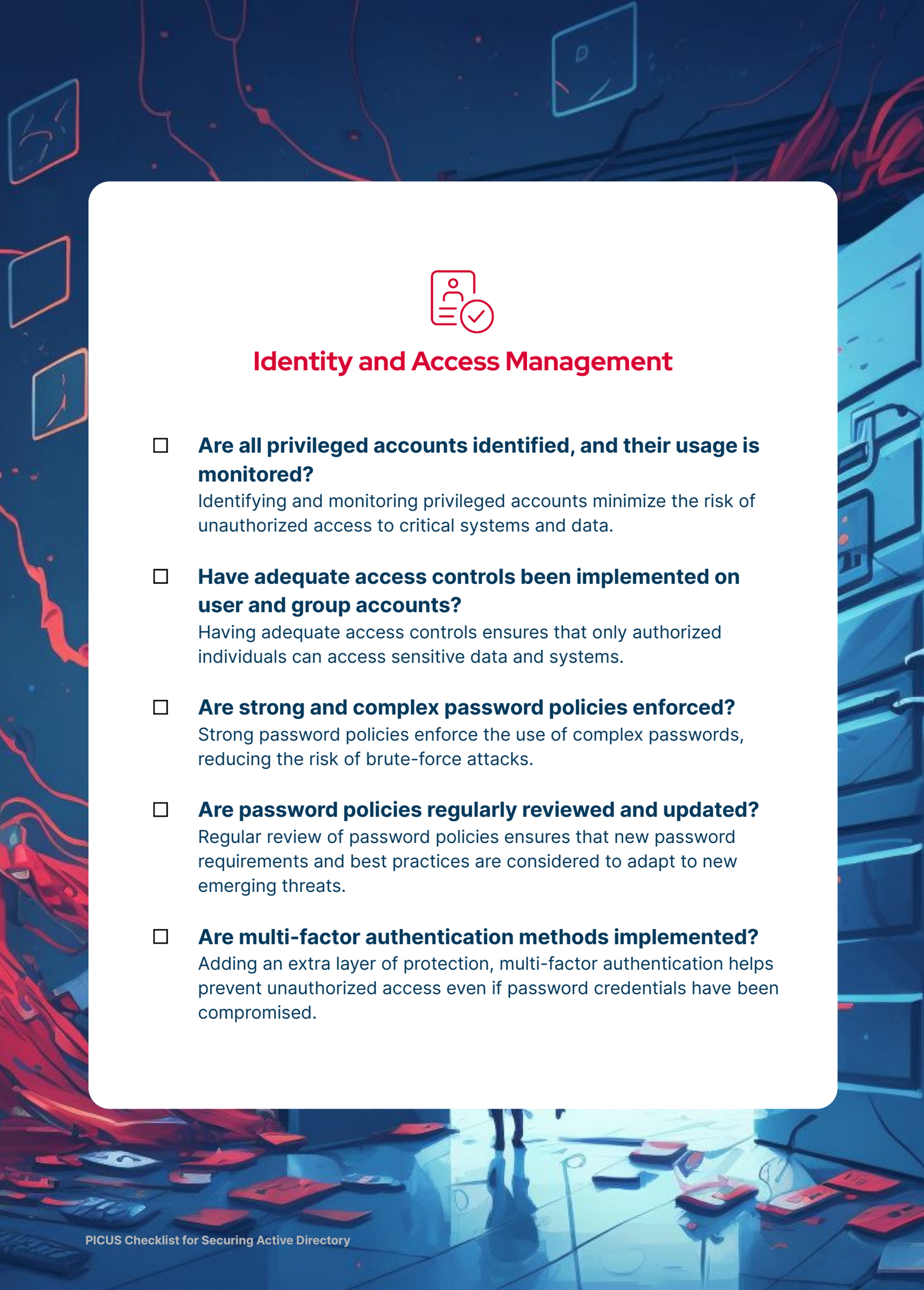
PICUS

Checklist for Securing Active Directory

Why Do You Need an Active Directory Security Checklist?

Securing Active Directory is vital to protect an organization's confidential data, intellectual property, and IT infrastructure against potential cyber threats. A breach in Active Directory could potentially result in catastrophic consequences, such as data breaches, unauthorized entry to resources, and ransomware attacks capable of disrupting business operations.

Hence, having a comprehensive checklist helps organizations secure Active Directory thoroughly. As Picus Security, we have prepared an Active Directory checklist that comprises eight categories with specific questions to identify security threats and vulnerabilities. Addressing these questions can assist organizations in strengthening their security posture, assure Active Directory remains secure and protected against threats of all magnitudes.



Identity and Access Management

- ☐ **Are all privileged accounts identified, and their usage is monitored?**
  Identifying and monitoring privileged accounts minimize the risk of unauthorized access to critical systems and data.

- ☐ **Have adequate access controls been implemented on user and group accounts?**
  Having adequate access controls ensures that only authorized individuals can access sensitive data and systems.

- ☐ **Are strong and complex password policies enforced?**
  Strong password policies enforce the use of complex passwords, reducing the risk of brute-force attacks.

- ☐ **Are password policies regularly reviewed and updated?**
  Regular review of password policies ensures that new password requirements and best practices are considered to adapt to new emerging threats.

- ☐ **Are multi-factor authentication methods implemented?**
  Adding an extra layer of protection, multi-factor authentication helps prevent unauthorized access even if password credentials have been compromised.

Monitoring and Logging

- ☐ **Are Active Directory logs continuously monitored and reviewed for suspicious activities?**
  Continuous monitoring of Active Directory logs enhances early detection of potential cyber threats, reducing detection time and damage.

- ☐ **Are log records regularly backed up and archived?**
  Regular backup and archiving of log records are crucial in forensic analysis and incident response in case of security breaches.

- ☐ **Are security events correlated and analyzed to identify potential threats?**
  Correlating and analyzing security events assist in identifying potential cyber threats, which can help organizations to take appropriate remedial action.

- ☐ **Are security events logged and alerted to appropriate personnel?**
  Logging and alerting of security events can facilitate quick response and timely action during security incidents.

- ☐ **Are changes to Active Directory policies and configurations logged, reviewed, and approved?**
  Logging and monitoring changes to AD policies and configurations can enhance the security posture of AD while preventing unauthorized changes.

Group Policy Management

- ☐ **Are Group Policies regularly reviewed and audited for consistency with security policies?**
  Regular review and audit of Group Policies are essential in identifying and resolving security gaps and non-compliance with security policies.

- ☐ **Are strict controls implemented and enforced on Group Policy Objects (GPO)?**
  Strict controls on GPO prevent unauthorized or malicious changes to security policies, potentially inducing security breaches.

- ☐ **Are Organizational Units (OU) structures well-defined and aligned with security policies?**
  Well-defined OU structures improve Group Policy management and support adequate enforcement of security policies.

- ☐ **Do Group Policies enforce least privilege access?**
  Enforcing least privilege access on Group Policies ensures that users have only the access required to carry out their tasks.

- ☐ **Are Group Policies regularly tested for validation and verification?**
  Testing Group Policies regularly verifies their effectiveness and ensures that they are in line with the security policies of the organization.

Domain Controller (DC) Security

- ☐ **Have physical security controls been implemented and enforced for Domain Controllers?**
  Physical security controls prevent unauthorized physical access to Domain Controllers, reducing the risk of data breaches and cyberattacks.

- ☐ **Are patches and updates regularly applied to Domain Controllers?**
  Regular application of patches and updates ensures that the latest security fixes are implemented, reducing the risk of vulnerabilities being exploited by potential cyber threats.

- ☐ **Are Domain Controllers restricted to only authorized personnel?**
  Restricting access to Domain Controllers to only authorized personnel minimizes the risk of security breaches.

- ☐ **Are Domain Controllers configured to log all security events?**
  Log collection enhances the ability to detect and respond to security incidents quickly.

- ☐ **Are integrity checks performed on Domain Controllers?**
  Performing integrity checks ensures that Domain Controllers are not tampered with, reducing the risk of security breaches.

Attack Path Management

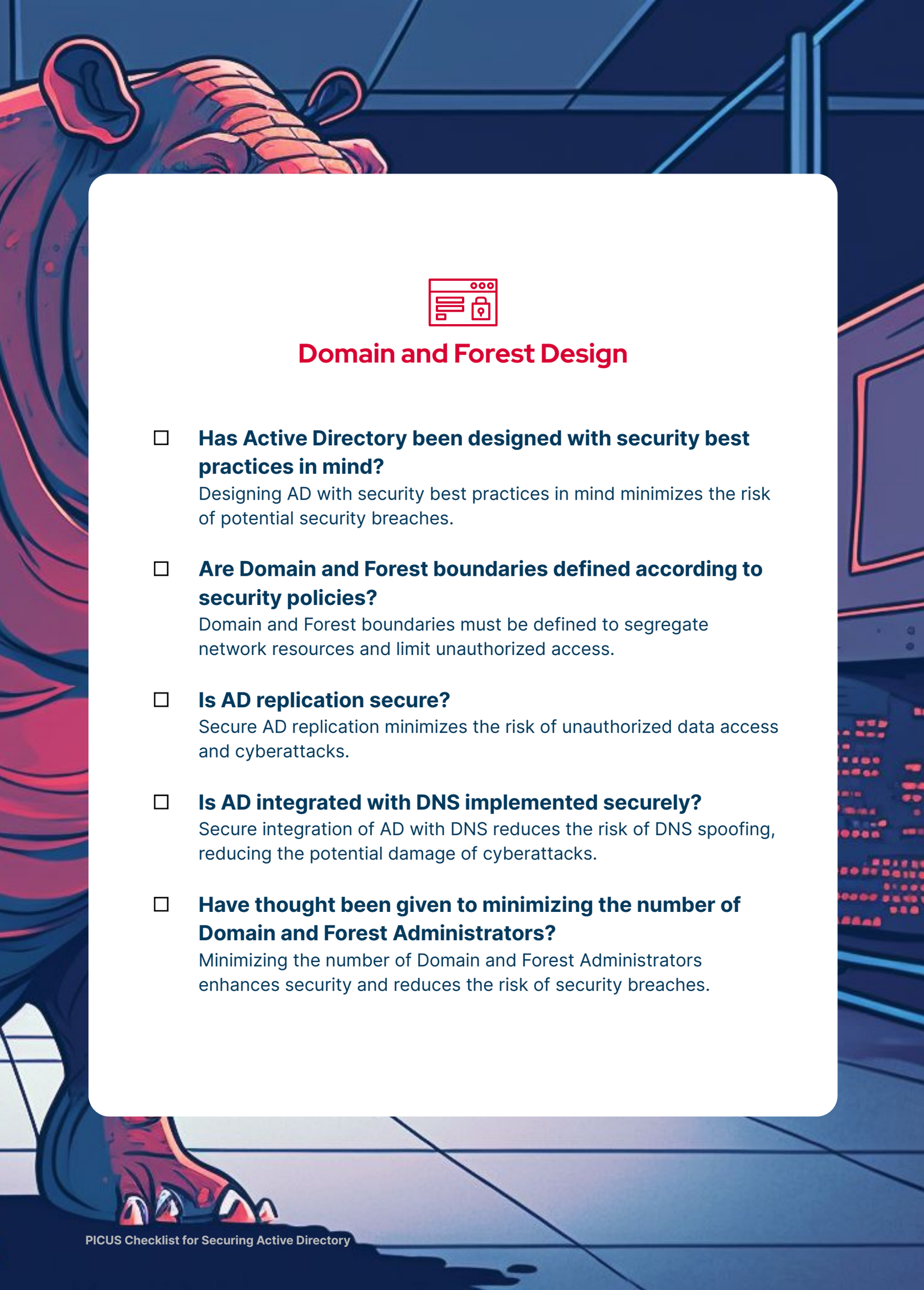
- ☐ **Are automated attack path validation conducted on Active Directory?**
  Regular attack path assessments of Active Directory identify potential security threats before cyberattacks can exploit them.

- ☐ **Are network segmentation and isolation mechanisms in place?**
  Segmentation and isolation mechanisms prevent the spread of security breaches across the Active Directory network, reducing the potential damage of cyberattacks.

- ☐ **Are centralization and standardization of critical processes and infrastructure adopted?**
  Centralization and standardization of processes and infrastructure support consistent deployment and efficient management of security controls.

- ☐ **Has Active Directory replication and trust relationships been implemented securely?**
  Secure implementation of Active Directory replication and trust relationships reduces the risk of unauthorized access and lateral movement within the network.

- ☐ **Are access controls implemented on servers and applications that have access to Active Directory resources?**
  Implementing access controls on servers and applications reduces the risk of unauthorized access to Active Directory resources.



Domain and Forest Design

- ☐ **Has Active Directory been designed with security best practices in mind?**
  Designing AD with security best practices in mind minimizes the risk of potential security breaches.

- ☐ **Are Domain and Forest boundaries defined according to security policies?**
  Domain and Forest boundaries must be defined to segregate network resources and limit unauthorized access.

- ☐ **Is AD replication secure?**
  Secure AD replication minimizes the risk of unauthorized data access and cyberattacks.

- ☐ **Is AD integrated with DNS implemented securely?**
  Secure integration of AD with DNS reduces the risk of DNS spoofing, reducing the potential damage of cyberattacks.

- ☐ **Have thought been given to minimizing the number of Domain and Forest Administrators?**
  Minimizing the number of Domain and Forest Administrators enhances security and reduces the risk of security breaches.

Security Validation

- ☐ **Has automated Security Control Validation implemented?**
  Security Validation via Breach and Attack Simulation ensures that any potential security gaps in Active Directory defenses are identified and remediated promptly.

- ☐ **Has third-party security auditing performed on Active Directory?**
  Third-party security auditing validates the security posture of Active Directory, reducing risk, and identifying ways to improve security measures.

- ☐ **Has a Vulnerability Management Program been adopted?**
  Vulnerability Management Programs assist in identifying, evaluating, and prioritizing security gaps to minimize the risk of cyber threats.

- ☐ **Have Red Team exercises been conducted?**
  Red Team exercises simulate realistic attacks to identify weaknesses in the security infrastructure while providing a valuable avenue to test incident response capabilities.

- ☐ **Has baseline security configuration and change management implemented?**
  Baselining security configuration and change management ensures that there is a known good configuration of Active Directory, minimizing the risk of unauthorized changes.

Recovery and Business Continuity

- ☐ **Are regular system and data backups performed and tested?**
  Regular backups and testing are essential for disaster recovery and business continuity, minimizing the potential impact of cyberattacks.

- ☐ **Are disaster recovery and business continuity plans documented, tested, and reviewed?**
  Disaster recovery and business continuity plans are essential in ensuring that the organization has an effective response plan to security incidents.

- ☐ **Are security incidents properly documented and tracked for follow-up and analysis?**
  Proper documentation of security incidents can be used for forensic analysis and future prevention of similar security incidents.

- ☐ **Has a disaster recovery and business continuity strategy been implemented to meet Service Level Agreements (SLAs)?**
  A disaster recovery and business continuity strategy that meets adequate SLAs ensures minimal impact on the organization's systems and services.

- ☐ **Are regular disaster recovery and business continuity exercises conducted?**
  Conducting regular exercises ensures that the organization is adequately prepared to respond to security incidents, minimizing the potential impact of cyberattacks.

About PICUS

At Picus Security, we help organisations to continuously validate, measure and enhance the effectiveness of their security controls so that they can more accurately assess risks and strengthen cyber resilience.

As **the pioneer of Breach and Attack Simulation (BAS),** our Complete Security Control Validation Platform is used by security teams worldwide to proactively identify security gaps and obtain actionable insights to address them.

www.picussecurity.com

picussecurity