**Notable CAT Gaps (from the CIS Top 20)**

*Note: there are other gaps that you need may need to investigate; we chose these statements based on our own perceived risk for a typical community bank. Your risk profile is surely different from that.*

|  |  |
| --- | --- |
| 1. Limit Access to Script Tools | Limit access to scripting tools (such as Microsoft® PowerShell and Python) to only administrative or development users with the need to access those capabilities. |
| 2. Use Unique Passwords on root and service accounts without MFA. | Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system. |
| 3. Regularly Tune SIEM | On a regular basis, tune your SIEM system to better identify actionable events and decrease event noise. |
| 4. Use Standard Hardening Configuration Templates for Databases | For applications that rely on a database, use standard hardening configuration templates. All systems that are part of critical business processes should also be tested. |
| 5. Segment the Network Based on Sensitivity (In the CAT, but as Intermediate) | Segment the network based on the label or classification level of the information stored on the servers, locate all sensitive information on separated Virtual Local Area Networks (VLANs). |
| 6. Require Multi-Factor Authentication | Require multi-factor authentication for all user accounts, on all systems, whether managed on-site or by a third-party provider. |
| 7. Use of DNS Filtering Services | Use Domain Name System (DNS) filtering services to help block access to known malicious domains. |
| 8. Implement DMARC and Enable Receiver-Side Verification | To lower the chance of spoofed or modified emails from valid domains, implement Domain-based Message Authentication, Reporting and Conformance (DMARC) policy and verification, starting by implementing the Sender Policy Framework (SPF) and the DomainKeys Identified Mail(DKIM) standards. |
| 9. Enable Command-Line Audit Logging | Enable command-line audit logging for command shells, such as Microsoft PowerShell and Bash. |
| 10. Maintain and Enforce Network-Based URL Filters | Enforce network-based URL filters that limit a system's ability to connect to websites not approved by the organization. This filtering shall be enforced for each of the organization's systems, whether they are physically at an organization's facilities or not. |

|  |  |
| --- | --- |
| 11. Utilize an Active Discovery Tool | Utilize an active discovery tool to identify devices connected to the organization's network and update the hardware asset inventory. |
| 12. Apply Host-Based Firewalls or Port-Filtering | Apply host-based firewalls or port-filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed. |
| 13. Disable Unnecessary or Unauthorized Browser or Email Client Plugins | Uninstall or disable any unauthorized browser or email client plugins or add-on applications. |