Secure Future Initiative actions aligned to CSRB

CSRB March 2024 Report recommendations

Section/ Rec #	Microsoft Corporate Security Culture (Rec 1-4)	CSP cybersecurity practices (Rec 5-9)	Audit logging norms (Rec 10)	Digital identity standards and guidance (Rec 11-13)	CSP transparency (Rec 14-17)	Victim notification processes (Rec 18-20)
Secure Future Initiative actions	**Culture, governance, and accountability** CEO and executive leaders mandating SFI and "security above all else" with weekly oversight New cross-company operating model aligned to SFI pillars to drive security-first culture, formation of Deputy CISO governance body Compensation of Microsoft senior leadership team will be partly based on our progress in meeting our security plans and milestones **Monitor and detect threats** Retain 100% of security logs for at least 2 years and make 6 months of appropriate logs available to customers*	**Protect identities and secrets** Protect identity infrastructure signing and platform keys with rapid and automatic rotation with hardware storage and protection (i.e., hardware security module (HSM) and confidential compute) Strengthen identity standards and drive their adoption through use of standard software development kit (SDKs) across 100% of applications* Ensure 100% of identity tokens are protected with stateful/durable validation* Adopt more fine-grained partitioning of identity signing keys and platform keys **Protect engineering systems** 100% of access to source code and engineering systems infrastructure is secured through Zero Trust and least-privilege access policies* **Protect tenants and isolate production systems** Protect 100% of Microsoft, acquired, and employee-created tenants, commerce accounts and tenant resources to the security best practice baselines Ensure only secure, managed, healthy devices will be granted access to Microsoft tenants **Monitor and detect threats** Automatically detect and respond rapidly to anomalous access, behaviors, and configurations across 100% of Microsoft production infrastructure and services Retain 100% of security logs for at least 2 years and make 6 months of appropriate logs available to customers*	**Monitor and detect threats** Retain 100% of security logs for at least 2 years and make 6 months of appropriate logs available to customers*	**Protect identities and secrets** Strengthen identity standards and drive their adoption through use of standard software development kit (SDKs) across 100% of applications* Ensure 100% of identity tokens are protected with stateful/durable validation* **Protect engineering systems** 100% of access to source code and engineering systems infrastructure is secured through Zero Trust and least-privilege access policies*	**Accelerate response and remediation** Increase transparency of mitigated cloud vulnerabilities through the adoption and release of Common Weakness Enumeration (CWE™), and Common Platform Enumeration (CPE™) industry standards for released high severity Common Vulnerabilities and Exposures (CVE) affecting the cloud Improve the accuracy, effectiveness, transparency and velocity of public messaging and customer engagement*	**Accelerate response and remediation** Improve the accuracy, effectiveness, transparency and velocity of public messaging and customer engagement*

* Action is aligned to multiple CSRB recommendations

CSRB recommendations 7,8,12,21-25 are not applicable to Microsoft or CSPs