cybereason

7000+ IRs LATER

The 11 Essential Cybersecurity Controls

Decades in incident response reveal battle-tested cybersecurity controls that minimize attack surface, improve detection and response, reduce incident impact and losses, and build cyber resilience (with compliance mappings for easy implementation).

THE 11 ESSENTIAL CONTROLS WITH AN INCIDENT RESPONDER'S PERSPECTIVE

1. PHISHING-RESISTANT MULTI-FACTOR AUTHENTICATION (MFA)

Traditional MFA can be easily bypassed, so phishing-resistant MFA (such as FIDO2) is now essential. Well-implemented phishing-resistant MFA often stops attackers at the perimeter.

2. ENDPOINT DETECTION & RESPONSE (EDR)

When tuned and monitored, EDR is our fastest path to understanding attacker behavior. Weak or incomplete coverage leaves blind spots.

3. PRIVILEGED ACCESS MANAGEMENT (PAM)

PAM slows down attacker escalation and provides audit trails. Without it, privilege escalation is trivial and blast radius expands exponentially.

4. CENTRALIZED LOGGING & RETENTION (SIEM)

Centralized logs are an investigator's backbone when combined with thorough EDR coverage. Missing, incomplete or short-retention logs cripple response speed and accuracy.

5. PATCHING & VULNERABILITY MANAGEMENT

When patching is mature and timely, we see far fewer preventable intrusions and unauthorized access incidents.

6. EMAIL SECURITY & PHISHING PROTECTION

Phishing is the #1 intrusion vector. Strong controls eliminate entire attack paths; weak controls give attackers easy entry.

7. ASSET INVENTORY & VISIBILITY (IT, OT, CLOUD)

You can't investigate what you don't know exists. Missing inventory wastes time and lets attackers hide in shadow IT.

8. NETWORK SEGMENTATION, ACCESS CONTROLS

Segmentation provides natural containment boundaries. Without it, lateral movement becomes trivial and compounds risks to data.

9. IRP PLANS & TABLETOP EXERCISES

Practiced teams respond faster and more cohesively. Without rehearsals, chaos compounds incident damage.

10. DATA CLASSIFICATION & MANAGEMENT

When data is classified, we can quickly assess exposure and regulatory impact. Without it, extra time is consumed to find fundamental answers.

11. OFFLINE, SEGMENTED, TESTED BACKUPS

Tested offline backups remove leverage from ransomware actors. Unsegmented or untested backups often fail when needed most.

See the full 11 Essential Cybersecurity Controls at
cybereason.com/essentialcontrols

Cybereason experts are available 24x7
response@cybereason.com

#	CONTROL	CIS V8	NIST CSF	NIST 800-171
1	**Multi-Factor Authentication (MFA)**	6.3 – Require MFA for External Apps 6.5 – Require MFA for Admin Access	PR.AC-7 – Users authenticated commensurate with risk	3.5.3 – Use MFA for local and network access
2	**Endpoint Detection & Response (EDR)**	10.1 – Anti-Malware Software 13.1 – Centralize Security Event Alerting	DE.CM-4 – Malicious code detected RS.AN-1 – Detection notifications investigated	3.14.1 – Identify, report, correct flaws 3.14.5 – Perform periodic scans
3	**Privileged Access Management (PAM)**	4.3 – Access Control for Admin Accounts 6.7 – Just-in-Time Privilege Elevation	PR.AC-4 – Permissions managed PR.AC-6 – Identities proofed & bound to credentials	3.1.2 – Limit access to authorized users 3.1.6 – Use least privilege
4	**Centralized Logging & Retention (SIEM)**	8.2 – Enable Audit Logging 8.3 – Collect Detailed Logs 8.5 – Retain Logs	DE.AE-3 – Event data aggregated & correlated PR.PT-1 – Audit/log records documented	3.3.1 – Create & retain audit logs 3.3.6 – Audit reduction & reporting
5	**Regular Patching & Vulnerability Mgmt**	7.3 – Apply Vendor Updates 7.5 – Automate Patch Management	PR.IP-12 – Vulnerability management implemented DE.CM-8 – Vulnerability scans performed	3.11.2 – Scan for vulnerabilities 3.14.1 – Identify, report, correct flaws
6	**Email Security & Phishing Protection**	9.1 – Block Phishing 9.2 – DNS Filtering 14.6 – Train on Phishing	PR.AT-1 – Training DE.CM-7 – Monitor email attachments PR.DS-2 – Data in transit protected	3.1.17 – Protect email 3.13.8 – Implement email protections 3.2.1 – Train to recognize threats
7	**Asset Inventory & Visibility (IT, OT, Cloud)**	1.1 – Asset Inventory 1.2 – Address Unauthorized Assets 2.1 – Software Inventory	ID.AM-1 – Devices inventoried ID.AM-2 – Software inventoried ID.AM-4 – External systems catalogued	3.4.1 – Maintain baselines & inventories 3.1.1 – Limit access to authorized users/devices
8	**Network Segmentation & Access Controls**	3.3 – Firewall Rules 14.4 – Segment Privileged Access 12.1 – Centralize Access Control	PR.AC-5 – Network integrity protected PR.PT-4 – Communications protected	3.1.3 – Control flow of CUI 3.1.20 – Control external connections
9	**Incident Response Plan & Tabletop Exercises**	17.1 – Assign Incident Managers 17.2 – Contact Authorities 17.4 – Conduct Exercises	RS.RP-1 – Response plan executed RS.IM-1 – Strategies tested & updated	3.6.1 – Incident-handling capability 3.6.2 – Track/report incidents 3.6.3 – Test IR capability
10	**Data Classification & Structured Data Mgmt**	3.4 – Inventory Data 3.6 – Encrypt Data 3.7 – Data Classification Scheme	ID.RA-1 – Vulnerabilities documented PR.DS-1 – Data-at-rest protected PR.DS-5 – Prevent leaks	3.1.22 – Control CUI in public systems 3.8.1 – Protect CUI 3.8.3 – Mark & label CUI
11	**Offline, Segmented, Tested Backups (RTO Validation)**	11.4 – Protect Recovery Data 11.5 – Automated Backups 11.6 – Restoration Tests	PR.IP-4 – Backups protected & tested PR.PT-5 – Recovery tested RC.RP-1 – Recovery plan maintained	3.6.1 – Incident-handling capability 3.6.2 – Document/report incidents 3.1.1 – Limit backup access