LevelBlue

9,000+ IRs later:
The 11 essential cybersecurity controls

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

The 11 essential cybersecurity controls with an incident responder's perspective

01

Phishing-resistant multi-factor authentication (MFA)
Traditional MFA can be easily bypassed using stolen credentials or common phishing kits. Well-implemented phishing-resistant MFA (such as FIDO2) is strongly recommended for stopping attacks at the perimeter.

02

Endpoint detection & response (EDR)
EDR gives defenders near real-time and historical visibility into attacker behaviors. It's an essential tool for early detection and rapid containment.

03

Privileged access management (PAM)
PAM protects high-value systems, accounts, and data by slowing down attacker escalation and providing audit trails. Applying Zero Trust to privileged access limits lateral movement and reduces the attack surface, verifying every elevation request.

04

Centralized logging & retention (SIEM)
Collecting and preserving logs into a SIEM platform is crucial for incident response investigations, regulatory compliance, and overall cyber resilience. Missing, incomplete, or short-retention logs can slow response speed and accuracy.

05

Patching & vulnerability management
Unpatched vulnerabilities are one of the most reliable entry points for attackers. Timely patching, configuration management, and security updates reduce the attack surface and prevent intrusions before they begin.

06

Email security filtering & phishing protection
Phishing and social engineering remain the leading intrusion vector based on LevelBlue incident response data. Strong email controls block many threats before they reach users and prevent against easy entry.

07

Asset inventory & visibility (IT, OT, cloud)
Having a current, accurate inventory of your assets is foundational. Attackers exploit unmanaged and unmonitored systems, especially in hybrid and cloud-heavy environments. Visibility underpins patching, access control, and incident response.

08

Network segmentation, access controls
Segmentation provides natural containment boundaries. Modern implementations extend it with Zero Trust for continuous identity verification, and with Secure Access Service Edge (SASE) architectures that enforce segmentation and access policy across branch, cloud, and remote users.

09

IRP & tabletop excercises
Practiced teams respond faster and more cohesively, speeding up containment. Tabletop exercises uncover process gaps, validate assumptions, and strengthen relationships across legal, IT, PR, and leadership teams before an actual intrusion occurs.

10

Data classification & management
When structured and unstructured data is classified and controls are implemented to manage, protect, and govern it, organizations can quickly assess exposure, regulatory impact, and prioritize protections.

11

Offline, segmented, tested backups
Tested offline backups remove leverage from ransomware actors and serve as a critical last line of defense. The other 10 controls are more impactful in preventing and containing attacks before they cause damage.

Learn More

See the full 11 essential cybersecurity controls at:
levelblue.com/essential-controls

LevelBlue experts are available 24×7
levelblue.com/irr

Framework	CIS Controls v8.1	NIST CSF 2.0	NIST SP 800-171 Rev 2
Multi-factor authentication	6.3 – Require MFA for externally-exposed applications 6.4 – Require MFA for remote network access 6.5 – Require MFA for administrative access	PR.AA-01 – Identities and credentials for authorized users, services, and hardware are managed PR.AA-03 – Users, services, and hardware are authenticated	3.5.1 – Identify system users and processes 3.5.2 – Authenticate identities 3.5.3 – Use MFA for local and network access
Endpoint detection & response	10.1 – Deploy and maintain anti-malware software 10.7 – Use behavior-based anti-malware software 13.1 – Centralize security event alerting 13.7 – Deploy a host-based intrusion prevention solution	DE.CM-09 – Computing hardware and software and their data are monitored to find potentially adverse events DE.AE-02 – Potentially adverse events are analyzed to better understand associated activities	3.14.2 – Provide protection from malicious code 3.14.6 – Monitor systems to detect attacks and indicators of potential attacks 3.14.7 – Identify unauthorized use of systems
Privileged access management	5.4 – Restrict administrator privileges to dedicated administrator accounts 6.8 – Define and maintain role-based access control	PR.AA-05 – Access permissions, entitlements, and authorizations are defined, managed, enforced, and reviewed, incorporating least privilege and separation of duties PR.AA-01 – Identities and credentials are managed	3.1.5 – Employ the principle of least privilege 3.1.6 – Use non-privileged accounts for non-security functions 3.1.7 – Prevent non-privileged users from executing privileged functions
Centralized logging & retention (SIEM)	8.2 – Collect audit logs 8.5 – Collect detailed audit logs 8.9 – Centralize audit logs 8.10 – Retain audit logs	PR.PS-04 – Log records are generated and made available for continuous monitoring DE.AE-03 – Information is correlated from multiple sources	3.3.1 – Create and retain system audit logs and records 3.3.2 – Ensure actions can be traced to individual users 3.3.6 – Provide audit record reduction and report generation
Patching, vulnerability management	7.3 – Perform automated operating system patch management 7.4 – Perform automated application patch management 7.7 – Remediate detected vulnerabilities	ID.RA-01 – Vulnerabilities in assets are identified, validated, and recorded PR.PS-02 – Software is maintained, replaced, and removed commensurate with risk ID.RA-06 – Risk responses are chosen, prioritized, planned, tracked, and communicated	3.11.2 – Scan for vulnerabilities 3.11.3 – Remediate vulnerabilities in accordance with risk assessments 3.14.1 – Identify, report, and correct system flaws
Email security, phishing protection	9.2 – Use DNS filtering services 9.5 – Implement DMARC 9.6 – Block unnecessary file types 9.7 – Deploy and maintain email server anti-malware protections 14.2 – Train workforce members to recognize social engineering attacks	DE.CM-09 – Computing hardware and software and their data are monitored to find potentially adverse events PR.AT-01 – Personnel are provided awareness and training PR.DS-02 – Data-in-transit is protected	3.2.1 – Make personnel aware of security risks 3.2.2 – Train personnel to carry out their security duties 3.14.2 – Provide protection from malicious code
Asset inventory & visibility	1.1 – Establish and maintain detailed enterprise asset inventory 1.2 – Address unauthorized assets 2.1 – Establish and maintain a software inventory	ID.AM-01 – Inventories of hardware managed by the organization are maintained ID.AM-02 – Inventories of software, services, and systems are maintained ID.AM-05 – Assets are prioritized based on classification, criticality, resources, and impact on the mission	3.4.1 – Establish and maintain baseline configurations and inventories 3.4.2 – Establish and enforce security configuration settings
Network segmentation, access controls	3.12 – Segment data processing and storage based on sensitivity 12.2 – Establish and maintain a secure network architecture 13.4 – Perform traffic filtering between network segments	PR.IR-01 – Networks and environments are protected from unauthorized logical access and usage PR.AA-05 – Access permissions and authorizations are defined, managed, enforced, and reviewed	3.1.3 – Control the flow of CUI in accordance with approved authorizations 3.13.1 – Monitor, control, and protect communications at system boundaries 3.13.5 – Implement subnetworks for publicly accessible system components
Incident response plans, tabletop exercises	17.1 – Designate personnel to manage incident handling 17.4 – Establish and maintain an incident response process 17.7 – Conduct routine incident response exercises	RS.MA-01 – The incident response plan is executed in coordination with relevant third parties once an incident is declared ID.IM-02 – Improvements are identified from security tests and exercises	3.6.1 – Establish an operational incident-handling capability 3.6.2 – Track, document, and report incidents 3.6.3 – Test the organizational incident response capability
Data classification & management	3.1 – Establish and maintain a data management process 3.2 – Establish and maintain a data inventory 3.7 – Establish and maintain a data classification scheme	ID.AM-07 – Inventories of data and corresponding metadata for designated data types are maintained PR.DS-01 – The confidentiality, integrity, and availability of data-at-rest are protected	3.8.1 – Protect CUI on system media 3.8.4 – Mark media with necessary CUI markings 3.1.22 – Control CUI posted or processed on publicly accessible systems
Offline, segmented, tested backups	11.3 – Protect recovery data 11.4 – Establish and maintain an isolated instance of recovery data 11.5 – Test data recovery	PR.DS-11 – Backups of data are created, protected, maintained, and tested RC.RP-03 – The integrity of backups and other restoration assets is verified before using them for restoration RC.RP-01 – The recovery portion of the incident response plan is executed	3.8.9 – Protect the confidentiality of backup CUI at storage locations *800-171 Rev 2 has thin backup/recovery coverage; the contingency-planning family lives in 800-53. 3.8.9 is the closest direct fit.