BEAR

Defensive Control Mapping

Break → Expand → Ascend → Rule

Defensive Control Mapping by

Christopher Six

The Architect & Author

Version 1.1 | January 2025

Standards Referenced:

NIST CSF 2.0 | ISO 27001:2022 | CIS Controls v8 | MITRE ATT&CK v14

BEAR Framework Concept by Ivan Novikov (Wallarm)

What is BEAR?

A practitioner's model for when speed matters

The Problem

MITRE ATT&CK is perfect for building detections. Lockheed Kill Chain is great for campaign analysis. But in the heat of an engagement or incident — they're overhead, not guidance. Too many boxes. Not enough focus.

The Solution

BEAR cuts through the noise with four questions that matter:

	Phase	Key Question	Transition
B	BREAK	Did they get in?	Outside → Inside
E	EXPAND	How far did they move?	One → Many
A	ASCEND	Did they get real power?	User → Admin
R	RULE	What can they do now?	Access → Impact

When to Use

Scenario	How BEAR Helps
Active Incident	Quickly assess where the attacker is and what's at risk
Red Team Debrief	Structure findings by impact, not just technique
Control Validation	Test defenses at each phase, find the gaps
Executive Briefing	Translate technical status into business risk

Where BEAR Sits vs MITRE and Lockheed

BEAR is not a replacement for MITRE ATT&CK or the Lockheed Kill Chain — it's a complement. Use MITRE for describing techniques and building detections. Use Kill Chain for thinking about campaigns and defense in depth. Use BEAR when you're in the middle of the action and need to cut through the noise fast.

BEAR	MITRE ATT&CK Tactics	Lockheed Kill Chain
Break	Initial Access, Execution	Exploitation, Installation
Expand	Discovery, Lateral Movement, Persistence	Installation, C2
Ascend	Privilege Escalation, Credential Access	C2, Actions on Objectives
Rule	Collection, Exfiltration, Impact	Actions on Objectives

Quick Reference

Phase	Key Question	Primary Focus	Top Controls
BREAKOutside → Inside	Did they get in?	Initial AccessExecution	MFA, Patching, WAF
EXPANDOne → Many	How far did they move?	Lateral MovementPersistence	Segmentation, EDR, ZTNA
ASCENDUser → Admin	Did they get real power?	Privilege EscalationCredential Access	PAM, AD Tiering, LAPS
RULEAccess → Impact	What can they do now?	CollectionExfiltrationImpact	Immutable Backups, DLP, IR

Control Prioritization by Phase

Phase	Focus	Top 3 Controls
BREAK	Prevent initial access	MFA everywhere, vulnerability management, WAF
EXPAND	Slow lateral movement	Network segmentation, EDR, Zero Trust
ASCEND	Limit blast radius	PAM, AD tiering, credential protection
RULE	Minimize impact	Immutable backups, DLP, incident response

• Phase: BREAK

"The moment outside becomes inside"

Attacker Objectives

→ Exploit web/API vulnerabilities
→ Abuse broken authentication flows
→ Leverage misconfigured edge services
→ Compromise forgotten or legacy VPNs
→ Achieve initial code execution

Defensive Controls

Attack Surface Management

Control	NIST CSF 2.0	ISO 27001	CIS v8
External asset inventory	ID.AM-1, ID.AM-2	A.5.9	1.1, 2.1
Continuous vulnerability scanning	ID.RA-1	A.8.8	7.1, 7.2
Attack surface monitoring	ID.RA-2	A.5.7	7.7
Shadow IT discovery	ID.AM-1	A.5.9	1.1, 2.1

Perimeter Hardening

Control	NIST CSF 2.0	ISO 27001	CIS v8
Web Application Firewall (WAF)	PR.DS-1	A.8.20	13.10
API gateway security	PR.DS-1	A.8.20	13.10
Edge configuration hardening	PR.PT-3	A.8.9	4.1, 4.2
VPN hardening & MFA	PR.AC-7	A.8.5	6.3, 6.4

Authentication Controls

Control	NIST CSF 2.0	ISO 27001	CIS v8
Multi-factor authentication	PR.AC-7	A.8.5	6.3, 6.4, 6.5
Conditional access policies	PR.AC-4	A.8.2	6.7
Password policy enforcement	PR.AC-1	A.5.17	5.2
Brute force protection	PR.AC-7	A.8.5	6.3
Authentication anomaly detection	DE.AE-1	A.8.16	8.11

Detection Opportunities

Indicator	Data Source	Detection Logic
Failed authentication spikes	IAM logs, VPN logs	Threshold alerting by source
Anomalous geographic access	Auth logs	Impossible travel detection
Exploit signature matches	WAF, IDS/IPS	Signature-based detection

Unusual API call patterns	API gateway logs	Baseline deviation

Key Metrics

• Mean Time to Patch (MTTP) for external-facing systems
• Percentage of external assets with MFA enforcement
• External vulnerability scan coverage
• Time from vulnerability disclosure to remediation

● Phase: EXPAND

"Turn one foothold into many options"

Attacker Objectives

→ Move to internal applications
→ Access file shares and data repositories
→ Pivot to cloud resources (Azure, AWS, GCP)
→ Compromise Kubernetes clusters
→ Access SaaS admin panels
→ Establish persistence mechanisms

Defensive Controls

Network Segmentation

Control	NIST CSF 2.0	ISO 27001	CIS v8
Network segmentation	PR.AC-5	A.8.22	12.2
Micro-segmentation	PR.AC-5	A.8.22	12.2
Zero trust network access (ZTNA)	PR.AC-5	A.8.22	12.8
East-west traffic inspection	DE.CM-1	A.8.16	13.3

Behavior Drift Detection

Control	NIST CSF 2.0	ISO 27001	CIS v8
User behavior baselining	DE.AE-1	A.8.16	8.11
Anomalous access detection	DE.CM-3	A.8.16	8.11
Peer group analysis	DE.AE-1	A.8.16	8.11
Session behavior monitoring	DE.CM-3	A.8.16	8.11
Lateral movement scoring	DE.AE-1	A.8.16	8.11

Endpoint Controls

Control	NIST CSF 2.0	ISO 27001	CIS v8
EDR deployment	DE.CM-4	A.8.7	10.1
Host-based firewall	PR.PT-4	A.8.20	13.1
Application whitelisting	PR.PT-3	A.8.19	2.5, 2.6
Endpoint hardening	PR.PT-3	A.8.9	4.1

Cloud Security

Control	NIST CSF 2.0	ISO 27001	CIS v8
Cloud Security Posture Mgmt (CSPM)	ID.AM-5	A.5.23	3.1
Cloud workload protection (CWPP)	DE.CM-4	A.8.7	10.1

Kubernetes security (KSPM)	ID.AM-5	A.5.23	3.1
Cloud IAM hygiene	PR.AC-4	A.5.18	5.4

Detection Opportunities

Indicator	Data Source	Detection Logic
Lateral movement patterns	EDR, network flow	SMB/WinRM/RDP unusual hosts
Internal reconnaissance	DNS, LDAP logs	LDAP enum, port scanning
New persistence mechanisms	EDR, Windows Events	Scheduled tasks, services
Unusual cloud API calls	Cloud audit logs	First-time API by principal
Behavioral baseline deviation	Behavior analytics	Anomaly score threshold breach

Key Metrics

• Segmentation effectiveness score
• Mean dwell time (detection to containment)
• Lateral movement detection rate
• Percentage of hosts with EDR coverage
• Behavior drift alert-to-investigation ratio

• Phase: ASCEND

"Get real power"

Attacker Objectives

→ Local privilege escalation (LPE) to root/SYSTEM
→ Domain Admin compromise
→ Kubernetes cluster-admin access
→ Powerful cloud IAM roles (Azure Contributor, AWS Admin)
→ CI/CD pipeline control
→ Certificate authority compromise

Defensive Controls

Privileged Access Management

Control	NIST CSF 2.0	ISO 27001	CIS v8
Privileged Access Workstations (PAWs)	PR.AC-4	A.8.2	12.6
Privileged Identity Management (PIM)	PR.AC-4	A.5.18	5.4, 6.1
Just-in-time elevation	PR.AC-4	A.5.18	6.1
Credential vaulting	PR.DS-5	A.5.17	5.2

Credential Protection

Control	NIST CSF 2.0	ISO 27001	CIS v8
LAPS / Windows LAPS	PR.DS-5	A.5.17	5.2
Credential Guard	PR.DS-5	A.8.9	10.5
Protected Users group	PR.DS-5	A.5.17	5.4
Kerberos hardening	PR.DS-5	A.5.17	5.4

Active Directory Security

Control	NIST CSF 2.0	ISO 27001	CIS v8
AD tiering model	PR.AC-4	A.8.2	5.4
AdminSDHolder monitoring	DE.CM-3	A.8.16	5.4
DCSync attack detection	DE.CM-3	A.8.16	8.5
GPO change monitoring	DE.CM-3	A.8.16	8.5

Privileged Behavior Analytics

Control	NIST CSF 2.0	ISO 27001	CIS v8
Admin activity baselining	DE.AE-1	A.8.16	8.11
Abnormal privilege usage detection	DE.CM-3	A.8.16	8.11
First-time elevation alerting	DE.AE-1	A.8.16	8.11

Service account behavior monitoring	DE.CM-3	A.8.16	8.11

Detection Opportunities

Indicator	Data Source	Detection Logic
Privilege escalation attempts	EDR, Windows Events	Token manipulation, UAC bypass
Sensitive group modifications	AD audit logs	DA, EA, Schema Admin changes
Kerberoasting activity	AD logs	Unusual TGS requests for SPNs
DCSync indicators	AD logs	Replication from non-DC

Key Metrics

- Number of standing privileged accounts
- Privileged access review frequency
- Mean time to detect privilege escalation
- Percentage of admins using PAWs

• Phase: RULE

"Use that power to shape reality"

Attacker Objectives

→ Establish quiet persistence (survive detection/remediation)
→ Own production environments
→ Stage future extortion capability
→ Data exfiltration
→ Destructive capability (ransomware, wiper)
→ Supply chain compromise

Defensive Controls

Data Protection

Control	NIST CSF 2.0	ISO 27001	CIS v8
Data classification	ID.AM-5	A.5.12	3.1, 3.7
Data Loss Prevention (DLP)	PR.DS-5	A.8.12	3.13
Encryption at rest/in transit	PR.DS-1, PR.DS-2	A.8.24	3.10, 3.11
Database activity monitoring	DE.CM-7	A.8.16	3.14

Backup & Recovery

Control	NIST CSF 2.0	ISO 27001	CIS v8
Immutable backups	PR.IP-4	A.8.13	11.2
Air-gapped backup copies	PR.IP-4	A.8.13	11.4
Backup integrity verification	PR.IP-4	A.8.13	11.3
Recovery time testing	RC.RP-1	A.5.30	11.5

Data Access Analytics

Control	NIST CSF 2.0	ISO 27001	CIS v8
Data access baselining	DE.AE-1	A.8.16	8.11
Bulk download detection	DE.CM-3	A.8.16	8.11
Anomalous data movement	DE.AE-1	A.8.16	8.11
After-hours access alerting	DE.CM-3	A.8.16	8.11

Resilience & Business Continuity

Control	NIST CSF 2.0	ISO 27001	CIS v8
Business continuity planning	RC.RP-1	A.5.30	11.1
Disaster recovery testing	RC.RP-1	A.5.30	11.5
Incident response plan	RS.RP-1	A.5.24	17.1-17.9

Communication plans	RS.CO-2	A.5.24	17.3

Detection Opportunities

Indicator	Data Source	Detection Logic
Large data transfers	Network flow, proxy	Volume anomaly external
DNS tunneling	DNS logs	High entropy subdomains
Shadow admin accounts	IAM logs	New accounts with admin rights
Backup deletion/modification	Backup system logs	Unusual backup operations

Key Metrics

• Data exfiltration detection rate
• Backup recovery success rate (tested)
• Mean time to recover (MTTR)
• Percentage of critical data classified

Change Log:

Version	Change	By:
v1.0	Base Document	C. Six
v1.1	Added	Behavior Drift

Change Rational:

Behavior drift (think UBEA, UBA)is a cross-cutting capability that spans all four BEAR phases.. It has been placed in "expand" as that's where dwell time detection matters most, with callouts in other phases.

BEAR is the “cut through the noise” layer and MITRE is where you go for the comprehensive mapping.

The framework’s value is in the speed and focus, not exhaustive coverage.