SCOPE Framework: Threat Management & Security Operations Control Domain

Table of Contents

Originating Component	SCOPE Framework Governance Committee
Releasability	Cleared for public distribution. Available in the SCOPE Framework Hub at [https://timtiptonjr.com/scope-hub].

Purpose: The Threat Management & Security Operations domain establishes the capabilities, processes, and supporting infrastructure required to detect, analyze, respond to, and anticipate cyber threats in real time. This domain encompasses incident response, threat intelligence, continuous monitoring, endpoint defense, adversarial simulations, and malware forensics—each contributing to a holistic and proactive security operations ecosystem. By aligning operational security functions with intelligence-driven insights and layered defenses, the organization can rapidly detect emerging threats, minimize impact, and continuously adapt to an evolving threat landscape while maintaining operational integrity and mission assurance.

Section 1. Incident Detection & Response (IDR)

The Incident Detection & Response (IDR) control family establishes the necessary mechanisms, procedures, and capabilities to detect, analyze, respond to, and recover from cybersecurity incidents in a timely and effective manner. This control family prioritizes operational readiness, cross-functional coordination, and continuous improvement to ensure that incidents are not only addressed but also used as catalysts for enhancing the broader security posture.

1.1 IDR-01: Incident Detection Capabilities

The organization shall implement and maintain detection mechanisms capable of identifying anomalous activity, unauthorized access, policy violations, and known or suspected cyber threats across its environment.

1.2 IDR-02: Incident Categorization and Classification

The organization shall establish and use a standardized taxonomy for categorizing and classifying incidents by severity, type, and potential impact, ensuring consistent triage and prioritization.

1.3 IDR-03: Incident Reporting Procedures

The organization shall develop and disseminate procedures for internal and external personnel to report suspected or confirmed incidents through secure and reliable channels.

1.4 IDR-04: Centralized Incident Management System

The organization shall utilize a centralized system for tracking, documenting, and managing the lifecycle of security incidents from detection through resolution and post-incident review.

1.5 IDR-05: 24/7 Monitoring and Alerting

The organization shall maintain continuous monitoring and automated alerting capabilities to ensure immediate detection and escalation of high-priority incidents.

1.6 IDR-06: Initial Incident Response

The organization shall define and implement processes to perform rapid containment, investigation, and mitigation of detected incidents in alignment with their classification.

1.7 IDR-07: Incident Response Plan (IRP)

The organization shall develop, maintain, and regularly test an incident response plan that defines roles, responsibilities, procedures, escalation paths, and communication protocols.

1.8 IDR-08: Role-Based Response Procedures

The organization shall define role-based incident response playbooks to guide technical and non-technical stakeholders during various incident scenarios.

1.9 IDR-09: Evidence Preservation and Chain of Custody

The organization shall implement procedures for collecting, preserving, and documenting digital evidence with an established chain of custody to support investigations and potential legal proceedings.

1.10 IDR-10: External Reporting and Notification Obligations

The organization shall identify and fulfill external incident reporting and notification requirements, including regulatory, legal, contractual, and stakeholder obligations, within required timeframes.

1.11 IDR-11: Threat Actor Attribution Support

The organization shall incorporate intelligence analysis, behavior profiling, and forensic data to assist in attributing incidents to known or suspected threat actors where feasible.

1.12 IDR-12: Integration with Threat Intelligence

The organization shall leverage threat intelligence to enrich incident data, contextualize attacks, and refine response strategies in real time.

1.13 IDR-13: Interdepartmental Coordination

The organization shall establish coordination protocols between cybersecurity, legal, public affairs, human resources, and business units during incident response activities.

1.14 IDR-14: Legal and Regulatory Coordination

The organization shall include legal counsel in incident response procedures to guide decisions related to liability, privilege, disclosure, and potential prosecution.

1.15 IDR-15: Incident Escalation Criteria

The organization shall define criteria and thresholds for escalating incidents to executive leadership, incident response teams, or external entities based on severity and impact.

1.16 IDR-16: Post-Incident Analysis and Lessons Learned

The organization shall conduct structured post-incident reviews to identify root causes, evaluate response effectiveness, and document opportunities for improvement.

1.17 IDR-17: Remediation and Recovery

The organization shall implement remediation plans to eliminate vulnerabilities exploited during an incident and validate recovery before full system restoration.

1.18 IDR-18: Incident Metrics and Reporting

The organization shall track and report key performance indicators (KPIs) and metrics related to incident detection, response time, recovery duration, and recurrence rates.

1.19 IDR-19: Continuous Improvement Program

The organization shall maintain a continuous improvement process for incident response by incorporating lessons learned, control gaps, and changes in the threat landscape.

1.20 IDR-20: Tabletop Exercises and Simulations

The organization shall conduct periodic tabletop exercises and real-world simulations involving relevant personnel to validate the effectiveness of incident response capabilities and readiness.

1.21 IDR-21: Supply Chain Incident Coordination

The organization shall define procedures for identifying and coordinating responses to incidents affecting or originating from third-party suppliers and service providers.

1.22 IDR-22: Insider Threat Incident Response

The organization shall maintain dedicated procedures for detecting and responding to insider threats, including intentional and unintentional acts by trusted individuals.

1.23 IDR-23: Communication During Incidents

The organization shall define secure communication protocols to be used during active incidents to prevent further compromise and ensure reliable coordination.

Section 2. Threat Intelligence & Threat Hunting (TIH)

The Threat Intelligence & Threat Hunting (TIH) control family establishes organizational capabilities to proactively identify adversary tactics, techniques, and procedures (TTPs), derive actionable intelligence, and perform structured hunts for hidden or emerging threats. These controls focus on equipping defenders with the insight, access, and analytical rigor necessary to move from reactive security operations to proactive risk mitigation and adversary disruption.

2.1 TIH-01: Threat Intelligence Program Development

The organization shall establish and maintain a threat intelligence program that includes strategy, objectives, resourcing, and defined use cases for intelligence integration.

2.2 TIH-02: Intelligence Requirements Definition

The organization shall define Priority Intelligence Requirements (PIRs) that align with business risks, critical assets, and threat actor profiles to guide intelligence collection and analysis efforts.

2.3 TIH-03: Threat Intelligence Collection Sources

The organization shall acquire threat intelligence from diverse sources, including commercial, open-source, government, ISAC/ISAO partnerships, and internal telemetry.

2.4 TIH-04: Threat Intelligence Validation and Vetting

The organization shall implement processes for validating, scoring, and deconflicting threat intelligence to assess credibility, relevance, and accuracy prior to dissemination or use.

2.5 TIH-05: Threat Intelligence Enrichment

The organization shall enrich raw intelligence with internal context, behavioral analytics, and historical event data to improve actionability and reduce false positives.

2.6 TIH-06: Tactical, Operational, and Strategic Intelligence Segmentation

The organization shall distinguish between tactical, operational, and strategic intelligence products and ensure appropriate audiences receive intelligence at the relevant level of abstraction.

2.7 TIH-07: Threat Intelligence Sharing Agreements

The organization shall enter into formal agreements or memberships with trusted external partners, vendors, or industry coalitions for reciprocal sharing of threat intelligence.

2.8 TIH-08: Adversary Emulation Profiles

The organization shall maintain adversary emulation profiles based on known threat actor TTPs to support scenario-based assessments, simulations, and red team activities.

2.9 TIH-09: Threat Modeling Integration

The organization shall integrate threat intelligence into threat modeling exercises for new systems, applications, or business processes to anticipate and mitigate relevant threats.

2.10 TIH-10: Fusion of Internal and External Intelligence

The organization shall correlate external threat intelligence with internal telemetry, incident records, and environmental observations to derive organization-specific threat visibility.

2.11 TIH-11: Threat Hunting Program Framework

The organization shall define and implement a structured threat hunting program that includes dedicated personnel, tools, hypotheses-driven methods, and metrics for success.

2.12 TIH-12: Threat Hunting Hypothesis Development

The organization shall establish procedures for developing hunting hypotheses based on threat intelligence, anomalies, kill chain gaps, or newly observed TTPs.

2.13 TIH-13: Threat Hunting Toolset and Infrastructure

The organization shall provision and maintain infrastructure and toolsets capable of querying large-scale data sets, endpoint telemetry, and network traffic for hunting operations.

2.14 TIH-14: Hunt Log Management and Analysis

The organization shall retain and analyze logs from threat hunting activities to identify patterns, validate hypotheses, and feed lessons into detection engineering.

2.15 TIH-15: Hunt Frequency and Scheduling

The organization shall define a regular cadence for threat hunting activities, with flexible adjustments based on shifts in the threat landscape, emerging threats, or incident indicators.

2.16 TIH-16: Collaboration with Security Monitoring Teams

The organization shall establish bi-directional collaboration mechanisms between threat hunting teams and security monitoring personnel to operationalize hunt outcomes and improve detection content.

2.17 TIH-17: Indicators of Compromise (IOCs) Lifecycle Management

The organization shall implement lifecycle management processes for IOCs, including creation, validation, sharing, expiration, and revocation.

2.18 TIH-18: Threat Actor Profiling

The organization shall maintain updated profiles of known and emerging threat actors relevant to its industry, geography, or technology stack, including their capabilities, motivations, and historical activity.

2.19 TIH-19: Threat Intelligence Dissemination Protocols

The organization shall define protocols for the timely dissemination of actionable intelligence to relevant stakeholders, ensuring proper classification, handling, and secure delivery.

2.20 TIH-20: Threat Hunting Outcome Reporting

The organization shall document and report the outcomes of threat hunting activities, including findings, gaps, false positive trends, and recommendations for detection enhancement or risk mitigation.

2.21 TIH-21: Threat Intelligence Performance Metrics

The organization shall establish and monitor key performance indicators (KPIs) and effectiveness measures for its threat intelligence and threat hunting operations.

2.22 TIH-22: Intelligence-Led Decision Support

The organization shall integrate threat intelligence into executive risk briefings, technology acquisition processes, and policy development to enable informed decision-making.

2.23 TIH-23: Analyst Training and Tradecraft Development

The organization shall require threat intelligence analysts and hunters to receive ongoing training in tradecraft, analytic rigor, bias mitigation, and use of structured analytic techniques.

Section 3. Security Monitoring & SIEM (SMS)

The Security Monitoring & SIEM (SMS) control family defines the foundational capabilities, processes, and governance for real-time visibility into security events and logs across the enterprise. These controls emphasize the design, deployment, and optimization of centralized monitoring solutions that enable timely detection of anomalies, compliance enforcement, and risk-aware decision-making based on correlated, high-fidelity data.

3.1 SMS-01: Centralized Log Aggregation

The organization shall implement centralized aggregation of security-relevant log data from infrastructure, applications, endpoints, and cloud environments into a secure, scalable platform.

3.2 SMS-02: SIEM Architecture and Design Standards

The organization shall establish and maintain architectural standards for SIEM platforms to ensure performance, scalability, security, and data fidelity across all data sources.

3.3 SMS-03: Logging Coverage Criteria

The organization shall define criteria for minimum log source coverage, ensuring the inclusion of critical assets, authentication systems, security controls, and high-risk applications.

3.4 SMS-04: Log Normalization and Parsing

The organization shall implement processes to normalize, parse, and enrich log data from diverse sources to a common schema for effective analysis and correlation.

3.5 SMS-05: Time Synchronization Across Log Sources

The organization shall ensure that all log-producing systems are synchronized to a consistent time source (e.g., NTP) to maintain chronological accuracy in event correlation and investigation.

3.6 SMS-06: Retention and Archival of Security Logs

The organization shall define retention policies for security logs based on business, compliance, and forensic requirements, with appropriate archival and access controls in place.

3.7 SMS-07: Access Control for Log Data

The organization shall restrict access to log data and SIEM dashboards to authorized personnel based on role, ensuring read/write permissions align with the principle of least privilege.

3.8 SMS-08: Security Event Correlation Rules

The organization shall develop and maintain correlation rules to detect known patterns of malicious or suspicious behavior using event relationships across systems.

3.9 SMS-09: False Positive Reduction Processes

The organization shall regularly tune correlation rules, detection logic, and alert thresholds to reduce false positives and improve signal-to-noise ratios.

3.10 SMS-10: Real-Time Alerting and Notifications

The organization shall configure the SIEM to generate real-time alerts for events requiring immediate attention, routed to appropriate personnel or ticketing systems.

3.11 SMS-11: Dashboards and Visualizations

The organization shall design and maintain dashboards and visualizations in the SIEM that provide actionable insights aligned with stakeholder roles, including SOC analysts, engineers, and executives.

3.12 SMS-12: Data Ingestion Monitoring

The organization shall monitor the health and completeness of log ingestion pipelines to ensure no critical data sources are lost, misconfigured, or producing malformed entries.

3.13 SMS-13: Integration with Security Tools

The organization shall integrate the SIEM platform with threat intelligence feeds, EDR, IAM systems, and other security tools to enrich monitoring capabilities and support automated response.

3.14 SMS-14: Compliance Use Case Development

The organization shall define and implement monitoring use cases aligned with regulatory and contractual compliance obligations, including access monitoring, data exfiltration detection, and privileged user activity.

3.15 SMS-15: Custom Use Case Lifecycle Management

The organization shall maintain a documented lifecycle for custom detection use cases, including definition, development, testing, deployment, review, and retirement.

3.16 SMS-16: SIEM Tuning and Optimization Schedule

The organization shall conduct regular tuning and performance optimization of SIEM queries, rules, and infrastructure to minimize latency and maximize detection efficacy.

3.17 SMS-17: Monitoring of Administrative Activity

The organization shall implement focused monitoring of administrative actions across systems, including privilege elevation, configuration changes, and user provisioning.

3.18 SMS-18: Anomaly Baseline Establishment

The organization shall define behavioral baselines using historical log data to identify anomalous deviations from expected patterns across users, systems, and networks.

3.19 SMS-19: SIEM Data Integrity and Availability Protections

The organization shall implement safeguards to ensure the integrity, availability, and security of SIEM-stored data, including access logging, encryption, and backup procedures.

3.20 SMS-20: Monitoring for Use Case Gaps

The organization shall assess and identify gaps in monitoring coverage relative to emerging threats, technology changes, or new business processes and prioritize development of new detection use cases accordingly.

3.21 SMS-21: Audit Trail of Analyst Actions

The organization shall log and review analyst interactions within the SIEM environment, including search queries, rule changes, and alert dismissals, to support oversight and accountability.

3.22 SMS-22: Separation of Duties in SIEM Administration

The organization shall enforce separation of duties between those responsible for SIEM configuration, rule writing, and incident investigation to prevent abuse and maintain integrity of detections.

3.23 SMS-23: SIEM Use in Security Metrics Reporting

The organization shall leverage SIEM-generated data to support reporting of security metrics, executive dashboards, and board-level risk briefings, ensuring traceability to operational events.

Section 4. Section 4: Endpoint Detection & Response (EDR/XDR)

The Endpoint Detection & Response (XDR) control family governs the deployment, configuration, and operational use of endpoint-centric and extended detection and response technologies. These controls prioritize visibility into endpoint activity, telemetry consolidation across multiple security layers, and automated or analyst-driven response actions to isolate, mitigate, and recover from threats. XDR capabilities are leveraged to expand endpoint protection into a unified ecosystem encompassing identities, cloud, email, and other telemetry sources.

4.1 XDR-01: EDR/XDR Platform Deployment

The organization shall deploy an EDR or XDR platform on all supported endpoints and systems deemed within scope for detection and response, with installation validated through automated and manual inventory checks.

4.2 XDR-02: Agent Health and Coverage Monitoring

The organization shall continuously monitor EDR/XDR agent health, coverage status, and heartbeat frequency to identify missing, offline, or tampered agents across the environment.

4.3 XDR-03: Endpoint Telemetry Collection Standards

The organization shall configure EDR/XDR agents to collect granular telemetry, including process activity, network connections, file operations, user behaviors, and registry changes, with minimal performance degradation.

4.4 XDR-04: Behavioral Detection Capabilities

The organization shall utilize the EDR/XDR platform's behavioral detection features to identify deviations from known-good patterns or adversary tradecraft not reliant on static signatures.

4.5 XDR-05: Signature and Heuristic Detection Updates

The organization shall enable and verify automatic updates of detection engines, threat signatures, and heuristic models to ensure coverage of the latest adversary techniques.

4.6 XDR-06: Endpoint Isolation Capability

The organization shall enable remote endpoint isolation through the EDR/XDR platform to contain potentially compromised systems during triage or investigation.

4.7 XDR-07: Automated Response Playbooks

The organization shall define and implement automated playbooks within the XDR platform to respond to specific high-confidence threat detections with predefined mitigation actions.

4.8 XDR-08: File and Process Containment

The organization shall leverage EDR/XDR capabilities to suspend or terminate malicious processes, quarantine files, and prevent the spread of threats without full endpoint isolation where appropriate.

4.9 XDR-09: Endpoint Investigation Tools

The organization shall utilize built-in tools within the EDR/XDR platform to conduct live or retrospective investigations of endpoints, including process tree visualization, timeline analysis, and remote shell access.

4.10 XDR-10: Centralized XDR Management Console

The organization shall maintain a centralized management interface for the EDR/XDR platform with role-based access and integration with alerting, ticketing, and monitoring systems.

4.11 XDR-11: Cross-Platform Telemetry Correlation

The organization shall configure the XDR platform to ingest and correlate telemetry from non-endpoint sources such as identity providers, cloud platforms, email systems, and firewalls to enrich detections.

4.12 XDR-12: Endpoint Threat Scoring and Prioritization

The organization shall implement threat scoring models within the XDR platform to prioritize detected threats based on confidence, impact, spread potential, and asset criticality.

4.13 XDR-13: Controlled Use of Remote Remediation Tools

The organization shall define procedures for secure use of remote remediation tools provided by the EDR/XDR platform, including file removal, script execution, and registry modification.

4.14 XDR-14: Threat Containment Policy Enforcement

The organization shall apply containment policies at the endpoint level via the XDR platform to restrict access to resources, networks, or applications based on risk levels or incident association.

4.15 XDR-15: Endpoint Forensic Snapshot Collection

The organization shall configure the XDR platform to capture forensic snapshots or memory dumps from affected endpoints during incident investigations upon analyst initiation or predefined triggers.

4.16 XDR-16: Endpoint Risk Posture Reporting

The organization shall leverage XDR-native dashboards and reports to assess risk posture across endpoint fleets, including vulnerable software, insecure configurations, and active threats.

4.17 XDR-17: Tamper Protection Enforcement

The organization shall enforce anti-tampering mechanisms on EDR/XDR agents to prevent unauthorized deactivation, modification, or evasion by local users or malware.

4.18 XDR-18: Host-Based Exploit Mitigation Integration

The organization shall integrate exploit mitigation technologies (e.g., memory protection, code injection prevention, application control) within the EDR/XDR platform where supported.

4.19 XDR-19: Alert Fidelity Assurance Processes

The organization shall implement alert validation workflows to ensure high-fidelity alerts are produced by the XDR platform, minimizing alert fatigue and ensuring meaningful triage.

4.20 XDR-20: Custom Detection Logic Development

The organization shall develop and maintain custom detection rules within the EDR/XDR platform to detect threats specific to its environment, applications, or configurations.

4.21 XDR-21: Response Action Audit Logging

The organization shall log and audit all response actions taken via the XDR platform, including automation-initiated and analyst-initiated actions, for accountability and forensic review.

4.22 XDR-22: Executive and Operational Reporting

The organization shall generate periodic reports from the XDR platform tailored to executives and security leadership, summarizing threat trends, incident response actions, and endpoint security posture.

Section 5. Red Team / Blue Team / Purple Team Exercises (RBP)

The Red Team / Blue Team / Purple Team Exercises (RBP) control family governs the structure, planning, execution, and evaluation of adversarial simulation and defense exercises across the organization. These controls are designed to ensure that offensive testing (Red), defensive monitoring and response (Blue), and collaborative improvement (Purple) are conducted systematically and yield measurable enhancements to detection, response, and security control efficacy without duplicating standard detection or incident response operations.

5.1 RBP-01: Adversarial Simulation Program Governance

The organization shall establish governance for offensive and defensive simulation activities, including roles, responsibilities, authorization processes, and data classification constraints.

5.2 RBP-02: Red Team Charter and Rules of Engagement (RoE)

The organization shall maintain a formal charter and detailed Rules of Engagement (RoE) for Red Team operations that define scope, permissible techniques, timing, notification protocols, and safety mechanisms.

5.3 RBP-03: Blue Team Readiness Assessment

The organization shall assess Blue Team readiness prior to exercises, ensuring adequate staffing, monitoring capabilities, escalation procedures, and isolation tools are in place to support real-time defensive operations.

5.4 RBP-04: Purple Team Integration Model

The organization shall define an integration model for Purple Team exercises that facilitates iterative collaboration between offensive and defensive teams, with defined communication and feedback loops.

5.5 RBP-05: Threat-Informed Exercise Design

The organization shall design exercises based on current threat intelligence, industry-relevant adversaries, and known TTPs to ensure realism and value to organizational defense posture.

5.6 RBP-06: Exercise Type Differentiation

The organization shall differentiate between red team, blue team, purple team, and hybrid exercises, maintaining clarity in scope, expected outcomes, and execution protocols for each.

5.7 RBP-07: Emulation Plan Development

The organization shall develop detailed emulation plans for each Red Team engagement that outline step-by-step attack chains, objective targets, and indicators of activity.

5.8 RBP-08: Defensive Control Testing

The organization shall test the effectiveness of deployed security controls during Red Team and Purple Team exercises, capturing bypassed or missed detections for remediation.

5.9 RBP-09: Real-Time Blue Team Performance Metrics

The organization shall track Blue Team metrics during exercises, such as detection time, triage time, containment speed, and escalation accuracy to evaluate defensive performance.

5.10 RBP-10: Exercise Safety and Risk Containment

The organization shall implement safeguards during live exercises to prevent unintended service disruption, data corruption, or user impact, including “kill switch” protocols.

5.11 RBP-11: Command and Control (C2) Channel Simulation

The organization shall simulate adversarial C2 channels during Red Team operations using realistic, covert, and evasive techniques that align with known attacker profiles.

5.12 RBP-12: Stealth and Evasion Techniques Testing

The organization shall include stealth and evasion techniques in Red Team scenarios to evaluate the organization’s ability to detect and respond to sophisticated intrusions.

5.13 RBP-13: Internal Collaboration Facilitation (Purple Teaming)

The organization shall coordinate Purple Team activities by co-locating or virtually integrating red and blue teams for shared analysis, detection engineering, and defensive tuning.

5.14 RBP-14: Security Control Gap Identification

The organization shall document any gaps in security visibility, alerting, response coordination, or control effectiveness discovered during team-based exercises.

5.15 RBP-15: Replay and Detection Engineering Sessions

The organization shall conduct replay sessions post-exercise to walk through Red Team activity logs with Blue Team personnel to engineer or improve detections.

5.16 RBP-16: Simulated Breach and Attack Scenarios

The organization shall conduct periodic simulated breach exercises (e.g., assumed breach or lateral movement scenarios) to test internal detection and response without external perimeter compromise.

5.17 RBP-17: Exercise Debrief and Hotwash Sessions

The organization shall perform structured debriefings after every team-based exercise to capture lessons learned, discuss cross-team perspectives, and define improvement actions.

5.18 RBP-18: Maturity Model for Team-Based Exercises

The organization shall adopt a maturity model to guide the progression of team-based security exercises, ranging from basic attack path validation to full adversary lifecycle emulation.

5.19 RBP-19: Exercise Scheduling and Frequency

The organization shall maintain a schedule for recurring Red, Blue, and Purple Team activities across business units and technical domains, incorporating rotation and scenario variation.

5.20 RBP-20: Data and Log Capture for Exercise Analysis

The organization shall ensure comprehensive logging of Red Team activity, Blue Team responses, and platform outputs during exercises to support retrospective analysis and tool tuning.

5.21 RBP-21: External Red Team Engagement Management

The organization shall establish vetting, onboarding, oversight, and post-engagement evaluation protocols for external Red Teams engaged in testing organizational defenses.

5.22 RBP-22: Training Exercises for SOC and IR Staff

The organization shall incorporate modified Red Team scenarios into training exercises for security operations center (SOC) analysts and incident responders to develop intuition and decision-making skills.

5.23 RBP-23: Reporting of Adversarial Simulation Outcomes

The organization shall document and report the results of adversarial exercises, including objectives met, undetected activities, defensive wins, and action plans for detection and response improvement.

Section 6. Malware Protection & Digital Forensics (MDF)

The Malware Protection & Digital Forensics (MDF) control family establishes the safeguards, investigative capabilities, and analytical processes necessary to prevent, detect, analyze, and recover from malicious software and related artifacts. These controls are distinct from incident response or endpoint detection—they focus specifically on the lifecycle of malware-based threats and the forensic mechanisms required to understand, attribute, and mitigate malicious code execution and its impacts on enterprise assets.

6.1 MDF-01: Malware Prevention Policy

The organization shall maintain a policy governing acceptable use, malware prevention practices, scanning frequency, and software restrictions across all information systems.

6.2 MDF-02: Multi-Layered Malware Defense Strategy

The organization shall implement a defense-in-depth approach to malware protection, utilizing multiple layers of controls such as anti-malware engines, sandboxing, threat emulation, and heuristic scanning.

6.3 MDF-03: Malware Signature Management

The organization shall ensure all malware protection solutions receive timely updates to detection signatures, heuristic definitions, and cloud-assisted intelligence feeds.

6.4 MDF-04: Advanced Malware Analysis Capability

The organization shall maintain capabilities to perform advanced analysis of suspected malware, including static analysis, dynamic behavior tracing, and unpacking of obfuscated code.

6.5 MDF-05: Sandboxing and Detonation Environments

The organization shall deploy isolated sandbox environments to safely detonate suspicious files and URLs for behavioral analysis, attribution, and validation of detection efficacy.

6.6 MDF-06: Malware Event Logging and Correlation

The organization shall collect and retain logs related to malware events, including file hashes, process paths, associated network traffic, and user interactions, with correlation to endpoint and network telemetry.

6.7 MDF-07: Executable File Reputation Validation

The organization shall evaluate unknown executables and scripts against internal and external reputation services prior to execution or installation on enterprise systems.

6.8 MDF-08: Removable Media Malware Controls

The organization shall implement specific controls for detecting, scanning, and restricting malware propagation via USB drives, optical media, and other removable storage devices.

6.9 MDF-09: Email and Web Gateway Malware Filtering

The organization shall configure email and web gateways to detect and block malware-laden attachments, links, and payloads using signature, sandboxing, and machine learning technologies.

6.10 MDF-10: Malware Infection Chain Mapping

The organization shall document and update infection chain models (e.g., MITRE ATT&CK) for known or emerging malware families relevant to the organization's risk profile.

6.11 MDF-11: Malicious Persistence Mechanism Detection

The organization shall monitor for signs of malware persistence techniques, including registry manipulation, scheduled tasks, service installation, and DLL hijacking.

6.12 MDF-12: Malware-Driven Data Exfiltration Detection

The organization shall identify and alert on behaviors indicative of data exfiltration resulting from malware infections, such as staged data, encrypted outbound traffic, or beaconing.

6.13 MDF-13: Host-Based Malware Remediation

The organization shall define standard procedures for host-based remediation of confirmed malware infections, including quarantine, artifact removal, and system re-imaging when required.

6.14 MDF-14: Malware Attribution and Classification

The organization shall classify malware into families, variants, and threat actor affiliations where possible to inform threat models, incident prioritization, and long-term defense tuning.

6.15 MDF-15: Memory Forensics Capability

The organization shall maintain the ability to acquire and analyze volatile memory from compromised or suspicious hosts to uncover in-memory malware, rootkits, and execution traces.

6.16 MDF-16: Disk and File System Forensic Acquisition

The organization shall implement procedures for secure acquisition of full disk images or targeted file system snapshots to support forensic investigations and legal hold requirements.

6.17 MDF-17: Chain of Custody for Digital Evidence

The organization shall enforce chain of custody protocols for all collected forensic evidence to ensure integrity, admissibility, and traceability throughout the investigative lifecycle.

6.18 MDF-18: Forensic Timeline Reconstruction

The organization shall use timestamped data from various logs, registries, and file systems to reconstruct a timeline of malware activity and affected system behaviors.

6.19 MDF-19: Reverse Engineering of Malicious Code

The organization shall maintain access to reverse engineering expertise or tooling for dissecting malicious binaries, scripts, and macros to understand function, intent, and system impact.

6.20 MDF-20: Forensics Lab Environment Segregation

The organization shall operate forensic analysis environments separate from production systems with tightly controlled access, data handling protocols, and malware detonation safeguards.

6.21 MDF-21: Coordination with Legal and HR for Malware Cases

The organization shall define procedures for involving legal counsel and human resources when forensic analysis reveals internal policy violations, intellectual property theft, or insider threat indicators.

6.22 MDF-22: Post-Malware Infection Assessments

The organization shall conduct structured assessments following malware infections to identify entry vectors, security control bypasses, residual risk, and required control enhancements.