AI-Driven Threat Detection and Autonomous SOC Controls Catalog

Version 1.0 | Reference Document for NIST CSF 2.0 OLIR Mapping

Document Type	Control Catalog / Reference Document
Reference Document Name	AI-Driven Threat Detection and Autonomous SOC Controls Catalog v1.0
Prepared by	Anar Israfilov, Founder, Cyberoon Enterprise Corporation
Intended Use	Reference document for OLIR-style mapping to NIST Cybersecurity Framework 2.0
Status	Draft for technical review
Date	2026-05-11

1. Purpose

This catalog defines a structured set of AI-driven Security Operations Center (AI SOC) controls for threat detection, endpoint telemetry analytics, ransomware behavior detection, alert triage, incident prioritization, and AI-assisted response workflows. It is intended to serve as the reference document for an OLIR-style mapping to NIST Cybersecurity Framework (CSF) 2.0.

2. Scope

The catalog focuses on operational cybersecurity capabilities that may be used by enterprise SOC teams, managed security service providers, healthcare security teams, detection engineers, and cybersecurity governance teams. The catalog does not claim to be a compliance standard, certification, or official NIST publication.

3. How to Use This Catalog

- Use the Control ID as the Reference Document Element in the OLIR mapping workbook.
- Use the Control Name and Description to explain the operational meaning of each AI SOC capability.
- Map each AI SOC control to relevant NIST CSF 2.0 subcategories using OLIR relationship values such as equal, subset of, superset of, and intersects with.
- Use evidence sources such as endpoint telemetry, SIEM events, analyst review records, incident tickets, playbooks, and dashboards to support implementation in real environments.

4. Control Catalog

Control ID	Control Name	Domain	Control Description	Evidence / Telemetry Examples	Primary CSF Alignment
AI-SOC-01	Behavioral Anomaly Detection	Detection	AI-driven identification of abnormal behavioral patterns across endpoints, users, services, and systems.	Endpoint events, authentication behavior, process activity, network indicators, baseline deviations.	Detect
AI-SOC-02	Endpoint Telemetry Analytics	Monitoring	Continuous analysis of endpoint, workload, and operational telemetry for security-relevant events.	EDR/agent events, system logs, process trees, file activity, network connections.	Detect
AI-SOC-03	Ransomware Behavior Detection	Detection	Detection of behavioral indicators associated with ransomware activity, encryption bursts, privilege abuse, and destructive actions.	File modification spikes, encryption behavior, shadow copy deletion, suspicious privilege use.	Detect / Respond
AI-SOC-04	Autonomous Alert Triage	Response	AI-assisted triage that correlates signals, reduces noise, and routes alerts based on severity and context.	Alert metadata, severity history, event clusters, analyst feedback, asset criticality.	Respond
AI-SOC-05	Threat Intelligence Enrichment	Risk Analysis	Integration of external and internal threat intelligence into detection, analysis, and prioritization workflows.	IOC feeds, TTP mapping, campaign metadata, internal incident history.	Identify / Detect

AI-SOC-06	AI-Assisted Incident Prioritization	Response	Risk-based prioritization of incidents using AI analytics, business context, asset criticality, and threat severity.	Asset criticality, user role, exploitability, threat confidence, business impact.	Respond / Recover
AI-SOC-07	Automated Containment Recommendation	Response	AI-assisted recommendation of containment actions for suspicious or confirmed malicious activity.	Incident type, affected asset, blast radius, playbook options, containment status.	Respond
AI-SOC-08	Detection Engineering Optimization	Improvement	Continuous improvement of detection logic, tuning, thresholding, and rule performance based on operational feedback.	False positive/negative trends, rule hits, detection drift, analyst feedback.	Govern / Identify / Protect
AI-SOC-09	Insider Threat Behavioral Analysis	Detection	Behavioral analytics designed to identify potential insider threat indicators and abnormal user activity.	Authentication anomalies, data access patterns, unusual privilege use, policy deviations.	Protect / Detect
AI-SOC-10	Healthcare Endpoint Risk Monitoring	Sector-Specific Monitoring	AI-assisted monitoring of healthcare endpoints, sensitive systems, and clinical operational environments.	Clinical workstation activity, endpoint health, sensitive-system alerts, availability indicators.	Identify / Detect
AI-SOC-11	Security Alert Correlation	Detection	Correlation of related security events and alerts across endpoints, identity, network, cloud, and SIEM sources.	SIEM alerts, EDR detections, identity alerts, network logs, cloud events.	Detect
AI-SOC-12	Autonomous SOC Workflow Orchestration	Response	AI-assisted orchestration of SOC workflows, escalation paths, playbooks, and operational response activities.	Playbooks, escalation rules, analyst queues, incident workflow state.	Govern / Respond
AI-SOC-13	Threat Behavior Modeling	Risk Analysis	Modeling of adversary behaviors, attack patterns, tactics, techniques, and likely progression paths.	TTPs, attack chain sequences, historical campaigns, observed telemetry.	Identify / Respond
AI-SOC-14	Endpoint Behavioral Fingerprinting	Detection	Creation of behavioral baselines and fingerprints for endpoints, users, and workloads.	Endpoint baseline, process patterns, user behavior, workload signatures.	Detect
AI-SOC-15	AI-Assisted Threat Hunting	Detection	AI-assisted proactive identification of suspicious activity, weak signals, and emerging attack patterns.	Hypotheses, weak signals, query results, detection leads, threat intel context.	Detect / Identify
AI-SOC-16	AI SOC Governance Oversight	Governance	Governance oversight for AI-assisted SOC capabilities, including roles, accountability, review, and operational controls.	Control ownership, review logs, model use policy, accountability records.	Govern
AI-SOC-17	AI Risk Scoring Dashboard	Governance	AI-assisted cybersecurity risk scoring and operational reporting for security leaders and SOC teams.	Risk scores, KRIs, incident trends, coverage metrics, severity distributions.	Govern / Identify
AI-SOC-18	Asset Telemetry Inventory	Asset Visibility	Telemetry-based support for identifying, validating, and monitoring assets within the security environment.	Endpoint identifiers, agent status, hostname data, network observations, cloud assets.	Identify
AI-SOC-19	Identity Behavior Analytics	Access Monitoring	AI-assisted monitoring of user, service, and identity behavior for suspicious authentication or access patterns.	Login behavior, privilege changes, failed authentication, unusual access paths.	Protect / Detect
AI-SOC-20	Privileged Access Anomaly Monitoring	Access Monitoring	Detection of abnormal privileged access, privilege escalation, and high-risk administrative behavior.	Admin activity, privilege changes, lateral movement indicators, sensitive access events.	Protect / Detect
AI-SOC-21	Vulnerability Exposure Prioritization	Risk Analysis	AI-assisted prioritization of vulnerabilities based on exposure, exploitability, asset criticality, and threat context.	Vulnerability scans, exploit intelligence, asset criticality, attack surface data.	Identify / Protect
AI-SOC-22	Security Data Normalization	Data Engineering	Normalization of security data sources to improve correlation, detection accuracy, and monitoring consistency.	Log schemas, parsers, normalized event fields, enrichment metadata.	Protect / Detect
AI-SOC-23	Forensic Evidence Prioritization	Incident Analysis	AI-assisted prioritization of forensic artifacts, timelines, logs, and evidence relevant to incident analysis.	Forensic timelines, memory/process artifacts, endpoint logs, alert clusters.	Respond
AI-SOC-24	Response Playbook Recommendation	Response	AI-assisted recommendation of incident response playbooks and mitigation steps based on alert context.	Incident class, playbook library, asset impact, containment options.	Respond

AI-SOC-25	Recovery Priority Analytics	Recovery	AI-assisted prioritization of recovery actions based on business impact, system criticality, and threat containment state.	Business impact, system dependency, recovery status, containment confirmation.	Recover
AI-SOC-26	Third-Party AI Security Monitoring	Supply Chain	Monitoring of third-party AI, SaaS, and managed security dependencies that affect SOC operations.	Vendor telemetry, integration logs, SaaS activity, third-party risk indicators.	Govern / Identify
AI-SOC-27	Detection Drift Monitoring	Improvement	Monitoring for degradation, drift, false positives, false negatives, and changing detection performance over time.	Detection performance metrics, analyst feedback, model drift indicators, alert quality trends.	Govern / Detect
AI-SOC-28	Security Data Privacy Controls	Privacy / Protection	Controls to reduce exposure of sensitive security, identity, patient, or operational data during AI-assisted analysis.	Data minimization rules, masking, access records, sensitive data classification.	Protect
AI-SOC-29	Human-in-the-Loop Escalation	Governance / Response	Escalation of high-risk AI-assisted conclusions to qualified human analysts or security leaders for review.	Analyst review decisions, escalation records, approval workflows, confidence scores.	Govern / Respond
AI-SOC-30	Cybersecurity Reporting Automation	Governance	Automated generation of security reporting, metrics, evidence, and operational summaries for governance and review.	Metrics, dashboards, incident summaries, evidence packages, executive reports.	Govern / Recover

5. Relationship to NIST CSF 2.0 OLIR Mapping

In the companion OLIR mapping workbook, NIST CSF 2.0 is treated as the Focal Document and this AI SOC Controls Catalog is treated as the Reference Document. Each row explains how a NIST CSF 2.0 subcategory relates to one AI SOC control. The mapping is a technical alignment aid and should not be treated as proof of compliance by itself.

6. Disclaimer

This catalog is an independent technical reference prepared for cybersecurity mapping and discussion purposes. It is not an official NIST publication, does not represent NIST guidance, and does not certify compliance with NIST CSF 2.0 or any other cybersecurity standard.

7. References

1. National Institute of Standards and Technology (NIST), The NIST Cybersecurity Framework (CSF) 2.0, February 26, 2024. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf
2. National Institute of Standards and Technology (NIST), NISTIR 8278A Revision 1, National Online Informative References (OLIR) Program: Submission Guidance for OLIR Developers, 2024. https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8278Ar1.pdf
3. NIST CSF 2.0 Reference Tool. https://csrc.nist.gov/projects/cybersecurity-framework/filters

8. Version History

Version	Date	Status	Notes
1.0	2026-05-11	Draft	Initial AI SOC Controls Catalog for OLIR-style mapping to NIST CSF 2.0.