Merit SOC - RFC 2350

1. Document Information

1.1 Date of Last Update

Version 1.1, November 2, 2026

1.2 Distribution List for Notifications

There is no dedicated distribution list for changes to this document at this time. Material changes will be communicated through Merit SOC member communication channels.

1.3 Locations Where This Document May Be Found

The current version of this document is available at https://www.merit.edu/soc

2. Contact Information

2.1 Name of the Team

Merit Network, Inc. Security Operations Center (Merit SOC)

2.2 Address

Merit Network, Inc.
880 Technology Drive, Suite B
Ann Arbor, MI 48108-8963
United States

2.3 Time Zone

Eastern Time (America/Detroit), UTC-5 (UTC-4 during daylight saving time)

2.4 Telephone Number

+1 734-527-5700

2.5 Facsimile Number

+1 734-527-4125

2.6 Other Telecommunication

None at this time.

2.7 Electronic Mail Address

misoc@merit.edu

2.8 Public Keys and Encryption Information

Merit SOC PGP is used for secure exchanges with Merit SOC

- User ID: Merit SOC misoc@merit.edu
- Key ID: EA30F1A074373DF0
- Fingerprint: 515E 648D 4F99 C5A2 755D 30CE EA30 F1A0 7437 3DF0

The public PGP key is available at the following location: https://keys.openpgp.org (Lookup by Email or Fingerprint)

2.9 Team Members

Individual Merit SOC personnel are not publicly identified. Participating organizations may obtain appropriate SOC contacts through their established Merit SOC relationship.

2.10 Other Information

General information about the Merit SOC is available at https://www.merit.edu/soc .

2.11 Points of Customer Contact

The preferred method for contacting Merit SOC is by email at misoc@merit.edu. For urgent matters, Merit SOC may be reached by telephone at 734-527-5700. Merit SOC provides 24x7 monitoring and support.

3. Charter

3.1 Mission Statement

The Merit SOC provides cybersecurity monitoring, detection, alerting, analysis, threat intelligence, threat hunting, and cybersecurity community support to help improve the security posture of participating Merit members, supporting the identification, analysis, communication, and coordination of security events and incidents affecting its constituency.

3.2 Constituency

The Merit SOC primarily serves Merit members and participating organizations that receive Merit SOC services. Specific eligibility, supported systems, service scope, and service levels are established through the applicable Merit SOC service agreement or service arrangement.

3.3 Sponsorship and/or Affiliation

The Merit SOC operates as part of Merit Network, Inc., a 501(c)3 Michigan nonprofit organization established in 1966 that provides networking, technology, and cybersecurity services to its members and participating organizations.

3.4 Authority

The Merit SOC operates within the authority established by Merit governance, applicable policies, and service agreements. Within its approved scope, the SOC monitors supported security data sources, analyzes and investigates security events, conducts threat intelligence and threat hunting activities, generates and communicates alerts, notifies and coordinates with participating organizations, escalates significant security activity, and provides analysis and recommendations to support incident response. The SOC does not have independent authority to perform containment, blocking, account changes, firewall changes, or remediation within a participating organization's environment. The participating organization retains responsibility for incident response, containment, remediation, and recovery unless additional authority or services have been explicitly established.

4. Policies

4.1 Types of Incidents and Level of Support

The Merit SOC monitors, analyzes, and provides support for security events and incidents affecting participating organizations, including malware and malicious activity, phishing and credential theft, suspicious network activity, compromised accounts or endpoints, indicators of compromise, command and control activity, malicious infrastructure, and vulnerability related security activity. Support may include detection, alert generation, triage, investigation, threat intelligence enrichment, threat hunting, notification, escalation, coordination, and technical recommendations. The SOC provides information and analytical support during incidents; incident containment, remediation, and recovery remain the responsibility of the participating organization unless explicitly included in a separate service arrangement. Merit SOC does not guarantee detection of every cybersecurity threat, vulnerability, or incident.

4.2 Co-operation, Interaction and Disclosure of Information

The Merit SOC cooperates with participating organizations, trusted cybersecurity organizations, and other appropriate incident response teams as necessary to support its constituency. Information may be shared when necessary to provide SOC services, coordinate security incidents, or address legal or regulatory requirements. Member identifying, confidential, or sensitive information is not disclosed outside the authorized scope without appropriate authorization, except where required or permitted by applicable law, policy, or agreement.

4.3 Communication and Authentication

The Merit SOC uses approved communication channels, including email and telephone, to interact with participating organizations. Requests involving sensitive information or potentially unauthorized activity may require additional verification of the requester's identity or authority. Sensitive information is communicated using methods appropriate to its sensitivity.

5. Services

5.1 Incident Response

5.1.1 Incident Triage

Merit SOC reviews reported or detected security activity, assesses available indicators and supporting information, and prioritizes activity for further analysis.

5.1.2 Incident Coordination

Merit SOC notifies participating organizations of relevant activity, escalates significant findings, and provides relevant alerts, logs, indicators, analysis, and threat intelligence in support of member led incident response.

5.1.3 Incident Resolution

Merit SOC provides information, analysis, recommendations, and coordination to support resolution of security incidents. The participating organization retains responsibility for containment, remediation, and recovery unless additional authority or services have been explicitly established.

5.2 Proactive Activities

Merit SOC conducts continuous security monitoring and detection across supported data sources, provides automated and analyst supported security alerting, produces threat intelligence and indicator of compromise analysis, performs proactive threat hunting, and analyzes phishing and email security related activity, including identification of phishing infrastructure and support for takedown activities where applicable. Where included in a member's service arrangement, Merit SOC also provides endpoint detection and response (EDR) capabilities, including licensed EDR tooling, ingestion of a member's existing EDR data, or a combination of both. Merit SOC additionally supports cybersecurity collaboration among participating organizations through community discussion forums, communities of practice, and periodic collaboration sessions, subject to the applicable service arrangement.

6. Incident Reporting Forms

There are currently no formal incident reporting forms. Incidents may be reported using the contact information provided in Section 2. Reports should include, when available, organization and contact information, a description of the suspected activity, affected systems or accounts, relevant dates and times, and any available indicators or supporting logs.

7. Disclaimers

While every precaution is taken in the preparation of information, notifications, and alerts, Merit Network, Inc. and the Merit SOC assume no responsibility for errors, omissions, or for damages resulting from the use of the information contained herein. Merit SOC services are provided on a commercially reasonable, best effort basis, and do not replace the participating organization's responsibility for maintaining appropriate cybersecurity controls or responding to security incidents.