CyberFuse SOC Analyzer agent

About CyberFuse

CyberFuse is a mobile-first, GenAI-powered cybersecurity platform designed to enhance and extend SOC capabilities through AI-driven correlation, visualization, and response. Built with a proprietary Sec-LM (Security Language Model), CyberFuse integrates seamlessly into Microsoft-based environments and augments existing tools like Microsoft Security Copilot, Sentinel, and Defender XDR.

Key Capabilities:

- Contextual Correlation Across Sources

  CyberFuse connects to diverse data streams—Microsoft Sentinel, Defender XDR, MISP, Wazuh, and open-source feeds—enabling unified threat context and enhanced decision support.

- AI-Powered Visual Intelligence

  CyberFuse dynamically generates executive-level visuals such as ISO heatmaps, incident impact charts, and remediation investment prioritization—aligning technical events with business context.

- Security Workflow Awareness

  The platform understands and interacts with security workflows (e.g., Microsoft Logic Apps, Defender playbooks, and other SOAR tools), helping teams visualize and accelerate response processes.

- Copilot-Aligned Agent Capabilities

  As a certified Microsoft ISV Partner, CyberFuse natively supports Microsoft Security Copilot agents, providing high-context telemetry, threat scores, and structured insights for faster incident triage and executive reporting.

- Flexible Deployment

  Offered as both a secure PaaS and on-premises solution, CyberFuse is ideal for highly regulated sectors such as banking, government, and healthcare.

CyberFuse is backed by partnerships with Microsoft and NVIDIA with a mission to make SOCs smarter, faster, and more autonomous through responsible GenAI adoption.

Purpose of the Agent (Customer benefit)

CyberFuse SOC Analyzer agent is designed to empower SOC teams by automating triage and analysis of security incidents ingested from the CyberFuse platform. It fetches incidents in near real time, evaluates their malicious intent, assigns a threat score, and provides actionable recommendations for containment and remediation. This reduces analyst workload, improves triage accuracy, and accelerates incident response cycles.

Customers will find value in:
- Enhanced SOC Efficiency: Automates repetitive triage tasks, saving analysts time and allowing them to focus on high-priority threats.
- Consistent Threat Scoring: Uses advanced AI models to standardize scoring and classification across all incidents.
- Actionable Guidance: Provides remediation recommendations directly within Microsoft Security Copilot, accelerating resolution time.
- Comprehensive Visibility: Correlates CyberFuse telemetry with other Microsoft tools for a unified security view.

Products used:
- Microsoft Security Copilot
- CyberFuse (Incident ingestion and analytics)
- Microsoft Sentinel (optional telemetry correlation)
- Microsoft Defender XDR (optional incident context enrichment)

Functional Design

CyberFuse SOC Analyzer Agent will:
1. Fetch incidents from CyberFuse API every 10 minutes or on demand.
2. Enrich context with metadata like source IP, tactics, techniques (MITRE ATT&CK), and behavioral indicators.
3. Classify incidents using the ClassifyIncidentsviaAI skill to determine if they are True Positive, False Positive, or require escalation.
4. Threat Score Assignment: Assign a score (0–100) based on severity, confidence, and attack surface impact.

5. Generate Actionable Insights: Recommend remediation and containment actions, mapped to SOC playbooks.
6. Report Generation: Produce detailed incident summaries with classification, score, and next steps.
7. SOC Analyst Workflow Integration: Surface results in Security Copilot as natural-language summaries or structured reports.

Triggers for Agent Activation

- Automatic Trigger: Runs every 10 minutes (configurable) to pull new incidents from CyberFuse.
- Manual Trigger: Security Copilot users can run the agent on-demand by providing a specific IncidentID.
- Contextual Trigger: Can be invoked when new high-severity incidents appear in Sentinel or Defender XDR to cross-reference CyberFuse data.

Plugins or Data Signals

Plugins Required:
1. CyberFuse Incidents API – Main incident ingestion and telemetry data source.
2. Microsoft Sentinel Plugin – Optional, for correlating incidents across SIEM data.
3. Microsoft Defender XDR Plugin – Optional, for enrichment with endpoint and identity telemetry.
4. Threat Intelligence Feeds (via MISP or MS Threat Intelligence) – For threat scoring and classification enrichment.

Data Signals Used:
- CyberFuse incident telemetry (alerts, behaviors, IOC data)
- MITRE ATT&CK mapping
- Endpoint, network, and identity logs from Microsoft 365 Defender
- External threat feeds for additional scoring context

Customer Onboarding/Deployment

1. Pre-requisites:

- Access to Microsoft Security Copilot with agent hosting enabled.
- API access to CyberFuse instance with incident telemetry enabled.
- Cyberfuse Platform

- Optional integration with Microsoft Sentinel and Defender for full context.

2. Setup Steps:
Import the CyberFuse SOC Analyzer Agent from the Security Copilot Agent gallery.
Configure API keys/URLs for CyberFuse in the agent settings.
(Optional) Connect Microsoft Sentinel and Defender plugins for additional enrichment.
- Validate connection by running a test incident triage query.

3. User Documentation:
- A step-by-step guide with setup screenshots.
- Incident triage workflows with examples of classification and recommended responses.
- Troubleshooting guide with logs and error resolution steps.

1. Contacts and Engineering Milestones

Role	Contact Details
Alliances/Business Development	Mgibreel@Cyberfuse.net
Product Manager	Sama@Cyberfuse.net
Engineering	Msalem@Cyberfuse.net