iCorps TECHNOLOGIES

# iCorps SOC-as-a-Service

## Next-Generation Threat Detection and Monitoring

### 24x7 Network Monitoring

Security Operations Center-as-a-Service (SOC-as-a-Service) is a 24x7 detection and monitoring service that combines cutting-edge Security Information and Event Management (SIEM) technology and established threat intelligence.

As your devices generate logs and events, they are collected and transmitted to the cloud in near time (within 15 minutes of data collection). Thousands of automated security correlation rules rapidly identify suspicious irregularities. In the event of an irregularity, iCorps Advanced Security Engineers receive actionable alerts to assess for false positives, investigate security incidents, and respond to targeted attacks. Our SOC monitors for potential threats, including user indentity vs. account lockouts, privilege elevation, data leaks and breaches, and suspicious network activity.

iCorps SOC-as-a-Service combines SIEM technology, threat intelligence, suspicious activity, and network security incidents to keep your network secure. It can be offered as a standalone offering or an enhancement to existing security solutions. Additional services, such as vulnerability management, are available. Not only can SOC-as-a-Service enhance your overall security posture, but it can:

- Reduce the Risk of a Data Breach
- Minimize Downtime and Loss from Security Incidents
- Assist with Business Continuity via On-Premise or Remote Remediation
- Aid in Compliance by Providing Real-Time Log, Performance, and Configuration Data from Network Devices, 24x7

**24x7 Network Monitoring and Alerting**

**Diverse Risk Remediation Alerts You to Potential Network Threats**

**Monitor Users, Workstations, Edge Devices, and Cloud Apps**

iCorps TECHNOLOGIES

# iCorps SOC-as-a-Service

## Next-Generation Threat Detection and Monitoring

### Network Security Monitoring

Detect potential threat activity like command and control connections, denial of service attacks, data exfiltration and reconnaissance.

- SIEM Analysis
- AI Analytics Engine
- Self-Service Reporting
- Multi-Tenancy Dashboard
- Network Intrusion Detection
- Physical or Virtual Appliance
- Supports Industry Compliance Standards

### Log Security Monitoring

Identify threat-like behavior in your systems such as impossible logins, multi-factor bypass, coordinated attacks, and rogue agents.

- SIEM Analysis
- AI Analytics Engine
- Self-Service Reporting
- Multi-Tenancy Dashboard
- Hundreds of Support Integrations
- Supports Industry Compliance Standards
- Deployment of Physical or Virtual Appliance for On-Premise Logs
- ROI on Existing Investments - Merge Data from Existing Security Tools for Increased Visibility

### Office 365 Security Monitoring

Monitor suspicious behavior like unauthorized access to cloud mailboxes, admin changes, impossible logins, and brute force attacks.

- Multi-Tenancy Dashboard
- SIEM Correlation + SOC Analysis
- Support for Custom Alerting and Reports
- Supports Industry Compliance Standards
- Visibility to Login Activity in the Dashboard
- Detects Potential Threats of Suspicious Activity in Office 365