

Managed SOC

Round-the-clock monitoring, detection and response with SIEM, SOAR and EDR

Attackers do not keep office hours. Many intrusions begin at night, at weekends or during holidays, and the longer they go unnoticed the more they cost. Building an in-house security operations centre means hiring analysts for every shift, buying and integrating tooling, and tuning it constantly.

SentryArk runs your security operations for you, 24/7. We bring your logs into a SIEM for central visibility, protect endpoints with EDR, and use SOAR playbooks to contain common threats in minutes rather than hours. Our analysts investigate every alert that matters and escalate only what needs your attention.

Because our SOC works alongside our penetration testers and red team, the detections watching your environment are built from how attackers actually operate.

24/7 SIEM, SOAR AND EDR

We work with the platforms you already run, or help you choose the right ones. Onboarding starts with a coverage map of your log sources, from cloud and identity to firewalls, servers and endpoints, so you know exactly what is monitored and what is not.

- Log and telemetry onboarding
- SIEM detection engineering
- EDR monitoring and isolation
- SOAR response playbooks
- Proactive threat hunting
- Incident and breach response

OFFENCE-INFORMED DETECTION

Every technique our testers use in client engagements becomes a detection rule, mapped to MITRE ATT&CK and tested against real attack simulations. We tune continuously to cut false positives, so your team is not buried in noise.

Our Team Yazhi hunters search your environment for signs of compromise that alerts alone would miss. When an incident does happen, our responders investigate, contain and help you recover, with reporting ready for management, auditors and CERT-In.

ONBOARDING AND OPERATIONS

Our SOC service follows a structured onboarding and a continuous operating cycle aligned with NIST incident response guidance. Every stage is documented, so you always know what is monitored, what was found and what was done about it.

Assessment and onboarding	01	We review your environment, agree log sources, escalation contacts and response times, then deploy collectors and EDR agents.
Detection engineering	02	We baseline normal activity, enable and tune detection rules mapped to MITRE ATT&CK, and build SOAR playbooks for common threats.
24/7 monitoring and triage	03	Analysts triage alerts around the clock, enrich them with threat intelligence and escalate confirmed incidents to your named contacts.
Hunting and response	04	Regular hunts look for what alerts miss. For confirmed incidents we contain through EDR and SOAR, find the root cause and support recovery.
Reporting and improvement	05	Monthly reports cover alerts, incidents, hunts and coverage. Findings from our offensive engagements feed back into new detections.

The service includes

- Log source coverage map
- Automated SOAR response playbooks
- Incident reports with root cause
- Tuned detections mapped to MITRE ATT&CK
- Monthly service and threat reports
- CERT-In ready incident documentation

ABOUT SENTRYARK

SentryArk is a team of security engineers, SOC analysts and offensive security specialists. Our consultants hold OSCE, CRT0, CEH and ISMS certifications. We have secured 20+ organisations, assessed 8K+ devices and 30+ applications, and reported 250+ vulnerabilities. Because the same team attacks and defends, our advice reflects how real attackers operate.