ebryx

EBRYX DETECTION AND RESPONSE SERVICES

Continuous security monitoring, detection and response capabilities are now regarded as essential for organizations of all sizes. Preventive technologies such as firewalls and malware protection systems can and do fail, often due to mistakes people make or due to imperfections in the preventive technology itself. A sound security posture requires both proactive detection of security incidents and responding to them in a timely manner.

Ebryx provides several managed security services through our Security Operation Centers (SOCs), located around the world, for continuous monitoring, threat hunting, incident response and protection of data theft by insider or external threat actors.

Managed SOC Service

Through fully-outsourced, managed SOC service our team of security analysts provides 24x7 proactive security monitoring, and incident remediation advisory powered by premium Cyber Threat Intelligence. Ebryx provides great value for money by offering a highly cost-effective managed SOC service in comparison to having an in-house team.

- 24x7 security monitoring and reporting
- SIEM troubleshooting and optimization
- Rapid threat detection & remediation advisory
- Custom data-source integration and rule writing
- Use-case development as per the business need
- Weekly meetings and monthly threat reports

Co-Managed SOC (L2 as a Service)

Ebryx Level2-Analyst-as-a-Service offering is designed for organizations who prefer to get the basic SIEM monitoring done by their internal security/SOC team. The service augments the internal SOC setup by providing more complex analysis and troubleshooting services whenever required.

- Non-persistent connection to the client’s existing SIEM deployed on-prem or cloud
- Advanced offense investigation for the escalated cases from L1
- Custom data sources integration, parsing and correlation rule writing
- SIEM rule-set tuning, thresholding and suppression to reduce False Positives
- Advisory role for client’s internal L1 team with weekly meetings and monthly progress reports
- Quarterly SIEM/SOC effectiveness review

Threat Hunting Service

Ebryx Threat Hunting service backed by certified, battle-hardened team, proactively and iteratively hunting through your network, cloud and endpoints to detect and isolate the most advanced threats which evade the conventional set of security controls deployed in your organization.

- Coverage of tactics and techniques based on MITRE ATT&CK framework
- Adversary focused hunt missions
- Advanced use-case development to detect TTPs of the region/industry-specific APT groups
- Enhanced OS telemetry for greater forensic visibility into the endpoints
- Monthly environment sweeps against the emerging threats
- Custom cross-correlation rule writing for disparate data-sources
- Malware Analysis and Reverse Engineering
- Continuous threat modeling to cater the dynamic threat landscape

Why Ebryx?

Our Team

Ebryx has deep expertise in cybersecurity. Our team of security analysts is well-equipped through renowned industry certifications like GIAC Reverse Engineering Malware (GREM), GIAC Certified Forensic Examiner (GCFE), GIAC Certified Intrusion Analyst (GCIA) & Offensive Security Certified Professional (OSCP).

Strong R&D Background

Our research and development services power some of the world's leading security products. We have contributed to several patents on malware classification and have been the first to uncover malware in consumer applications and services offered by leading global brands.

Clients and Partners

Some of the world's leading tech companies are using our services to help them improve their security posture. We are also value added resellers and implementation partners to some of the most innovative security tech companies around. These capabilities enable us to become your primary security partner.

About Ebryx

Ebryx is a leading cybersecurity, software and hardware solutions company with vast experience in security product engineering, malware research and managed services for customers around the world. Our team of security analysts is well-equipped through renowned industry certifications like GIAC Reverse Engineering Malware (GREM), GIAC Certified Forensic Examiner (GCFE), GIAC Certified Intrusion Analyst (GCIA) & Offensive Security Certified Professional (OSCP).

| securenow@ebryx.com