CAPTAIN Cyberscaler

CAPTAIN CYBERSCALER ADVANCED SECURITY SERVICES: BASIC BUNDLE

→ EMAIL SECURITY

Email remains the top attack vector for cyber breaches, making robust email security essential. Our services include:

- Malware Detection: Identify and neutralize malware threats.
- Phishing and Ransomware Detection: Prevent phishing attempts and ransomware attacks.
- Phishing Tests: Conduct regular tests to maintain employee awareness.
- Zero-Day Threat Protection: Defend against unknown threats.
- Email Encryption: Secure email communications.

→ WEB SECURITY

Many websites are inadequately tested, making them vulnerable to malware. Our web security services protect against these risks:

- Phishing and Malware Blocking: Prevent access to malicious websites.
- Enforcement of Acceptable Use Policies: Ensure compliant web usage.
- Remote Filtering and SSL Inspection: Securely filter web traffic and inspect encrypted connections.

→ ENDPOINT PROTECTION AND EDR

Endpoints are prime targets for malware. Our Endpoint Detection and Response (EDR) service offers:

- Ransomware and Malware Scanning: Monitor and protect all endpoints and servers.
- Quarantine and Remediation: Isolate and remediate infected devices.
- Integration with Threat Intelligence Feeds: Stay updated with the latest threat information.

→ DEVICE ENCRYPTION

Device encryption is crucial for protecting data on lost or stolen devices. Our encryption services include:

- Full Disk Encryption Enforcement: Ensure all devices are encrypted.
- Encryption Management: Regularly update and manage encryption keys.

THANK YOU

CAPTAIN HYPERSCALER, LLC

MORE SERVICES

- Client requirements: Provide IT contacts that will open tickets and interact with Captain Cyberscaler SOC. This SOW does not provide end-user helpdesk (which can be provided at additional cost).
- Baselining the service: Deploy the agent to all end user endpoints and servers; identify and remediate anomalies such as unknown applications or services, remove any applications or services that are not in policy, work toward a secure steady-state environment.
- Continuous monitoring and detection of security threats: Continuous monitoring of network traffic, endpoints, servers, and other critical assets for signs of suspicious or malicious activity.
- Prompt investigation and prioritization of security incidents: Prompt investigation of security alerts and incidents to determine the nature and severity of the threat. Prioritization of incidents based on their severity and potential impact on the organization's operations.
- Proactive threat hunting and response: Proactive hunting for advanced threats and indicators of compromise within the organization's environment. Use of threat intelligence feeds and behavioral analytics to identify potential security risks before they escalate into full-blown incidents.
- Forensic analysis and reporting: Detailed forensic analysis of security incidents to identify the root cause, attack vectors, and tactics used by threat actors. Generation of comprehensive incident reports documenting findings, remediation steps taken, and recommendations.
- Continuous improvement and optimization of security processes: Collaboration with stakeholders to identify gaps in security controls and implement proactive measures to strengthen defenses.
- Compliance and regulatory support: Guidance on implementing security best practices and controls to meet regulatory obligations.

+1 248-395-3989

https://captainhyperscaler.com