CAPTAIN CYBERSCALER MANAGED SECURITY SERVICES

We have the security skills to cover you 24/7/365.

With threat actors using sophisticated multi-prong cyber tactics to get at your data combined with the rapidly expanding network of mobile, IoT and connected devices and lack of certified security skills and resources, it's time to get help.

➜ SOME STARTLING CYBERSECURITY FACTS:

- Breaches increased by 72%
- Average breach cost is $4.45M
- Cybersecurity workforce gap reached 4 million in 2023
- Average time to identify a breach is 207 days
- Average ransomware payout increased from $812,380 in 2022 to $1,542.333 in 2023
- More than 77% of organizations do not have an incident response plan

➜ DO YOU KNOW WHAT THE MOST COMMON CAUSE FOR THE RAGING NUMBER OF CYBER BREACHES IS?

➜ MORE THAN:

- 80% of organizations report a shortage of cybersecurity skills. (Source: ISSA)• Average breach cost is $4.45M
- 45% of in-house IT and security people lack the required expertise to deal with advanced threats

➜ TIME TO ACT NOW!

Captain Cyberscaler Managed Security Service offerings are aimed at simplifying the lives of IT managers and CTOs alike. Our security experts work like an extended arm to your IT and security team helping secure your business round the clock. Be it tackling new threat actors or addressing the problem of skill shortage, our Managed Security packages are designed keeping in mind the diverse business needs and budgets.

✔ WHY FUTURISM'S MANAGED SECURITY SERVICES?

- Full stack of security defense-in-depth levels available
- Service based on best of breed security products/technology
- Monthly service fee - no product or capital costs
- LowerTCO
- 24/7/365 coverage and support
- SOC 2 Type 2 Compliance
- ISO 27001 Certified
- CMMI Level 3 Certified

✔ OURMANAGED SECURITY SERVICES SUITE OFFERS THE FOLLOWING TWO PACKAGES:

- Starter offering
- Advanced Malware offering

➜ STARTER SECURITY PACKAGE

MITIGATE ATTACK SURFACE FOR A RANGE OF ADVANCED THREATS

Backed by leading global threat intelligence technology (Sophos), our Starter Security Pack offers a comprehensive suite of flexible managed security services to protect against a wide range of advanced threats/ vulnerabilities and reduce the attack surface significantly.

✔ EMAIL SECURITY

- Detects phishing attempts/Ransomware/malware
- Phishing tests for employee awareness
- Zero-day threat protection

✔ WEB SECURITY

- Enforce acceptable use policies
- Block attempts to click on websites containing malware
- Remote Filtering and SSL Inspection

✔ ENDPOINT PROTECTION INCLUDING EDR

- Scan and detect Ransomware and malware across all endpoints including mobile
- Quarantine and remediate infected devices, machines, servers, etc
- Advanced risk and threat analysis

✔ DEVICE ENCRYPTION

- Enforce full disk encryption
- Encryption management
- Remote access

➜ ADVANCED THREAT PROTECTION PACKAGE

Get ahead of advanced and sophisticated threat actors with our advanced threat protection package powered by IBM Security.

Get round-the-clock protection from the most advanced threat vectors and respond to security incidents much faster. Our Advanced Threat Protection package uses IBM QRadar and intelligence feeds from X-Force to provide up-to-the-minute protection from novel threats including new strands of Ransomware.

➜ INSIDER THREAT DETECTION

PRIVILEGED USER MONITORING

- Preconfigured alerts and notifications for DoS attacks and hijacked accounts
- Behavioral analytics

TRUSTED HOST AND ENTITY COMPROMISE

- Determine risk score of an entity (e.g. disgruntled employee)
- Track Network Activity
- Remote Access Activity (Credential theft, password sharing)
- Identity (credential violations, account takeover, privilege escalations)
- DNS (Tunneling, Exfiltration)
- File Integrity Monitoring

ABNORMAL AUTHENTICATION BEHAVIOR

- Real-time alerts for brute force attacks, password guessing, and unauthorized access
- Customize rules to detect unusual network activity

CLOUD DISCOVERY

- Track abnormal cloud usage and workload
- Centralized security monitoring and behavior analysis
- Cloud network visualization in real-time
- Container security
- Detect multi-vector attacks
- Identify misconfigurations
- Advanced user monitoring capabilities

✔ ADDITIONAL OFFERINGS

➜ BACKUP & RECOVERY

- If you don't back up your data you can't recover from a ransomware attack
- If you do back up your data you can usually recover within hours
- Local backup, remote immutable backup
- We ensure your data is backed up on a regular basis
- Regularly test backups and run recovery tests

➜ VULNERABILITY AND PATCH MANAGEMENT

- With over 28,000 vulnerabilities discovered in 2023, it's impossible for a small IT staff to keep up.
- We do this for you, keeping SLAs for critical patches
- Work with you to automate resources that don't need maintenance windows
- Work with you to schedule maintenance windows for critical resources
- Test patches on test system
- Deliver reports for compliance

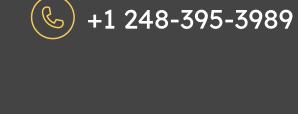### ➜ IDENTITY AND ACCESS MANAGEMENT

- Making sure that directories are kept up to date with the addition and deletion of access.
- Integrate with HR tools such as KPG
- Upgrade access management with Privilege Access Management and Multi-Factor Authentication
- Create and enforce access policies for third party supply chain vendors

➜ MOBILE DEVICE MANAGEMENT

➜ IOT DEVICE MANAGEMENT

We provide critical cyber security protection that enhances the capabilities of IT Security teams that are understaffed.

Contact us now so we can partner with you to fight the bad guys!