PROVEN SOCaaS
SECURING BUSINESSES

At Bridgehead IT, our commitment to excellence means delivering enterprise grade security with a personalized approach. You can count on our seasoned experts to keep you protected, informed, and confident in your technology.

200+
Partners Trusted Across Industries

24 MIN.
Avg. Response Time in 2025

96%
Of Incidents Responded To Within An Hour

Fast Response Times

Immediate Assistance. Our team is always on standby to address your security concerns promptly. Threats and issues are handled quickly, minimizing downtime and keeping your systems protected. Our goal is to take swift action and keep your operations running smoothly.

Personalized Support

Talk to a Real Person. We value human interaction. When you reach out, you will speak directly with a member of our US based team. This ensures you receive real time assistance from professionals who understand your needs. Dedicated Case Manager. Every client is assigned a dedicated case manager as a consistent point of contact. They will guide you through every step, answer your questions, and provide ongoing support.

Expert Guidance

Tailored Advice. We take the time to explain complex security issues in simple, understandable terms. Our team provides specific guidance based on your current security posture and helps you plan your next steps. Expertise on Demand. Whether you are implementing new security measures or assessing potential threats, our experience is available to help you make informed decisions.

EDR Tool Agnostic

Endpoint Detection and Response tools monitor and respond to threats on endpoints such as laptops and servers. Bridgehead uses industry leading solutions like Microsoft Defender for Endpoint. Our proprietary threat management system also integrates with your existing enterprise EDR tools to provide flexibility without compromising protection.

OUR SERVICES

	STANDARD SERVICE	PREMIUM PACKAGE
MONITORING:		
EDR Monitoring	x	x
Server Log Monitoring		x
Firewall Log Review		x
24x7x365 Monitoring		x
VULNERABILITY MANAGEMENT:		
Internal Vulnerability Scans		x
External Vulnerability Scans		x
MAINTENANCE:		
Report Configuration	x	x
Proactive EDR Changes		x
Reactive EDR Changes	x	x
Bring Your Own Tool (BYOT)*	x	
INCIDENT HANDLING:		
Managed Threat Response		x
Configure Alerting (Customer Only)	x	
Isolation and Containment		x
IDENTITY:		
Daily User Risk Reviews	x	x
Realtime Response*	x	x
THREAT ANALYTICS:		
Alert Review and Reporting	x	x
Endpoint Log Review	x	x
Root Cause Analysis Of Alerts		x

* Use the enterprise security tools you already have — no need to rip and replace. We integrate with solutions like CrowdStrike, SentinelOne, MDE, Huntress, and more.

*Real-Time Response is available with applicable Microsoft AIP (Azure Information Protection) licensing or approved equivalent.

Incident Management: Bridgehead IT's SOCaaS covers monitoring, alerting, and remediation for routine security events. However, **full Incident Management (IM)** is not included. IM applies to events that meet one or more of the below criteria:

Impact **10% or more** of users or endpoints (minimum 10 devices/users), involve critical infrastructure such as servers or domain controllers, backup servers, etc. or require forensic analysis, legal reporting, or coordinated recovery efforts.

Expert Guidance

Partner with Bridgehead IT to safeguard your business's digital assets and drive technological advancement.

Contact us now to invest in your future and achieve guaranteed outcomes that bring peace of mind and improve your bottom line.

Gary Beadle

Director Of Business Development

Contact:

(210) 237-4253
Gary.Beadle@BridgeheadIT.com
linkedin.com/in/gary-beadle-bb544a11