FOXTECH DEFEND

FEATURES LIST

FOXTECH
DEFEND

Features List	DEFEND Essentials	DEFEND	Notes/Description
Security Operations Centre			
Integrated Security Operations	✓	✓	We integrate with your other Security tools and products, monitor them and use them to take defensive actions.
Access to UK Cyber Security experts	✓	✓	UK experts available by phone, email, and instant messaging.
True CyberSecurity Partnership	✓	✓	FoxTech is dedicated to understanding your unique security needs offering customised strategies and robust support.
Pro-active advice	✓	✓	We're here to help make sure you're doing the right things. Not just generating alerts for you.
Cloud Monitoring			
O365/Google Workplace	✓	✓	Continuous cloud monitoring across AWS/Azure, providing real-time threat detection and response
IaaS Montioring: Azure, AWS, GCP	✓	✓	Real-time O365/Google Workplace monitoring immediate threat identification and remediation
SaaS Apps		✓	Proactive threat detection, analysis, and swift response across SaaS applications.
Host Intrusion Detection			
File Integrity Monitoring	✓	✓	Monitors changes to critical system files and configurations, alerting to unauthorised changes. Crucial in detecting potential breaches.
Server Monitoring	✓	✓	In-depth analysis of server activities and application behavior to identify threats.
Workstation montioring		✓	XDR (Extended Detection and Response) agent on workstations for real-time threat detection through log analysis.
Netflow Monitoring			
Network flow monitoring		✓	Leveraging flow data from your network devices enables early detection and alerts on malware Command & Control connections.
Protective DNS		✓	Anycast DNS service blocks malicious domains in real time, with FoxTech Defend monitoring.

FOXTECH
DEFEND

Features List	DEFEND Essentials	DEFEND	Notes/Description
Threat Intelligence			
Threat intelligence feeds	✓	✓	Advanced threat detection and response using current intelligence on adversary tactics and Indications of Compromise (IoCs)
Dark Web Monitoring		✓	Ongoing dark web surveillance to detect company information leaks, mitigating risks before they impact your business.

Rapid Incident Response			
Instant Response		✓	Pre-defined automated responses to immediately defend against attacks.
Extended Detection and Response (XDR)	✓	✓	Pre-defined response actions such as: Block IP at firewall; Isolate Device; Remove e-mail from mailbox
Day 1 Incident Response Manager	✓		We will provide an incident response manager for the first day to coordinate actions after a major incident.
Week 1 Incident Response Manager		✓	We will provide an incident response manager coordinates first-week actions post major incidents.
Bespoke Incident Response Plan		✓	We will work with you to create a bespoke, and workable, incident response plan

Forensic Log Storage			
6 months log retention	✓		We will keep logs for 6 months to allow for the investigation of historic events
12 months log retention		✓	We will keep logs for 12 months to allow for the investigation of historic events
Tamperproof, offsite log storage	✓	✓	Logs stored offsite, with chain of signatures to protect from tampering

Compliance Reporting			
Unified security dashboard	✓	✓	All security events aggregated in **FoxTech DEFEND** dashboard.
Weekly Summary Report	✓	✓	Weekly security summary reports, sent via email.
Quarterly In-Depth Report	✓	✓	In-depth written report created by our analysts once per quarter.
Monthly security review		✓	Monthly meeting to review any key activities and recommendations

Features List	DEFEND Essentials	DEFEND	Notes/Description
Expert Analysis			
Full triage and analysis of alerts	✓	✓	Our Security Experts will comprehensively examine alerts for nature, impact, and accuracy.
MITRE ATT&CK Model mapping	✓	✓	Threats mapped to MITRE ATT&CK for structured defense strategies.
Dedicated UK Analysts	✓	✓	Staffed by experienced cybersecurity professionals based in the UK, providing expert analysis and support.
Proactive Threat Hunting		✓	Proactive threat hunting involves in-depth analysis and investigation to uncover and neutralize previously unidentified threats.
Human Security			
Policy Management		✓	The platform promotes compliance and security awareness through policy management.
Security Awareness Training		✓	Comprehensive, bite-sized cybersecurity training to bolster employee skills in recognising and defending against cyber threats.
Policy portal for auditers		✓	A secure portal for auditors to access company policies, enhancing transparency and efficiency in compliance reviews.
Phishing simulations		✓	Phishing simulations test and enhance employee threat awareness.

FOXTECH
DEFEND

Thank You!

To get a demo or start your free trial,
please contact us today

☎ 0330 2235622

✉ info@foxtrot-technologies.com

in https://www.linkedin.com/company/foxtechuk/