

A wireframe illustration of a padlock in the center, with two hands on either side, all rendered in a light purple color. The padlock and hands are composed of interconnected lines and dots, giving them a digital or network-like appearance. The background is a solid dark purple.

Managed Security Service

Protect Your Business With Managed Security Solutions



80-90%

of ransomware originated through unmanaged devices

(Source: Microsoft)

Adversary in the Middle

attacks are increasing making traditional MFA less effective

54%

of phishing campaigns targeting consumers impersonated online software and service brands.

(Source: Microsoft)

99%

of identity attacks are password attacks.

(Source: Microsoft)



How do we deal with these threats?

DIY

- Buy a product
- **Deploy:** do we have the skills in-house?
- **Monitor:** whose job is that? 24x7 etc.
- Who Remediates?
- Doesn't change the security landscape per se.

SUBSCRIBE TO A SECURITY OPERATIONS CENTRE (SOC)

- Like a burglar alarm

Quorum's Managed Security - Services



Managed Security Service

Onboarding Project and ongoing Managed Security Service



Cyber Essentials Readiness

Pre-assessment against Cyber Essentials criteria

Assistance with remediation activities

Completing Assessment

Managed Security Service



Managed Security Service



Protect your business with
Managed Security Solutions



Increased threat: Cyber-attacks are becoming more frequent and sophisticated, targeting businesses of all sizes.



Significant Impact: The impact of a cyber-attack can include significant financial penalties but can also be extremely detrimental to your brand.



Do more with less: Many businesses are purchasing services and tools from multiple vendors which can be costly and may not integrate well to your overall IT ecosystem.



Do the basics; Regular basic security hygiene still protects against 99% of attacks.



Round the clock: Attackers don't work a 9-5. Businesses now need the ability to react 24x7 to attacks.



Education: Staff will be targeted and taking the correct action can nullify many cyber-attacks. Employers need to find a way of regularly updating their staff on cyber threats.



Audits; are becoming more and more difficult to pass without cyber security basics in place.

Service Benefits

Protection



Implement dedicated security software for endpoints, identity, Office 365, and SaaS apps to reduce the likelihood of successful phishing, malware, or identity compromise.

Detection



Implement continuous detection and monitoring to minimise attacker dwell time, with automatic behaviour and trend analysis and alert triaging to reduce false positives.

Improvements



Continuously review and improve security by assessing configurations, applying best practices, and guiding major security enhancements.

Key Features

24/7 INCIDENT MANAGEMENT

PHISHING SIMULATION

CYBER HYGIENE

DETECTION TUNING

REPORTING

AUDIT SUPPORT

**THREAT AND VULNERABILITY
MANAGEMENT**



With additional
alerting &
monitoring of
security related
events.

Key Features

24/7 INCIDENT MANAGEMENT

PHISHING SIMULATION

CYBER HYGIENE

DETECTION TUNING

REPORTING

AUDIT SUPPORT

**THREAT AND VULNERABILITY
MANAGEMENT**

Twice a year or on a
timeline agreed with
the client.

Key Features

24/7 INCIDENT MANAGEMENT

PHISHING SIMULATION

CYBER HYGIENE

DETECTION TUNING

REPORTING

AUDIT SUPPORT

**THREAT AND VULNERABILITY
MANAGEMENT**

Continuously and proactively enhance configurations & services, using best practices & Microsoft Defender XDR telemetry.

Key Features

24/7 INCIDENT MANAGEMENT

PHISHING SIMULATION

CYBER HYGIENE

DETECTION TUNING

REPORTING

AUDIT SUPPORT

**THREAT AND VULNERABILITY
MANAGEMENT**



Analytics used for alerting and monitoring will be tuned for false positives or disabled if irrelevant

Key Features

24/7 INCIDENT MANAGEMENT

PHISHING SIMULATION

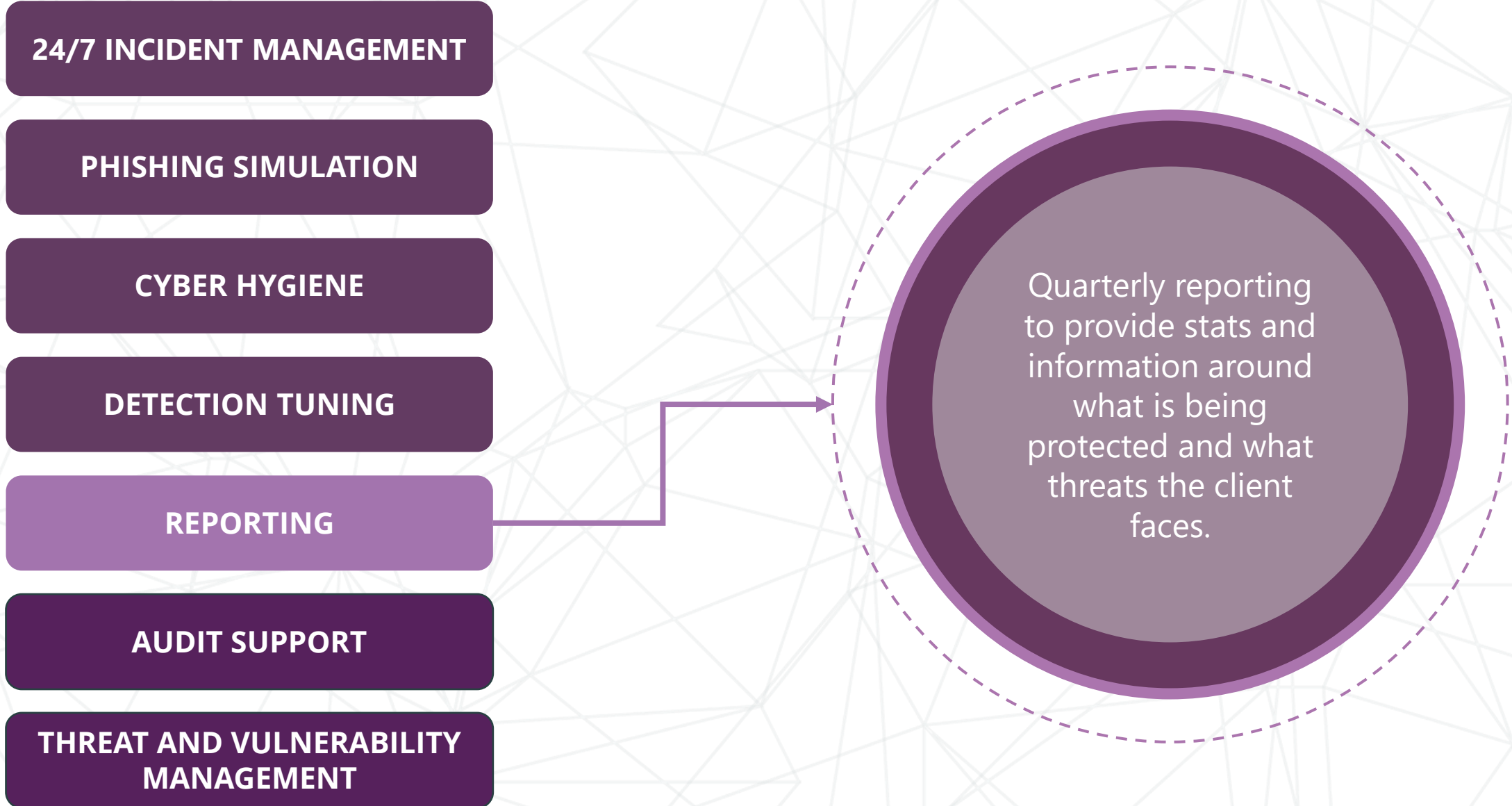
CYBER HYGIENE

DETECTION TUNING

REPORTING

AUDIT SUPPORT

**THREAT AND VULNERABILITY
MANAGEMENT**



Quarterly reporting to provide stats and information around what is being protected and what threats the client faces.

Key Features

24/7 INCIDENT MANAGEMENT

PHISHING SIMULATION

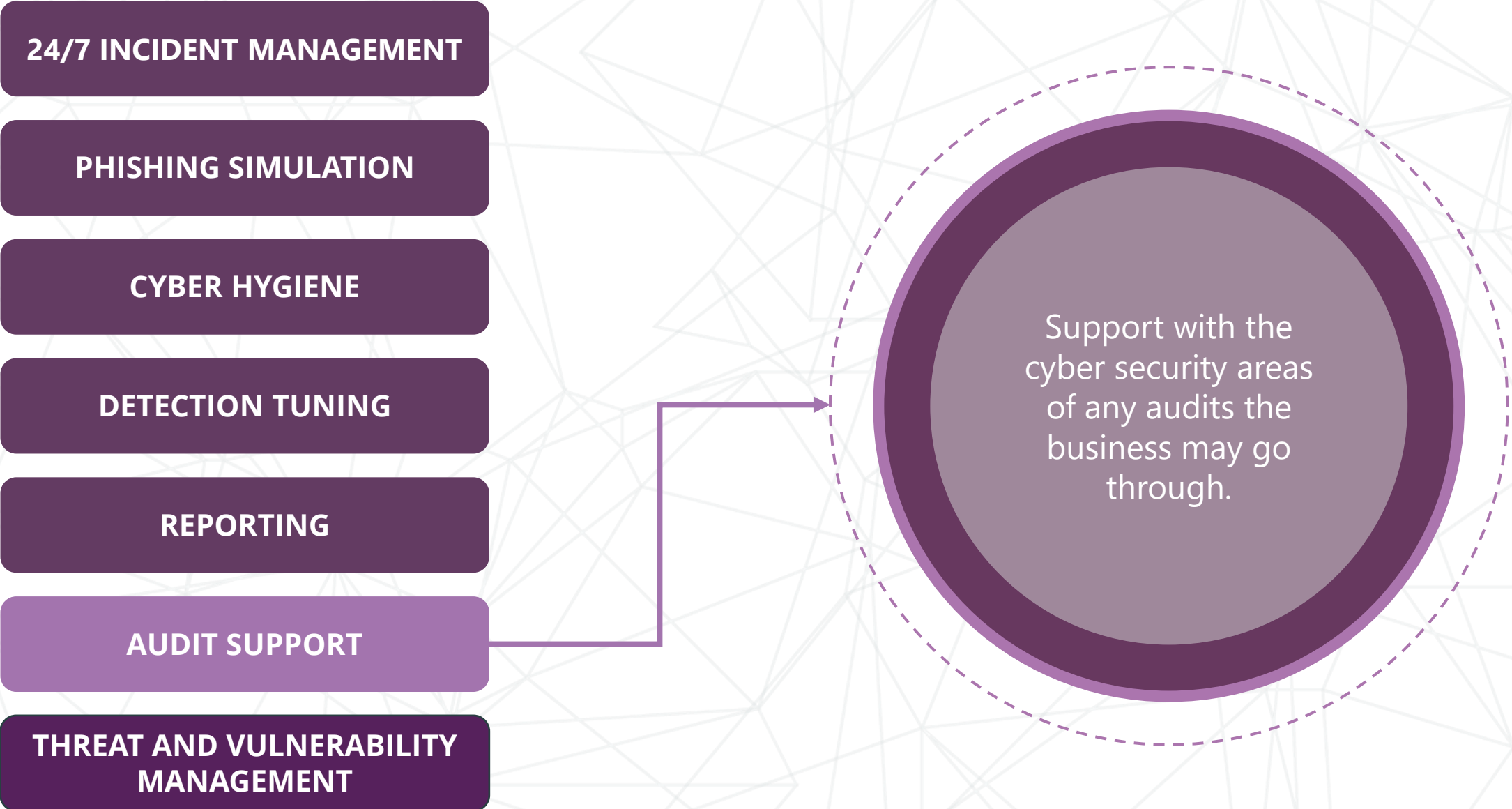
CYBER HYGIENE

DETECTION TUNING

REPORTING

AUDIT SUPPORT

**THREAT AND VULNERABILITY
MANAGEMENT**



Support with the
cyber security areas
of any audits the
business may go
through.

Key Features

24/7 INCIDENT MANAGEMENT

PHISHING SIMULATION

CYBER HYGIENE

DETECTION TUNING

REPORTING

AUDIT SUPPORT

**THREAT AND VULNERABILITY
MANAGEMENT**

Monitor and remediate key vulnerability issues, like unpatched devices or outdated software, and promptly address zero-day alerts.

Journey To Our Managed Security Service

DEPLOY



Microsoft Microsoft Defender XDR



Microsoft Defender for Cloud



Microsoft Sentinel

BASELINE REVIEW

Identity Review and Hardening

Endpoint Management

Email Authentication Review

SERVICE

Continual Security Monitoring

Incident Response

Threat Hunting

Cyber Hygiene

Phishing Submissions

Analytic Tuning

Phishing Simulation

Reporting

Journey To Our Managed Security Service

DEPLOY



Microsoft Microsoft Defender XDR



Microsoft Defender for Cloud



Microsoft Sentinel

BASELINE REVIEW

Identity Review and Hardening

Endpoint Management

Email Authentication Review

SERVICE

Continual Security Monitoring

Incident Response

Threat Hunting

Cyber Hygiene

Phishing Submissions

Analytic Tuning

Phishing Simulation

Reporting

Journey To Our Managed Security Service

DEPLOY



Microsoft Microsoft Defender XDR



Microsoft Defender for Cloud



Microsoft Sentinel

BASELINE REVIEW

Identity Review and Hardening

Endpoint Management

Email Authentication Review

SERVICE

Continual Security Monitoring

Incident Response

Threat Hunting

Cyber Hygiene

Phishing Submissions

Analytic Tuning

Phishing Simulation

Reporting

Managed Security Service

PRE-REQUISITES

E3 + E5 Security licensing or E5 License
Business Sponsor aligned
Intune available
Scrapman application management tool available

CONTRACTUAL REVIEW

Managed Service Agreement implemented
Service Delivery Manager assigned
Monthly Cost defined

ONGOING SUPPORT

Quarterly Reports
Phishing Simulation
Detection Tuning
Threat and Vulnerability Management

ONBOARDING PROJECT

Estimated 16–20-week onboarding timeframe
A form of Protection Starts from Week 2
Time and materials engagement



Cyber Essentials



99%

of internet-originating vulnerabilities are mitigated using the Cyber Essentials technical controls.

82%

Cyber Essentials users are confident that the technical controls provide protection against common cyber threats.

91%

say that the scheme has directly improved their confidence at being able to consistently implement steps to reduce cyber security risks.

80%

fewer cyber insurance claims are made when Cyber Essentials is in place.
(compared to organisations without certification)

88%

of users believe that the scheme has directly improved their understanding of the steps they can take to reduce risks.

69%

of users report that Cyber Essentials has increased their market competitiveness.



Three simple stages guide you through the process.

PRE-ASSESSMENT

We evaluate your IT security posture with a gap analysis to identify areas not meeting Cyber Essentials standards, followed by a remediation plan with clear recommendations.

REMEDiation SUPPORT

We help you address the identified gaps to meet Cyber Essentials requirements, protecting your systems against threats like phishing and malware.

FINAL ASSESSMENT

We conduct a final review and facilitate the official Cyber Essentials Certification assessment, ensuring you can confidently demonstrate compliance.

Certification is priced based on your business size for transparency.

Cyber Essentials Readiness



1.5-week Project

Estimated Price: £6,825

Deliverables:

Gap analysis
Remediation Plan
Document findings and recommendations

Project scoped based on pre-assessment findings

Goal of the project is to resolve open gaps

Quorum can deliver the Cyber Essentials Assessment

Fixed Price based on business size (number of employees)

