ITogether Service Definition Document – Check Point FWaaS

Detailed Description
Check Point Managed Services provide continuous, expert-led management of cyber security controls across network, cloud, endpoint, and email environments. The service is designed to reduce operational burden on internal IT teams while improving threat detection, response, and security posture. The service combines 24x7 monitoring, policy management, threat investigation, and incident response delivered by certified security specialists operating from dedicated security operations centres. Check Point Managed Services can be used as a full outsourced security operations capability or as a co-managed service alongside an internal IT or cyber security team. The service is suitable for organisations that require round-the-clock security coverage but do not have the resources, skills, or budget to operate an in-house security operations centre. Services are delivered using Check Point security platforms and tooling, with structured onboarding, defined service levels, and regular reporting.

Business Benefits
• Improved security posture Continuous monitoring and proactive threat management reduce exposure to cyber risks and improve overall resilience. • 24x7 coverage without internal SOC costs Provides round-the-clock security operations without the need to recruit, train, and retain specialist staff. • Reduced operational burden Day-to-day security monitoring, investigation, and response activities are handled by specialists, freeing internal teams to focus on strategic priorities. • Faster detection and response Security events are identified and triaged quickly, reducing dwell time and limiting business impact. • Access to specialist expertise Customers benefit from experienced cyber security professionals with deep product and threat intelligence knowledge.

- Predictable service delivery
  Managed services are delivered under defined scopes and service levels, supporting budget certainty and governance.
- Supports public sector compliance
  The service helps organisations demonstrate active monitoring, incident management, and continuous improvement aligned with public sector cyber expectations.

Standard Service Components

SECURITY MONITORING

- Continuous monitoring of security events and alerts
- Correlation of events across multiple security controls
- Use of threat intelligence and behavioural analysis
- Identification of suspicious or malicious activity
- Coverage can include network security, cloud security, endpoint protection, and email security depending on customer requirements.

INCIDENT DETECTION AND RESPONSE

- Triage and validation of security alerts
- Investigation of confirmed security incidents
- Containment and mitigation actions in line with agreed playbooks
- Escalation to customer teams where required
- Support during active cyber incidents
- The service can operate as first-line response or as part of a co-managed incident response model.

POLICY AND CONFIGURATION MANAGEMENT

- Ongoing review of security policies
- Rulebase and configuration management
- Change implementation aligned to agreed processes
- Support for platform updates and feature enablement
- This ensures security controls remain effective as environments and threats evolve.

THREAT INTELLIGENCE AND HUNTING

- Use of global and regional threat intelligence
- Proactive identification of emerging threats
- Threat hunting activities to identify hidden risks
- Continuous improvement of detection logic
- This supports early identification of advanced or targeted attacks.

REPORTING AND GOVERNANCE

- Regular operational reports
- Visibility of incidents, trends, and response actions
- Executive-level summaries for senior stakeholders
- Support for audit and assurance activities
- Reports are designed to be suitable for both technical teams and non-technical decision makers.

SERVICE ONBOARDING AND TRANSITION

- Initial service setup and scoping
- Integration with existing security platforms
- Definition of roles, responsibilities, and escalation paths
- Knowledge transfer and service acceptance
- Onboarding is structured to minimise disruption and ensure service readiness.

SERVICE DELIVERY MODEL

- Delivered remotely as a managed service
- Operates 24 hours a day, 7 days a week
- Co-managed or fully managed options available
- Delivered by certified Check Point security professionals

Optional Service Components
To be discussed during scoping exercise.

Service Exclusions
Anything not specifically included in either the above or when the project is formally scoped.

Standard Support Services
8x5 support, Monday to Friday 9am to 5pm

Assumptions
Any and all information will be provided by the customer to enable the full onboarding of the product without hinderance

Contact

Name	Role	Tel	Email
Tim Ripper	Account Director	0113 341 0123	tim@itogether.co.uk
Simon Richardson	Director	0113 341 0123	simon@itogether.co.uk