



Light Touch soc

A proactive light touch approach to threat detection with continuous security improvement:

- Improve threat detection and response
- Dedicated time from Security Experts
- Ease the pressure on in-house teams
- Weekly Security Monitoring with report
- Monthly Security Improvement report
- No long term commitment, based on a subscription model



Challenges of A Security Operation Centre (SOC)

- Large up-front costs for security tools
- Long timescales for setup and configuration
- Long term commitment (1 – 3 Years)
- Lack of resource and skills internally
- Outsourcing risks (Long commitment/lack of value)
- One size fits all (Never meets the needs)
- Normally a big bang approach
- No dedicated IT security team
- Cancellation of contract means they must start again
- Expensive and complex billing (Unpredictable)

Light Touch SOC For Microsoft

- Workshop to understand the business requirements
- Phased Approach
- Little upfront costs for security tools
- Microsoft Azure Sentinel setup (Theirs forever)
- Including Microsoft O365
- Predictable billing based on effort
- Scalable and shrinkable
- Weekly summarised reporting
- Security posture scoring with recommendations
- Monthly service review
- No long-term commitments
- Dedicated security analysts
- Transferable to other outsourced providers
- Little risk in terms of commitment

