Cyber Security Centre of Excellence

Business Case v3.0 Overview

March 2021

B/21/11






Digital and Security
powered by NSS

Scott Barnett, Head of Information and Cyber Security
Deryck Mitchelson, Director of National Digital and Security

Partners

NHS National Services Scotland

National Cyber Security Centre
a part of GCHQ

TAYCITIES
Smarter + Fairer

Abertay University

NHS Tayside

gov.scot

Scottish Business Resilience Centre

University of Dundee

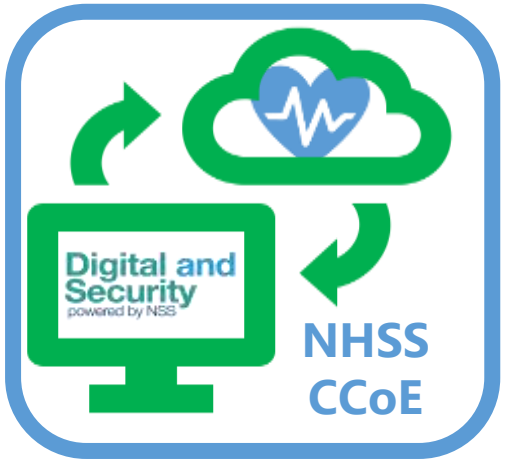
University of St Andrews

Digital and Security
powered by NSS

Executive Summary

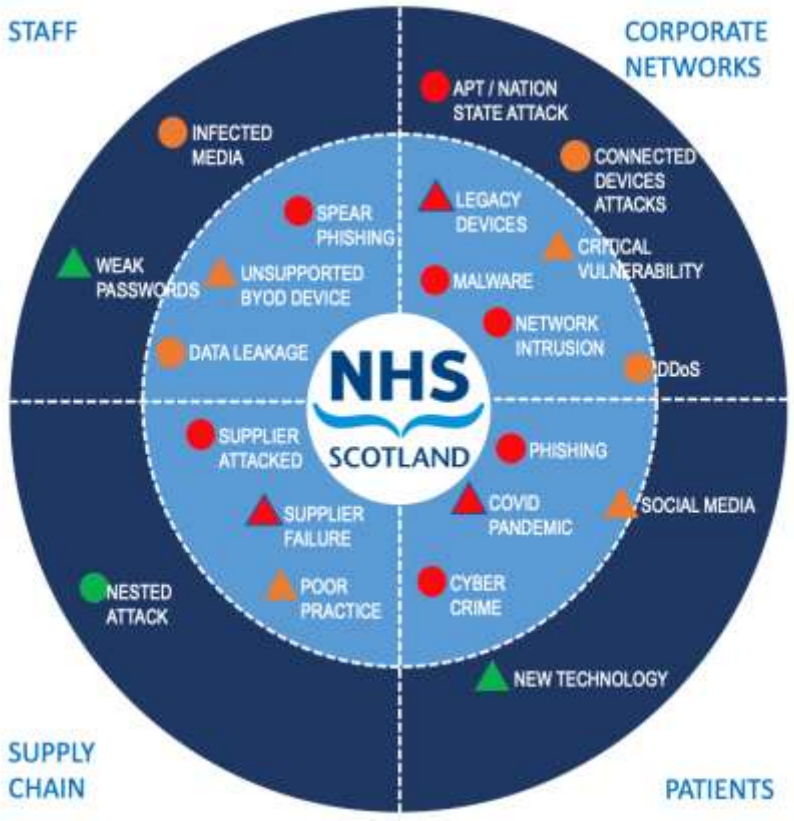
- Level of cyber threat is increasing – 2020 and 2021 seeing threefold increase in adverse cyber specific events. Covid has increased focus on healthcare for organised crime and nation states. Ransomware threat continues to affect public bodies in Scotland and increasingly healthcare is becoming a target
- Scottish Digital Strategy puts digital at the heart of everything we do – essential that digital services are underpinned by strong information and cyber security practices.
- NSS will expand current constrained capability to deliver cost effective NHS Scotland Cyber Centre of Excellence (CCoE) encompassing:

    - 3 full time regional cyber co-ordinators providing local operational expertise and alignment into the national service. The first of these resource is now in place supporting North of Scotland healthcare
    - 24/7 security monitoring and alerting for critical national services and the 22 Health Boards
    - effective cyber incident response and preparation
    - proportionate security and governance reporting
    - strategic and operational cyber threat intelligence collection and dissemination
    - cyber security awareness at both local and national level
    - working with NHS National Education Scotland to establish professional development in cyber
    - tailored cyber security standards, guidance advice and consultancy

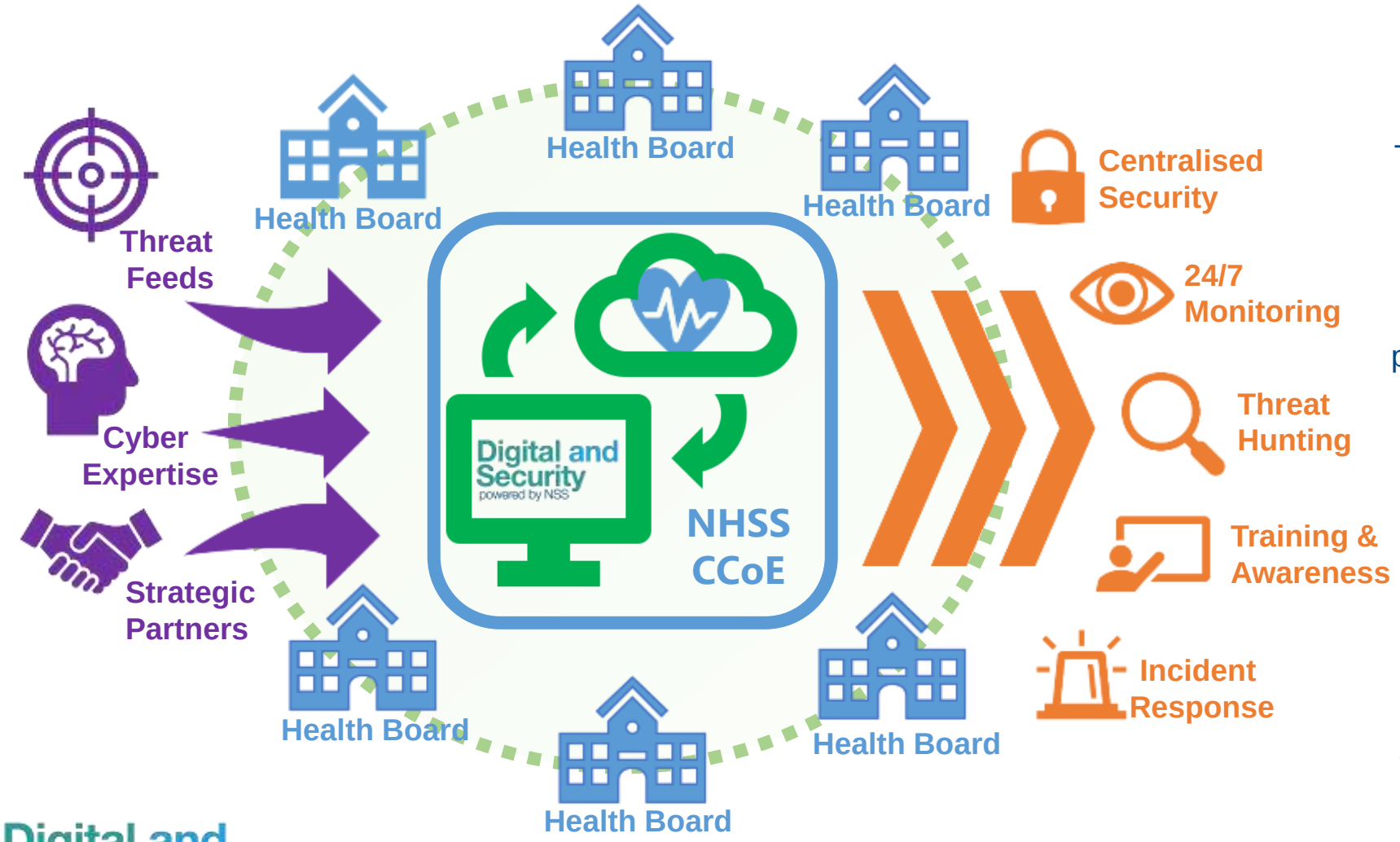


Once for Scotland Approach

- CCoE will be located within the CyberQuarter, Abertay University, Dundee – taking advantage of UK and Scottish Government funding for Tay Cities Deal and developing a pipeline of cyber talent and job opportunities
- We have reserved sufficient space in the CyberQuarter for expansion into Social Care if required and to provide a co-location opportunity, across public sector, bringing like-minded cyber talent together and a cyber-SWAT team
- Services provided directly align with NIS D standards and NHSS Information Security Policy Framework and will assist Board compliance while strengthening controls and cyber response
- Delivering on principles and cross-cutting enablers detailed in the Scottish Government's Cyber Resilient Scotland Strategy
- CCoE, including a fully functioning 24/7 Security Operations Centre delivered at a fully funded cost of £100K per health board over six years to the end of 2026.



NHS Scotland Cyber Centre of Excellence



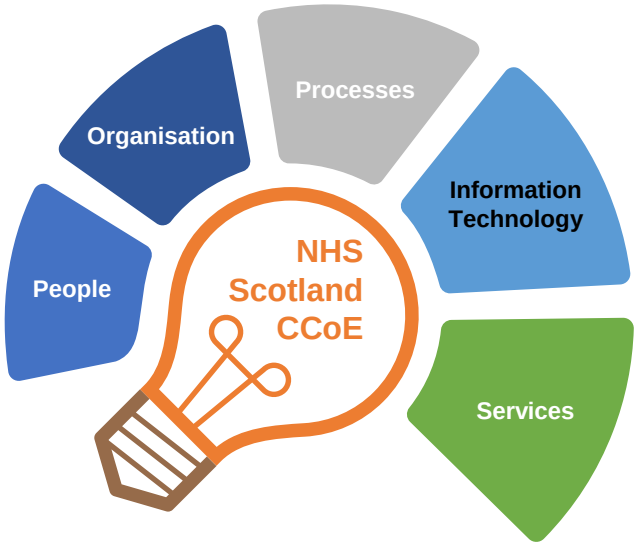
The Cyber Security Centre of Excellence (CCoE) SOC will act as a shared Cyber Threat Monitoring and Response Service for the 22 health boards that constitute NHS Scotland.

Work in full collaboration with Boards providing situational awareness of bad traffic on their networks, actionable threat intelligence from multiple sources and incident analysis and support.

It will also serve as a focal point of Cyber Intelligence sharing with other Scottish, UK and international Government departments and agencies.

Changing the cyber security and awareness culture of the NHS Scotland workforce, enabling them to work safely from multiple locations and adopt national best practice is one of the CCoE's key enablement pillars.

CCoE Key Enablement Pillars



*driving **excellence** through continuous improvement*

Centralised Security

- ✓ A centralised 'Once for Scotland' approach to security standards
- ✓ Aligned with NIS Directive
- ✓ Networking cyber expertise across Scotland
- ✓ Providing Security Assurance services to local Boards
- ✓ Empowering local Board decision making

24/7 Monitoring

- ✓ A single pane of glass view of our national cyber security posture
- ✓ Windows 10 Advanced Threat Protection
- ✓ Continuous monitoring of changing risk and requirements
- ✓ Enhancing local Board level identification and response to new cyber threats

Threat Hunting

- ✓ Consolidated threat intelligence for proactive hunting and eradication of cyber threats in our networks
- ✓ Continuous vulnerability assessment and security testing of critical national systems
- ✓ Deploying NCSC services across Scotland

Incident Response

- ✓ National capability to support local Boards
- ✓ Centralised library of contacts and playbooks
- ✓ Single point of contact for partner agencies –NHS Digital, Police Scotland, NCSC, Competent Authority
- ✓ Trained responders available 24/7

Training & Awareness

- ✓ Proactive awareness campaigns to combat the latest cyber threats
- ✓ Specialist accredited cyber security training
- ✓ Aligned with national strategy and tailored for NHS Scotland
- ✓ Harnessing existing national capability
- ✓ Partnering with Scottish Computer Gaming Sector

*driving **excellence** through continuous improvement*

NHS Scotland Cyber Centre of Excellence

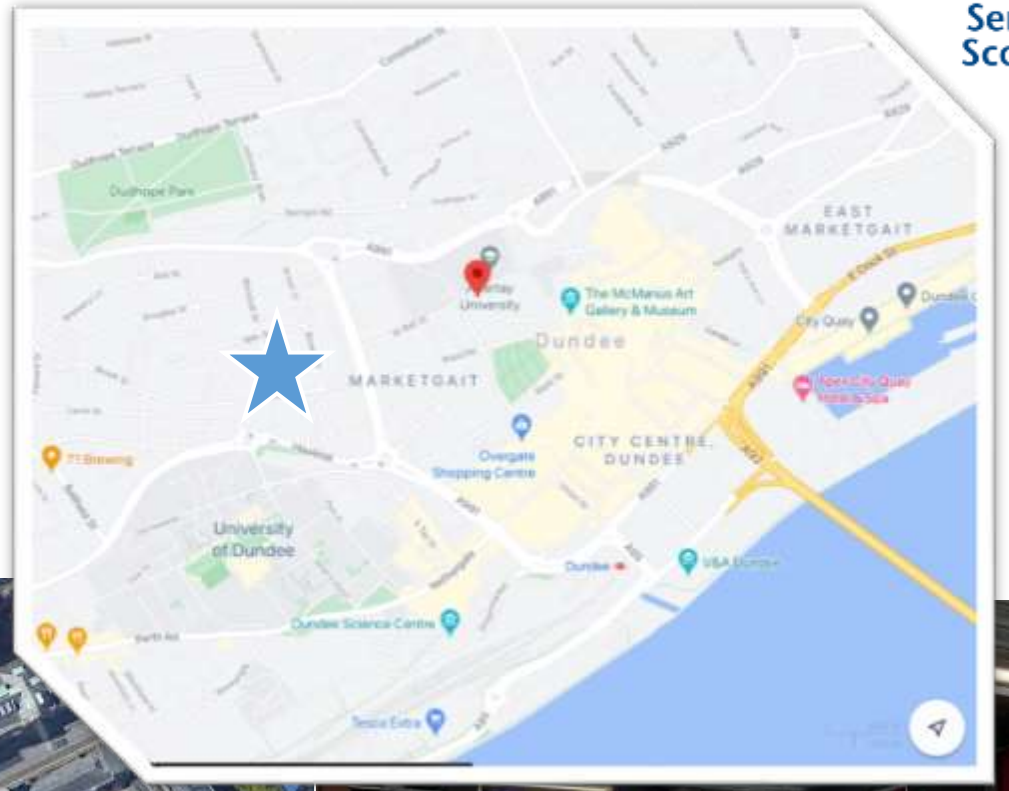
Premises have been identified by key strategic partner, Abertay University, within their campus for the CCoE. This is available, fully configured, at a cost of approximately £82,000 per annum, including facilities management, heating and lighting and physical security. The size of the facility secured is deliberately over-specified, ensuring scalability to provide services to Social Care organisations and potentially other areas of the Scottish Public Sector in the future.

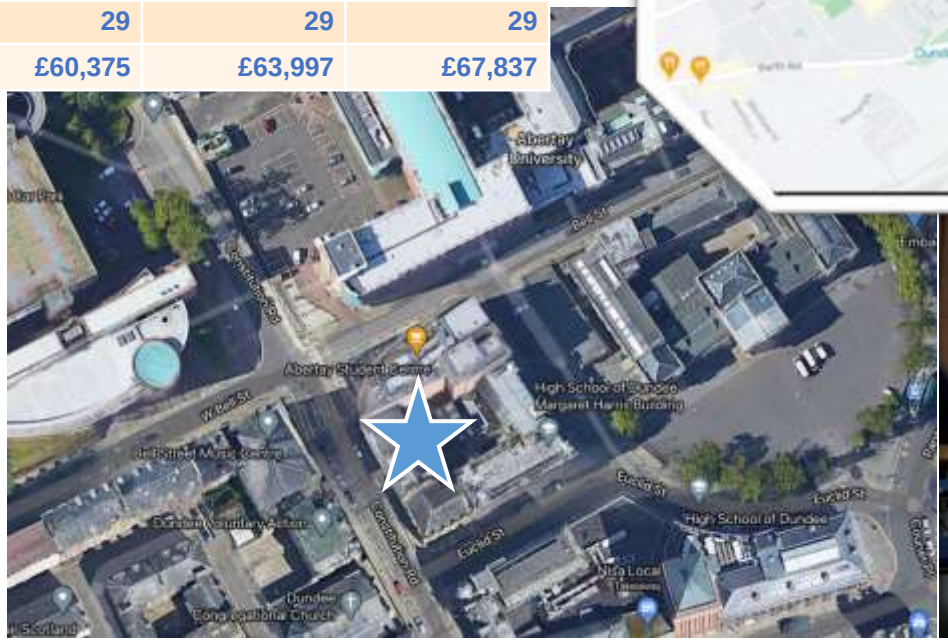
Based in Dundee City Centre, with easy access to transport links, academic partners and the forthcoming Cyber Quarter, this space is fully configurable for NSS. Resourcing is tapered across six years, reaching a full complement of 29 staff. In addition, there is ample capacity to provide suitable desk and learning space for Abertay University under-graduate placements as well as other temporary staff, should we need to flex the capacity to deal with a major incident.

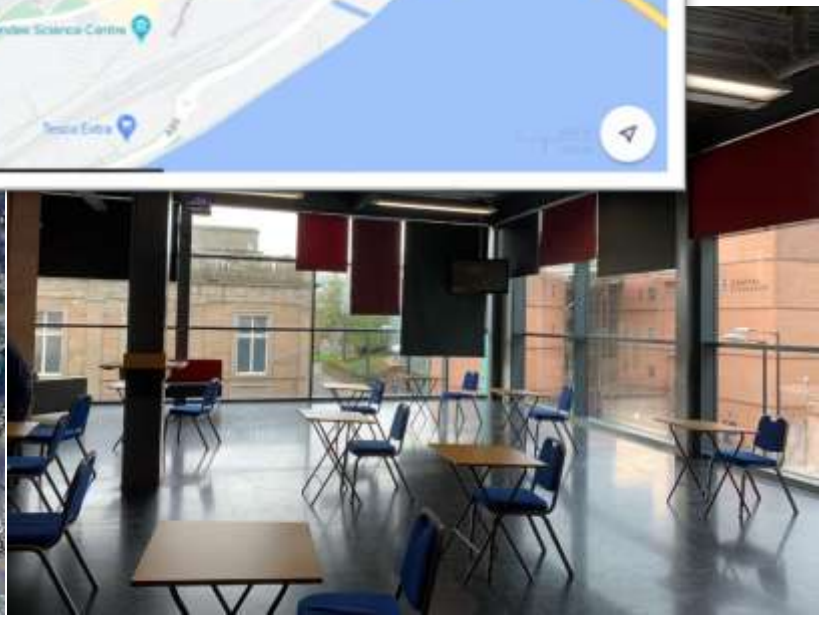
2021	2022	2023	2024	2025	2026
14	27	29	29	29	29
£16,677	£48,797	£56,957	£60,375	£63,997	£67,837

Equivalent value per Board figures for this staffing model are detailed above. NSS DaS will, in providing cyber security services for our Board, commit to providing a total of 8.5 FTE per annum.

The staffing levels in the table reflect a tapered roll out to cater for an assumed requirement of 24/7 security monitoring and response services by end of 2023.







Digital and Security powered by NSS

NHS National Services Scotland

CCoE Service Model

The CCoE will be established to provide services across the NHS that can be easily scaled into Social Care and other areas of public sector if desired. Initial focus will be health boards with none or limited cyber capability as identified in NIS D audits.

These will be either wholly provided or deployed by the CCoE or will be a joint effort depending on the capability and requirements for each Organisation.

This approach is illustrated here and can be tailored for each Board. This will form part of the Charter created that details engagement specifics and demarcation points for each organisation consuming CCoE services.

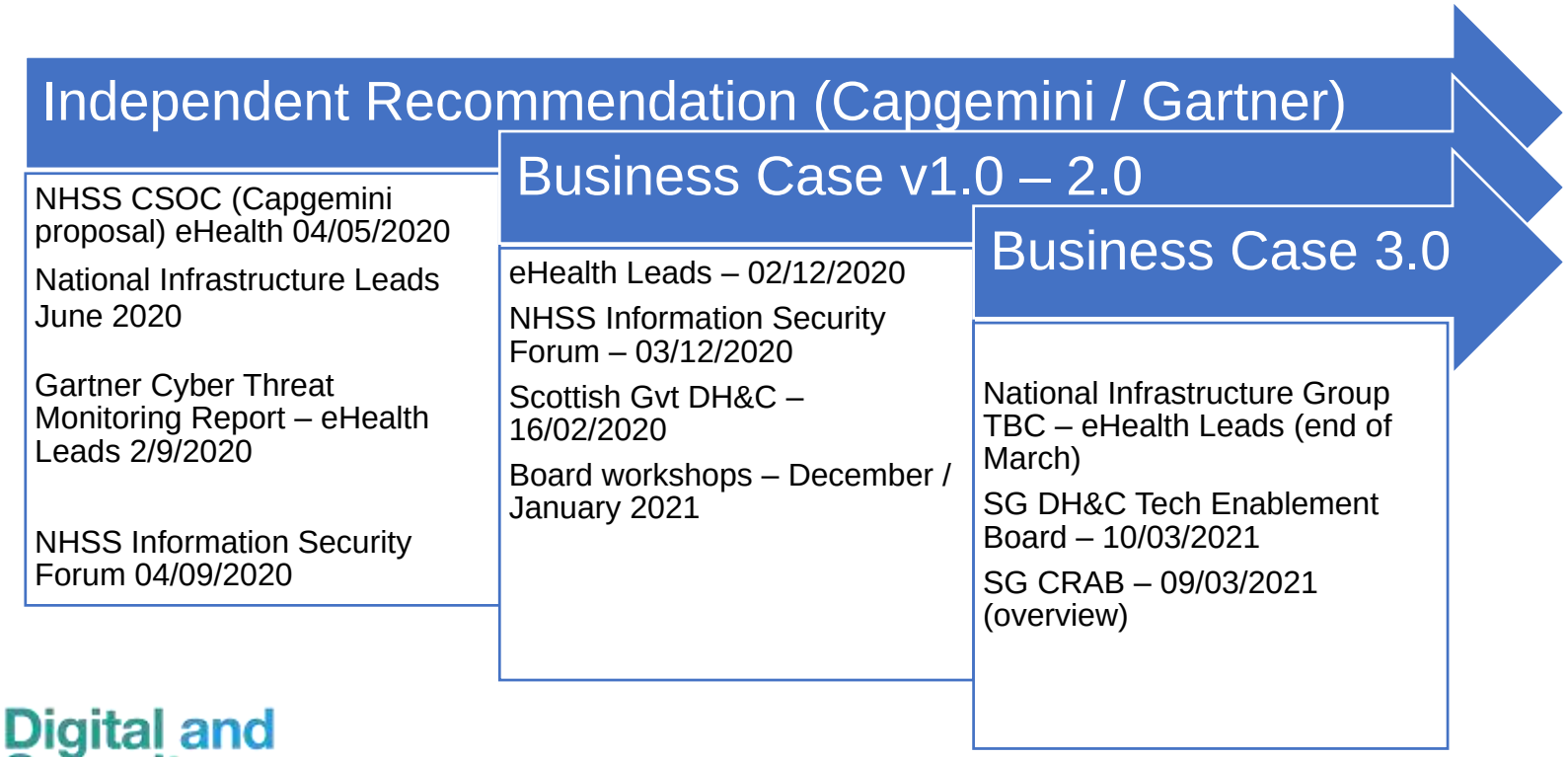
Service	NHS NSS	NHSS Orgs
Proactive		
Threat Hunting		
Vulnerability Management		
Security Posture Monitoring		
Threat Intelligence & Coordination		
Attack Simulation		
Security Platform Management*		
Reactive		
Incident Response and Support		
Reporting		
Malware Analysis (Initial assessment)		
Malware Analysis (Advanced)		
Intrusion Detection		
Security Orchestration & Automation		
Use Case Management		
Strategic		
Policy and Procedure Support		
Security Awareness & Training		
Security Testing		
Asset Management		
Threat Modelling		
Security Architecture Support		
Risk Assessment & Support		
Community Engagement		
Attack Simulation		

Key:

- Provided by the CCoE
- Provided by other part of NHS National Services Scotland
- Provided by third part under control of the CCoE
- Joint provision by CCoE & Local Organisation
- Explicitly out of scope

Engagement Timeline

The final Business Case has been developed from an independent proposal and recommendation from Capgemeni, first presented to NHS Scotland eHealth Leads and Infrastructure Group in Q2 of 2020. Since then, regular updates have been provided to eHealth Leads, the NHS Scotland Information Security Forum, the Infrastructure Group and Boards Information Security specialists have been invited to take part in operating model workshops in December 2020 and January 2021. Version 2.0 of the business case was presented in depth to eHealth Leads in February 2021, with feedback incorporated into Version 3.0. NHS Chief Executives were briefed in January 2021.



Bespoke, detailed, engagement will take place as Boards prepare to join the Centre. Individual Charters will be prepared and agreed, covering demarcation points, services expected and where relevant, service level agreements.

A Governance Board will also be convened to oversee the progress and work of the CCoE. Each Board who are members of the CCoE will be represented at this Board, along with Digital Health and Care as the NIS Competent Authority.

CCoE Security Operations Centre Capability Model

Advanced threat tooling to detect malicious activity in the environment using threat identification techniques. Network analytics, sandboxing and file trajectory analysis.

Collation of multiple sources of actionable threat intelligence. Consuming multiple feeds with internal Intelligence. Feeding threat hunting function

Orchestrated processes to aid threat hunting and achieve containment of threats in < 1 hour

Drive continuous improvement in threat detection and response, red teaming and scenario planning

Level 1

Analyse telemetry and SIEM and respond to alerts based on defined playbooks. Respond to calls from Boards.

Level 2

Proactively hunt for threats based on a wider set of data points. Onboard additional event sources and configure content to aid detection

Level 3

IR team using existing talent in Health boards provide CERT function to drive containment and eradication of major threats

CCoE Regional Engagement Model

The NHS CCoE is designed to leverage, enhance and grow the cyber talent within our Boards. By delivering a ‘pipeline’ of talent through cyber security undergraduate placements in partnership with Abertay University, and promoting a ‘Fusion Centre’ for existing staff to come and spend time on secondment, the Centre will deliver services across all five key enablement pillars, via three levels:

Level 1 (CSOC)	**Oversee and configure our security monitoring tools. They continuously monitor for alerts generated by these tools, which are correlated by a Security Information and Event Management System (SIEM). They then review and triage these to ensure that a genuine security incident is occurring And enrich the data they consider with threat intelligence. Genuine incidents are escalated to Level 2.**
Level 2 (CSOC)	**Address real security incidents. They evaluate Level 1 incidents and begin to pinpoint affected systems and the extent of the attack. They carry out investigations to find the perpetrator, type of attack, and the data or systems impacted and create and implement a strategy for containment and recovery. Includes long term post incident review and solutions recommendation and scoping.**
Level 3 (Regional and SMEs)	**Lead on critical incidents. Arrange and oversee vulnerability assessments and penetration tests to assess the resilience of the Boards to key threats. Create and disseminate contextual strategic threat intelligence reports and integrate SOC services with the wider cyber security services delivered through the CCoE. Develop new and leverage existing cyber awareness campaigns commensurate with the threat landscape. Liaise with vendors and external partners to continually improve cyber security services on a national scale.**

As well as the day to day operational focus of the CSOC, a key success factor for the CCoE will be the efficient and timely engagement of existing resources within the Boards. Our model provides for three Regional Level 3 co-ordinators, who can leverage existing capabilities and act as point persons for incidents, NIS remediation initiatives, exercising and threat hunting services.

Costings

Staffing	2021	2022	2023	2024	2025	2026
Coverage of all 22 Boards	15%	25%	50%	100%	100%	100%
Total FTE staffing levels	14	27	29	29	29	29
NSS funded FTE	8.5	8.5	8.5	8.5	8.5	8.5
Net Staff FTE	5.5	18.5	20.5	20.5	20.5	20.5
Net Staff Cost per Board	**£16677.05**	**£48,797.36**	**£56,957.36**	**£60,374.82**	**£63,997.27**	**£67,837.14**

Staff

SIEM	£247,500	£412,00	£825,000	£1,237,000	£1,650,00	£1,650,00
Orchestration & Automation	£143,000	£310,500	£324,000	£324,000	£324,000	£324,000
Cost Per Board	**£18955**	**£32841**	**£52227**	**£56242**	**£89727**	**£89727**

Tools

Tay Cyber Quarter Membership	£15000	£82,000	£82,000	£82,000	£82,000	£82,000
Access links and ancillary infrastructure	£50,000	£55,000	£55,000	£45,000	£45,000	£45,000
Board Integration	**£700,000**	**£700,000**	**£800,000**	-	-	-
Cost Per Board	**£34772.73**	**£38045.45**	**£42.950.91**	**£5772.73**	**£5772.73**	**£5772.73**

Build

Given the financial challenges faced by NHS Scotland in the coming years, exacerbated by the ongoing pandemic caused by Covid 19, the CCoE proposal offers the best value in delivering a consolidated cyber security service to all Boards.

The Centre will enhance existing capability within Health Boards providing significant equivalent financial value to each of them. A small cost element has been incorporated to assist in the integration of Boards with the Centre due to incompatibilities or requirements for tooling. These will be one-off costs and therefore are charged to the first three years of the programme. Microsoft Defender ATP and other elements of the Security & Compliance bundle are not included in the costs for the CCoE as these are pre-existing national initiatives.

Item	Six Year EVPB*	Total six year cost
Staff costs	314641	£6,922,102
SIEM Tool	273705	£6,021,500
Orchestration tools	79523	£1,749,500
Tay Cyber Quarter membership & accommodation	20455	£450,000
Access links and ancillary infrastructure	13409	£295,000
Board Integration	£100,000	£2,200,000
Total Costs	£801,733	**£17,638,102**

*Equivalent Value per Board: