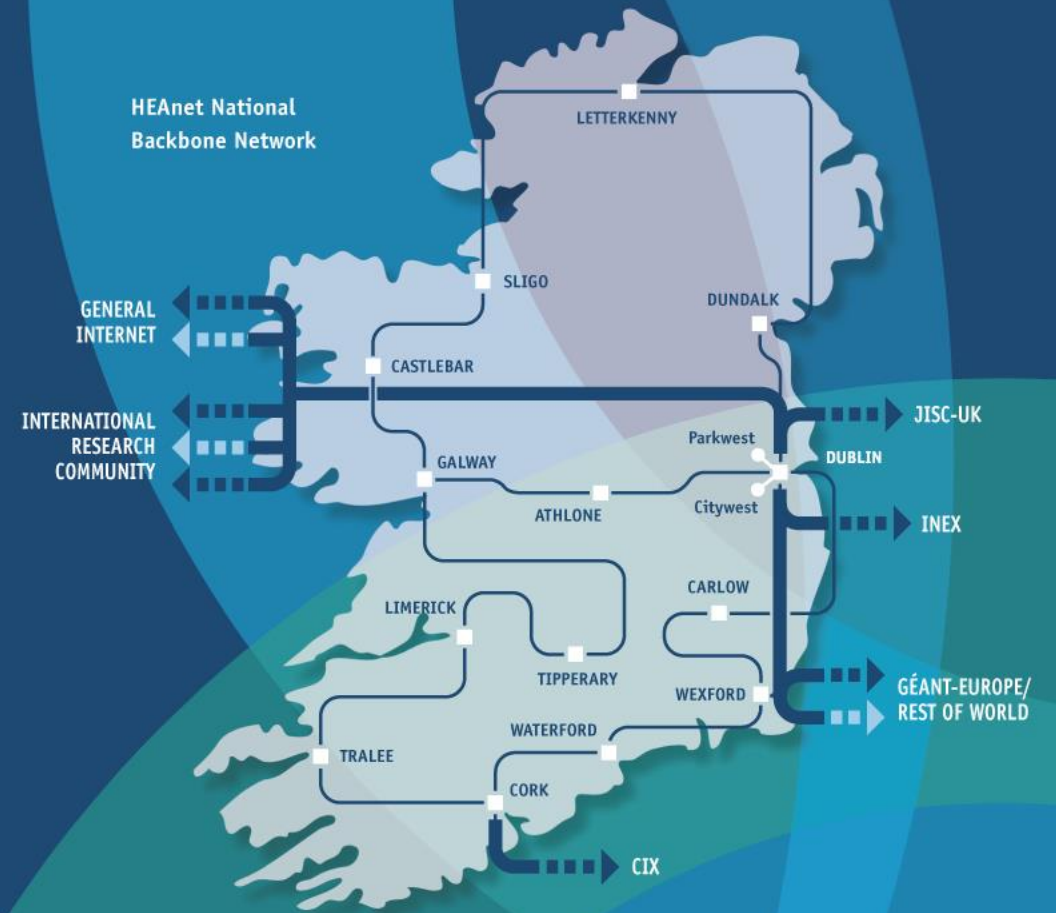


HEAnet Security Services

Louise O'Sullivan, Security Services Manager

Brian Nisbet, Service Operations Manager

Andy Byrne, Project Manager



A Poll for the Audience

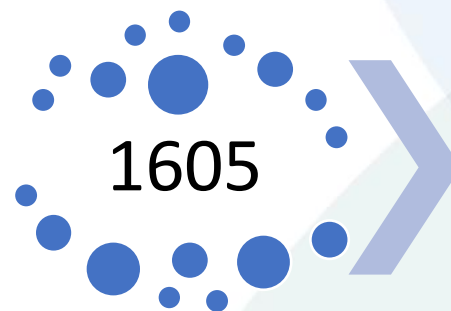
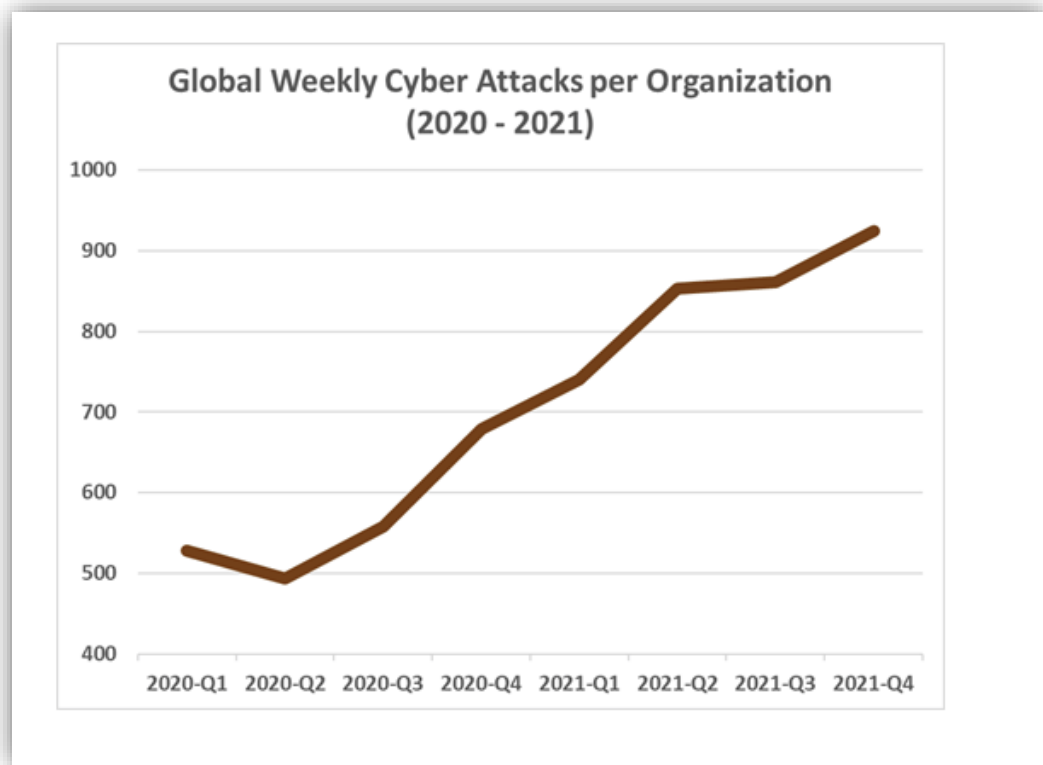


Website: <https://www.sli.do/>

Code: #HEAnet2022

Cyber Security Trends

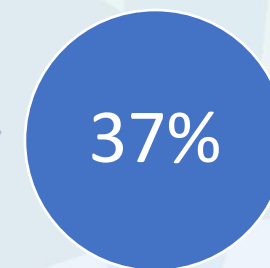
The Education sector has recently surpassed Healthcare and Government as the industry that suffers the most ransomware attacks.



Education and Research organisations hit by weekly cyberattacks.

600%

Cybercrime up 600% Due To COVID-19 Pandemic

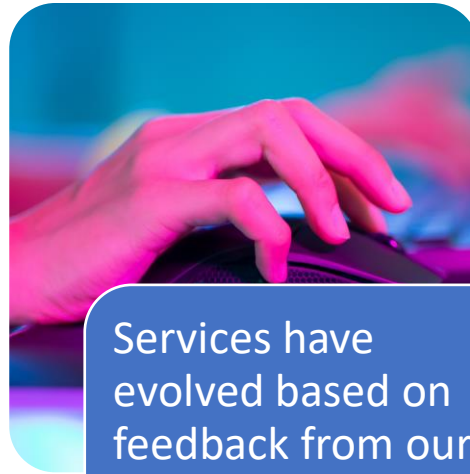


All businesses and organisations were hit by ransomware

ICT Security Services



Introduced in 2017
at our annual
conference



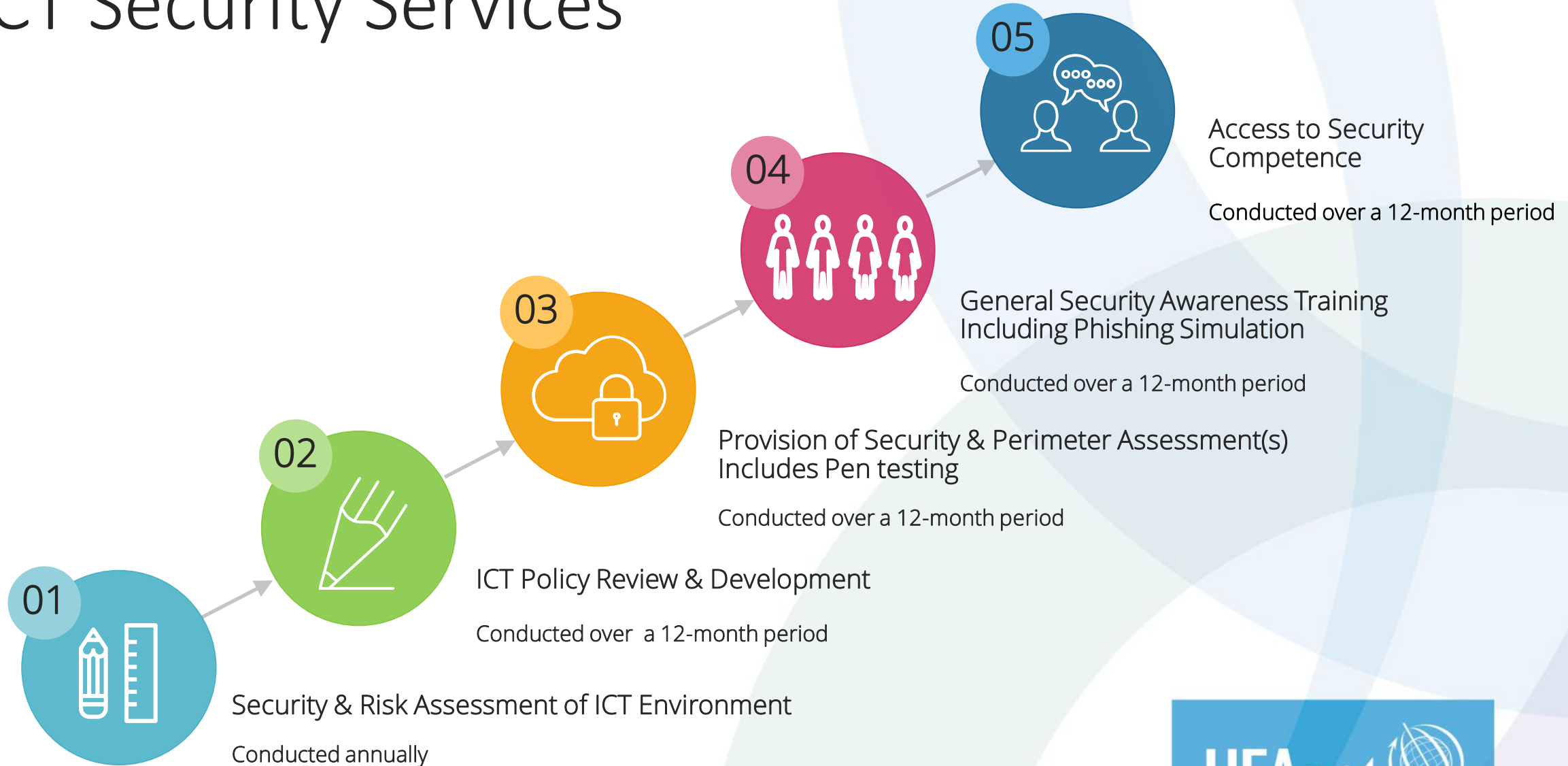
Services have
evolved based on
feedback from our
client

- Introduction of Phishing Simulation
- Pen Testing
- No. of training sessions

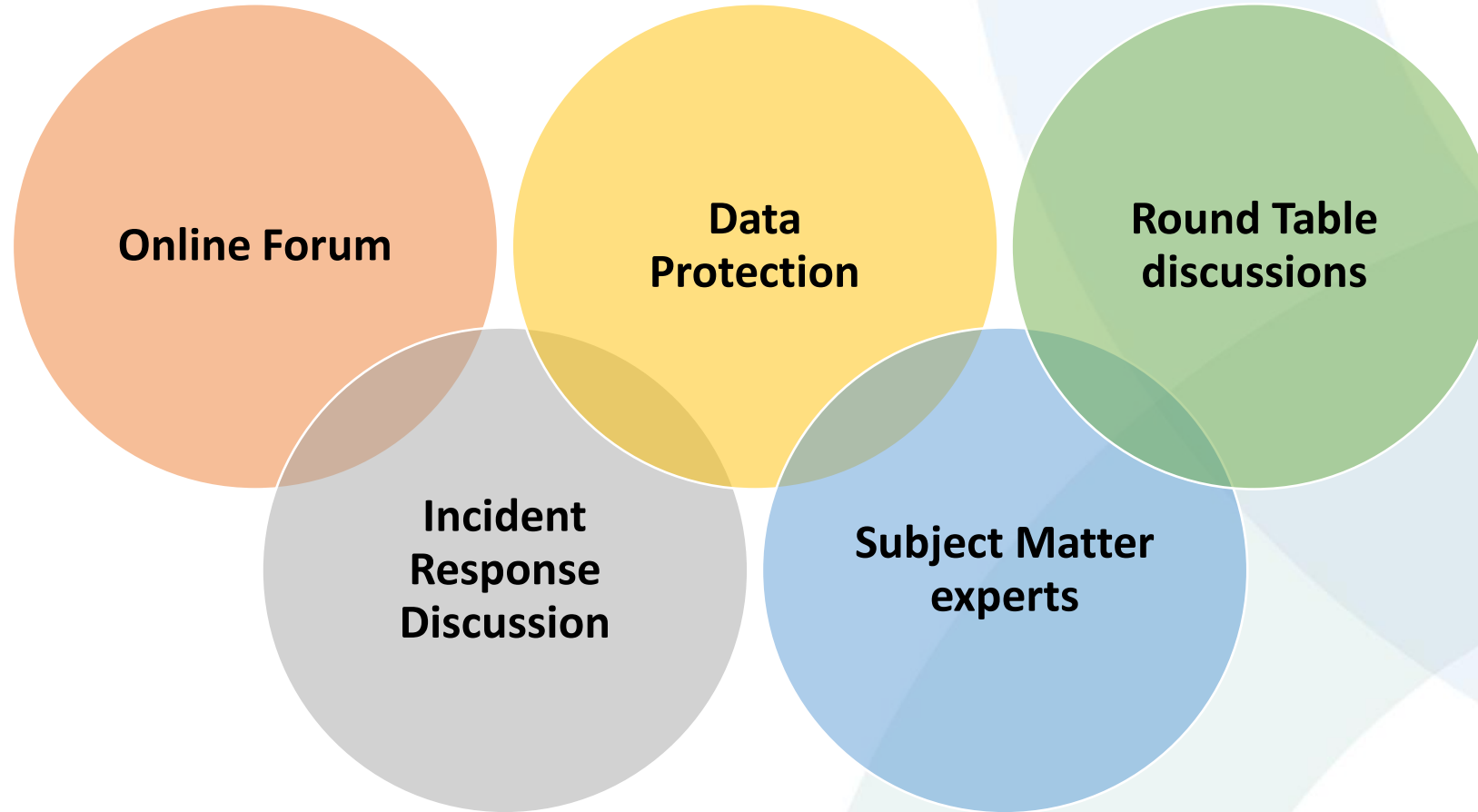


Team of highly
skilled individuals

ICT Security Services



Access to Security Competence



Key Pen Testing Trends

Broken access controls (privilege escalation)

Cryptographic Failures (sensitive data exposure)

Injection (SQLi, XSS)

Over permissive file upload (malicious file)

Cross- Site Request Forgery

Security Misconfiguration

Key Security and Perimeter trends

Cleartext Protocol in Use

Unsupported Operating Systems/Software

Outdated Services/Software with Known Vulnerabilities

SSL/TLS Related Vulnerabilities(SSLV2/3, TLS V1.0, Sweet 32, POODLE)

Information Leakage (Backup files, directory listing, Robots.txt file)

Over the past two years..

35

**Vulnerability
and Penetration
testing**

3000+

**Training session
attendees**

55

**Policies
reviewed /
created**

07

**Phishing
Campaigns**

04

**Ransomware
Mitigation
Workshops**

Brian Nisbet



HEAnet Emergency Contact

In the event of an emergency such as a Connectivity outage, DDoS attack, Security incident or any HEAnet service failure

Please contact

HEAnet

Ireland's National Education & Research Network



+353 1 660 9040

HEAnet Service Desk:

09:00 - 17:30 Monday to Friday
(except public holidays)

Out-of-hours 24/7 Support:

Ask for the on-call engineer



noc@heanet.ie

Andy Byrne

A Poll for the Audience



Website: <https://www.sli.do/>

Code: #HEAnet2022

SOC & SIEM Discovery Project

SOC – Security Operation Centre

SIEM – Security Information and Event Management.



Current Challenges



SOC & SIEM Model



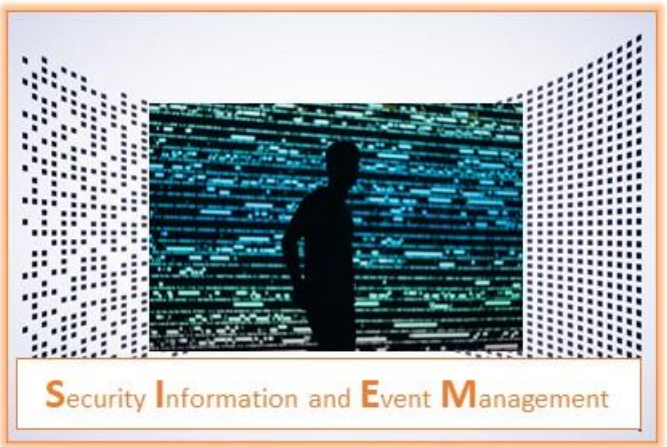
LOG Sources



Clients



Security Operations Centre



Security Information and Event Management

Why are we doing this ?



Shared Service



Cyber Insurance / Compliancy



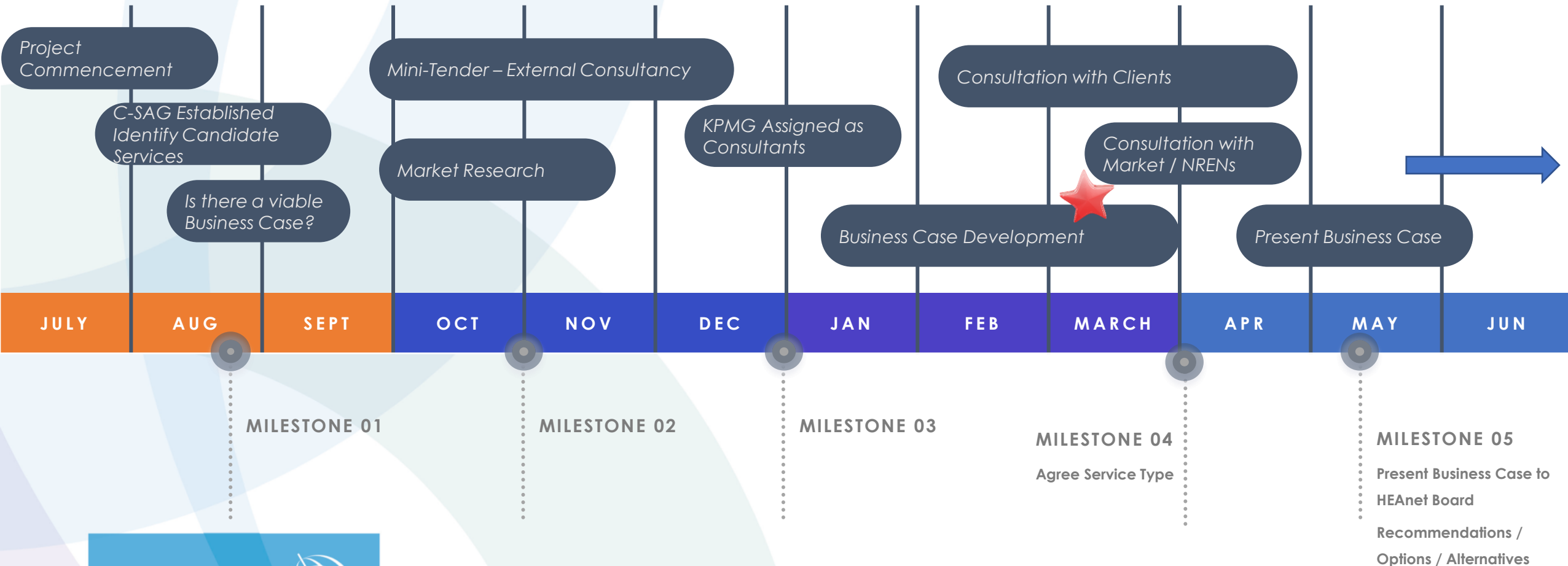
Security Analysts

Major Milestones of Project

- Client Consultation / Shortlisting
- Business Plan – Feasibility Study
- Board Approval
- Funding
- Procurement
- Deployment

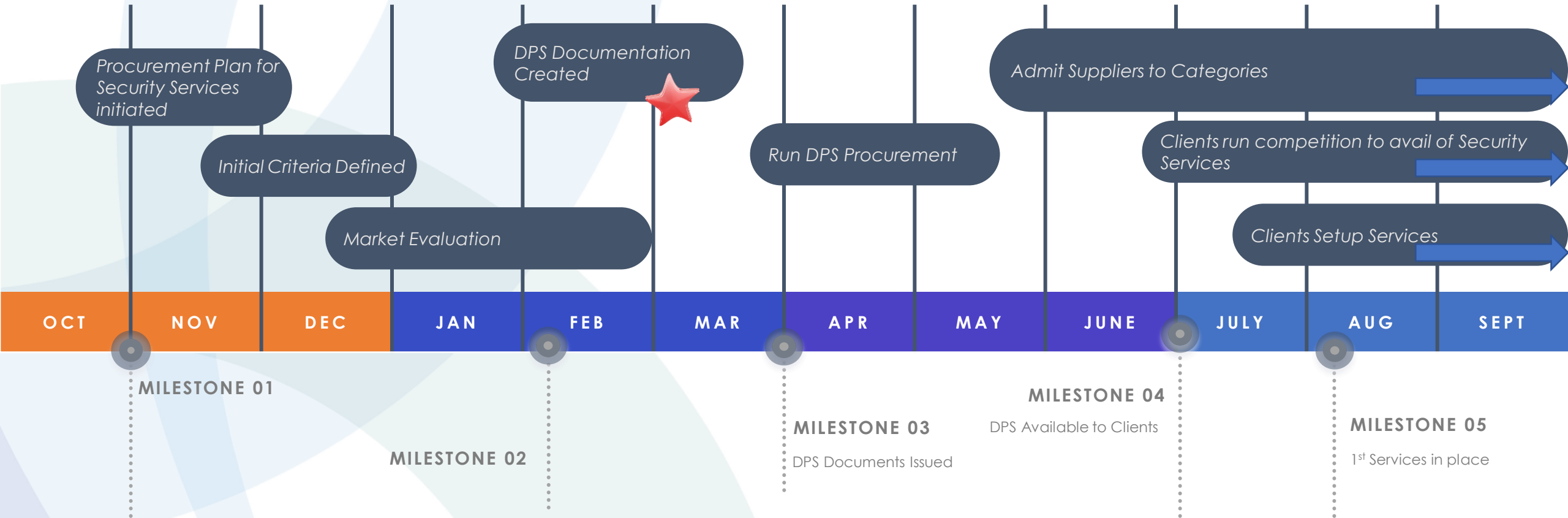


Managed SOC & SIEM Discovery Phase Business Case



Managed SOC & SIEM Discovery Phase

Dynamic Purchasing System (DPS)



What have we learned so far

Not many centralised public plans

High Cost Item

Smart option is to outsource service

Common & Overlapping Threats

Many clients running PoCs

Benefits of shared service through HEAnet; Jisc, SURF

SOC & SIEM Client Survey Results

- 57 Respondents
 - **68% of Clients have no SOC & SIEM**
 - **62%** have identified the main business drivers for a SOC service
 - **66% likely to avail of a Centralised SOC/SIEM**
 - **44%** want fully outsourced, **40%** want hybrid
 - **20%** want Re-active SOC, **60%** want Pro-active SOC
- **70%** of clients host on Public Cloud
- **95%** of clients use SaaS (O365)
- **70%** of clients use Endpoint Protection (MS Defender)

Summary

- Valued Centralised Service
- The need for this solution is growing
- Reduce Time, Cost & Risk



A Poll for the Audience



Website: <https://www.sli.do/>

Code: #HEAnet2022

Thank You

Louise O'Sullivan, Security Services Manager

Brian Nisbet, Service Operations Manager

Andy Byrne, Project Manager

