The SOC and the NOC at JISC

Mark Worthington

Dave Neller


Jisc
Dave Neller
Head of Network Engineering


Jisc
Mark Worthington
Security centre operations manager

The Jisc NOC Teams

Jisc Service Desk (JSD)	Network Engineering Group (NEG)	Core Architecture Team (CAT)
• 1st Line – NMS • Services • Upskilling • Major Incidents • Operations Contacts • Contact Centre • 24/7/365	• 2nd Line • Managed Router Service • Access to Core/Infrastructure • Customer Facing • 24/7/365 - On-call • Product/Service development • Field and Operations	• 3rd Line • Infrastructure and Core network • Capacity planning and provision • Project lead • 24/7/365 - On-call • Network Design • Dedicated Optical Team

CSIRT *was…*

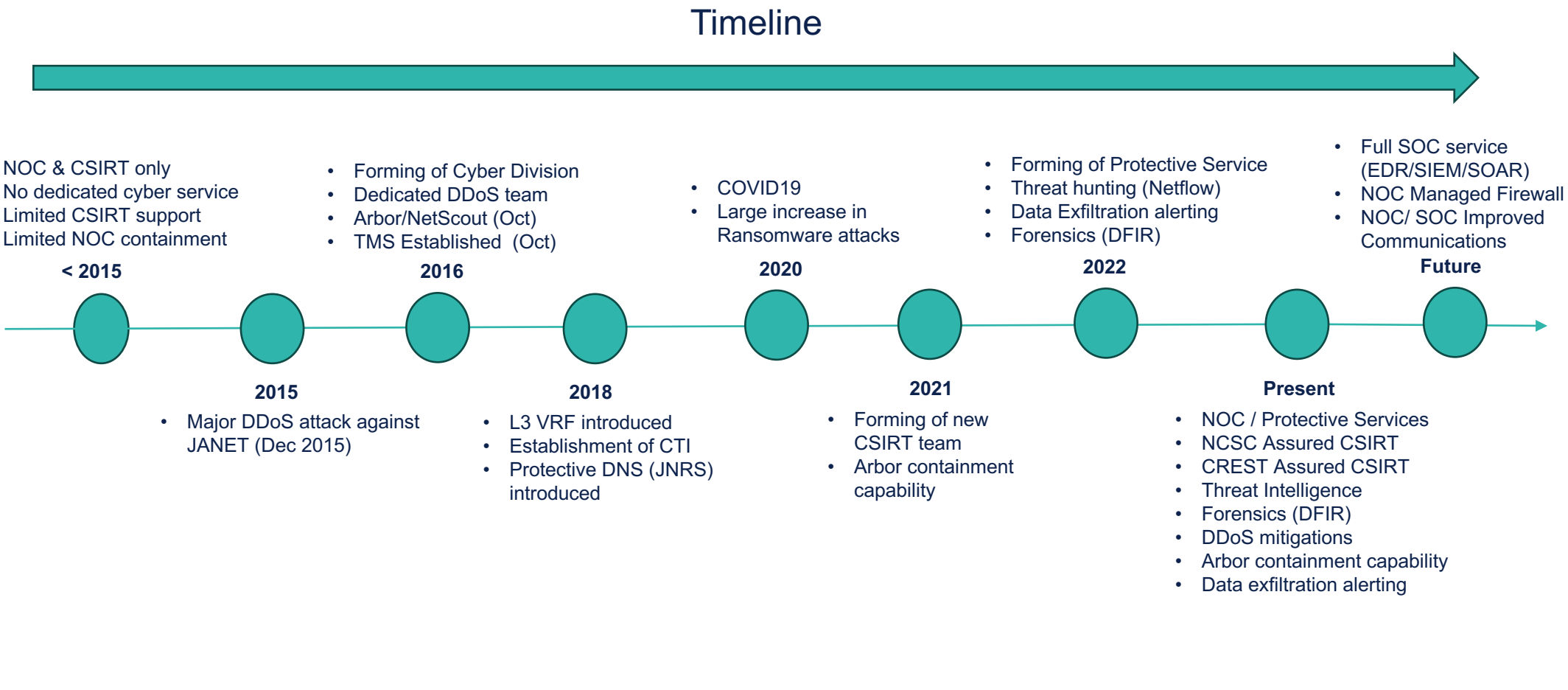
Incident Response (CSIRT)	Network Engineering Group (NEG)

• Incident response (advice & guidance only)
• Limited netflow alerting capability
  • Primarily open source driven
  • DDoS detections
  • Scanning activity
• Limited host forensic capability
	• DDoS mitigations via MRS

Where we were (Whac-A-Mole)

- NOC and CSIRT
- Netflow exports from core
- Reactive response to live incidents
- Blocks placed manually by NOC on a-end or MRS
  Only involved with Janet side, up to firewall demarc
- Working as separate teams

Jisc NOC/SOC Capability Timeline



Where we are

- NOC / SOC / CSIRT
- Netflow exports from core
- Working between teams for capacity planning and projects
- Shared access to data

The Jisc SOC Teams

Incident Response (CSIRT)	Cyber Threat Intelligence (CTI)	Defensive Services (DS)	Digital Forensics (DFIR)	Cyber Security Threat Monitoring (CSTM)
• Incident Management • Containment, eradication, and recovery support • EDR/XDR deployment (CrowdStrike) • Security hardening workshops (AD, M365, Azure, AWS)	• Analyse the current & emerging threat landscape • Exploit and Threat Monitoring • Threat Actor Profiling • Threat Intelligence sharing	• DDoS monitoring and mitigation • Network monitoring for all Janet connected organisations • Host and Network containment	• Identification of IOCs, TTPs & incident scope to support IR • Root Cause Analysis • Compromise Assessment • Incident reporting	• Threat Detection based on SIEM Use Cases • MITRE ATT&CK® aligned • 24/7 alerting

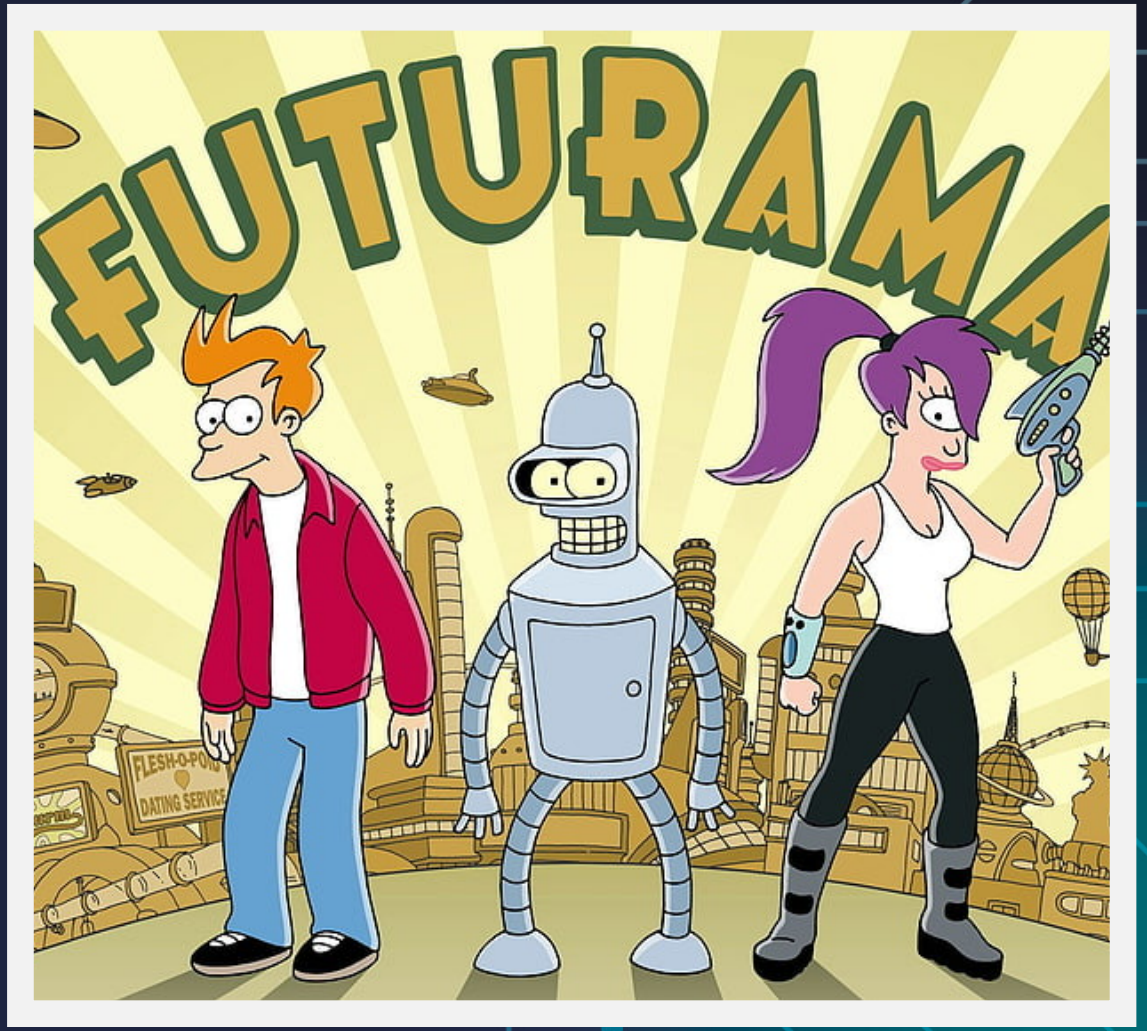
NCSC Cyber Incident Response Level 2 Accredited

CREST Cyber Incident Response Accredited

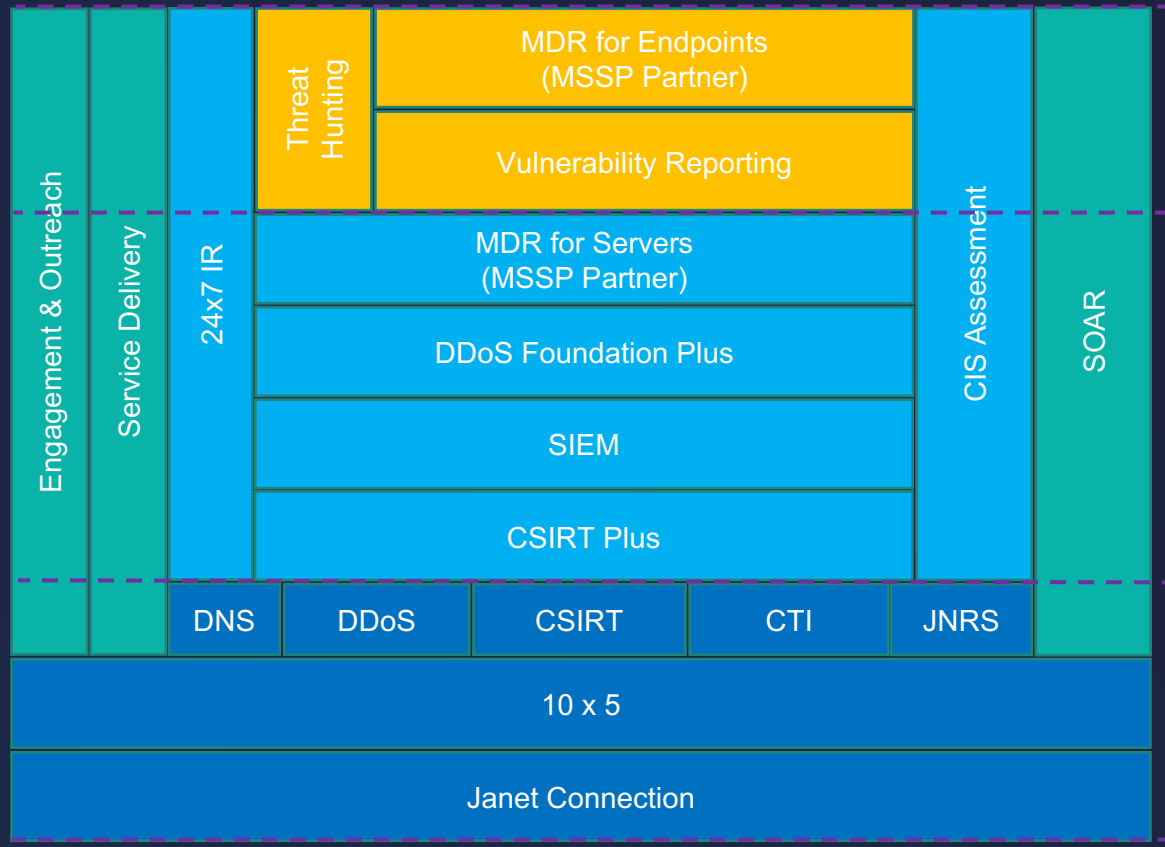
Advice, Guidance and Communities (Cyber Community)

Where we are going (The World of Tomorrow)

- NOC / SOC / CSIRT
- NOC Managed Firewall
- Better communication between teams in general
- Better / shared visibility of active mitigations



Security Centre (SOC)



SOC Tier 2

SOC - Tier 2
- Tier 2 + Tier 1 + Membership
- Organisational Threat Hunting
- Internal & External Vulnerability Reporting

SOC Tier 1

SOC - Tier 1
- Tier 1 + Membership
- CSIRT on call Containment 24x7 2-hour response
- Cloud based SIEM (CSTM)
- EDR/XDR (Servers) Manage, Detect and Respond
- Round the clock protection against DDoS attacks
- Annual CIS Health check (3 days)

Membership

In Membership
- CSIRT - 10 x 5 4-hour response SLA
- Foundation DDoS mitigation service
- CTI - Cyber Threat Intelligence
- Primary/Secondary Name Service
- Major incident support
  - Including CTI and Foundation Forensics
  - EDR support max 30 days

Professional Services

CSP etc…

splunk> Enterprise Security

Microsoft Defender

CROWDSTRIKE

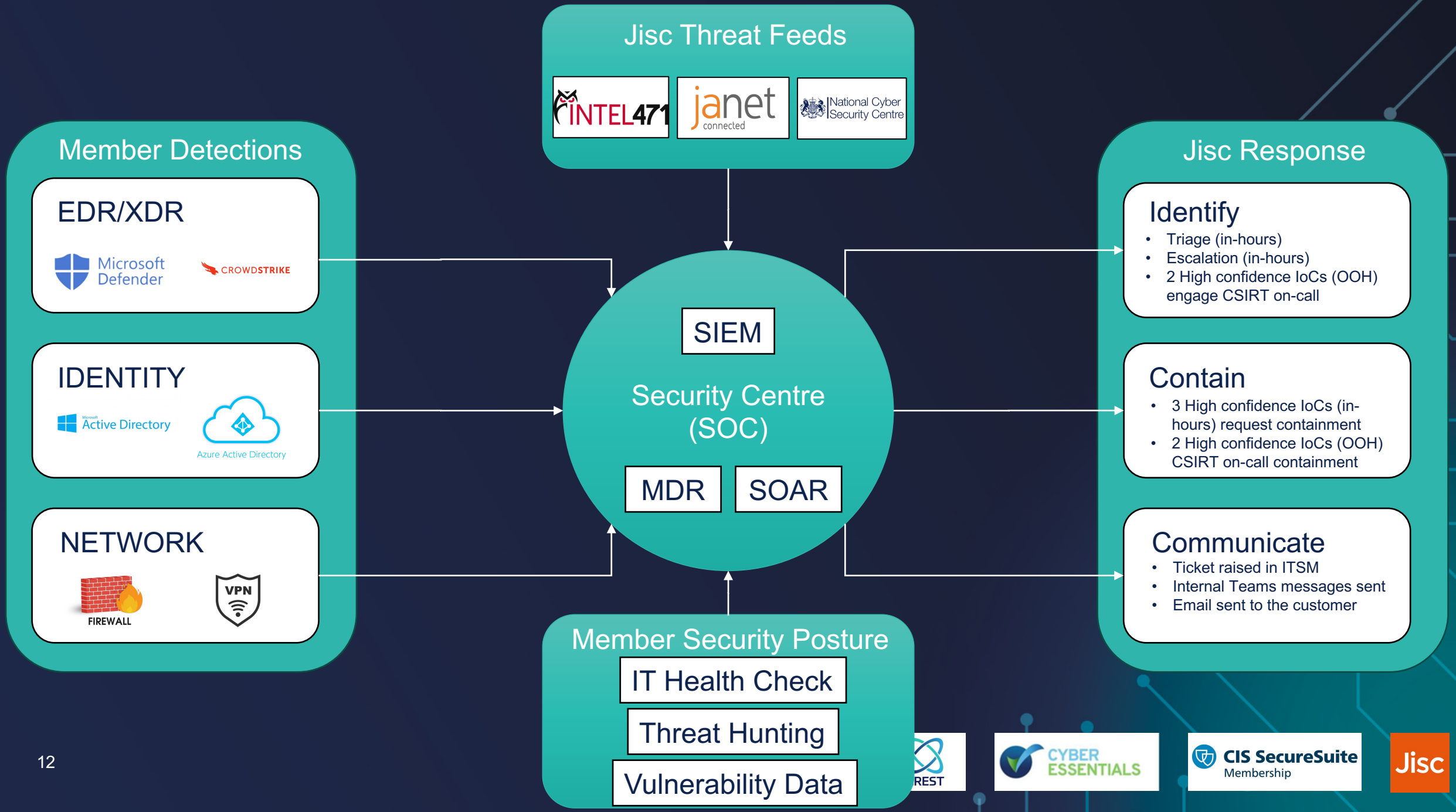
Assured Service Provider in association with National Cyber Security Centre Cyber Incident Response (Level 2)

CREST

CYBER ESSENTIALS

CIS SecureSuite Membership

Jisc


Jisc Threat Feeds
INTEL471
janet connected
National Cyber Security Centre
Member Detections
EDR/XDR
Microsoft Defender
CROWDSTRIKE
IDENTITY
Active Directory
Azure Active Directory
NETWORK
FIREWALL
VPN
SIEM
Security Centre (SOC)
MDR
SOAR
Jisc Response
Identify
Triage (in-hours)
Escalation (in-hours)
2 High confidence IoCs (OOH) engage CSIRT on-call
Contain
3 High confidence IoCs (in-hours) request containment
2 High confidence IoCs (OOH) CSIRT on-call containment
Communicate
Ticket raised in ITSM
Internal Teams messages sent
Email sent to the customer
Member Security Posture
IT Health Check
Threat Hunting
Vulnerability Data

Questions?

Thank you

Mark Worthington
SOC manager
mark.worthington@jisc.ac.uk

Dave Neller
Head of Network Engineering
david.neller@jisc.ac.uk

Janet NOC
0300 300 2212

irt@jisc.ac.uk
jisc.ac.uk/cyber-security

operations@ja.net
jisc.ac.uk/janet

Assured Service Provider
in association with National Cyber Security Centre
Cyber Incident Response (Level 2)

CREST

CYBER ESSENTIALS

CIS SecureSuite Membership

Jisc