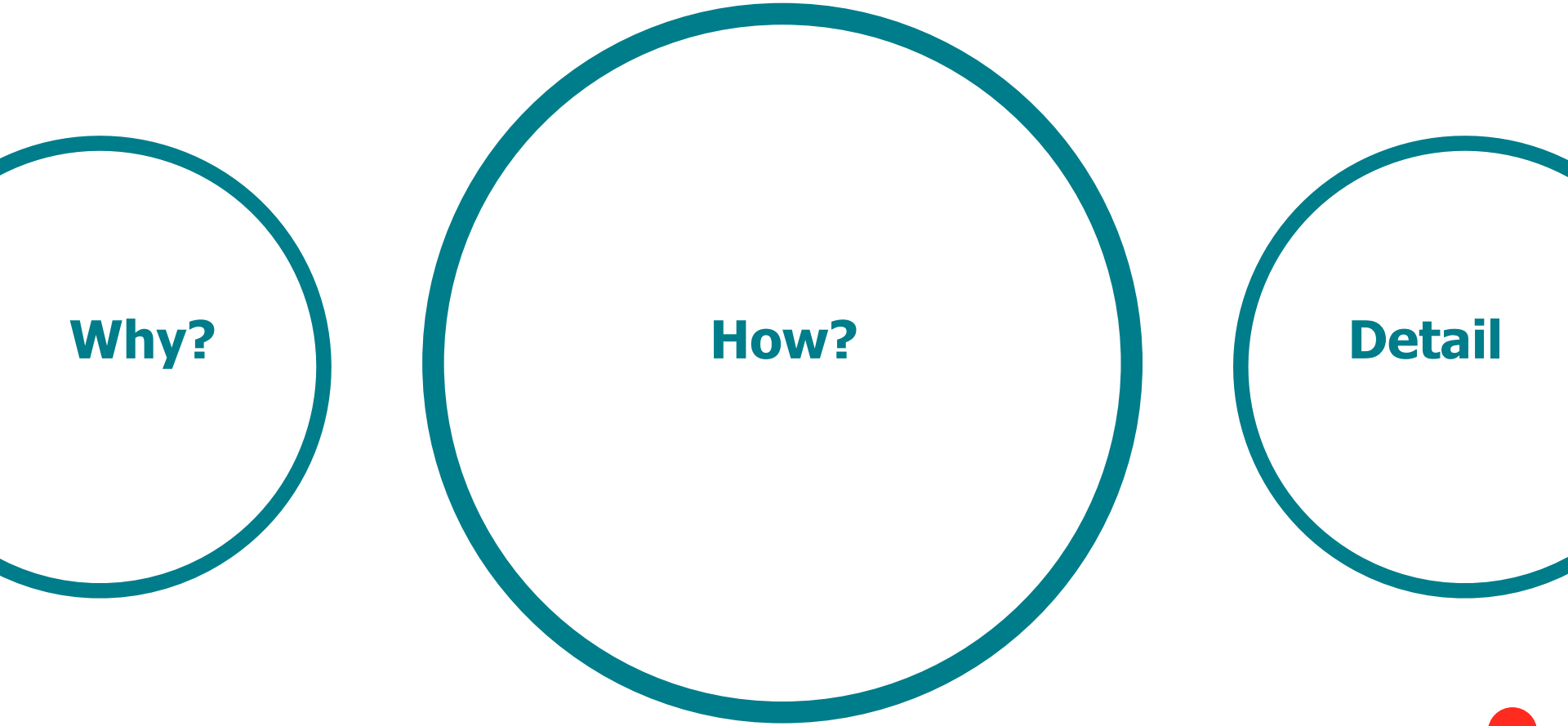
Safely Assessing Operational Technology (OT) Environments

Nick Hayes, Global Head of Technical Direction

CrestCon 2019



Today’s Learning

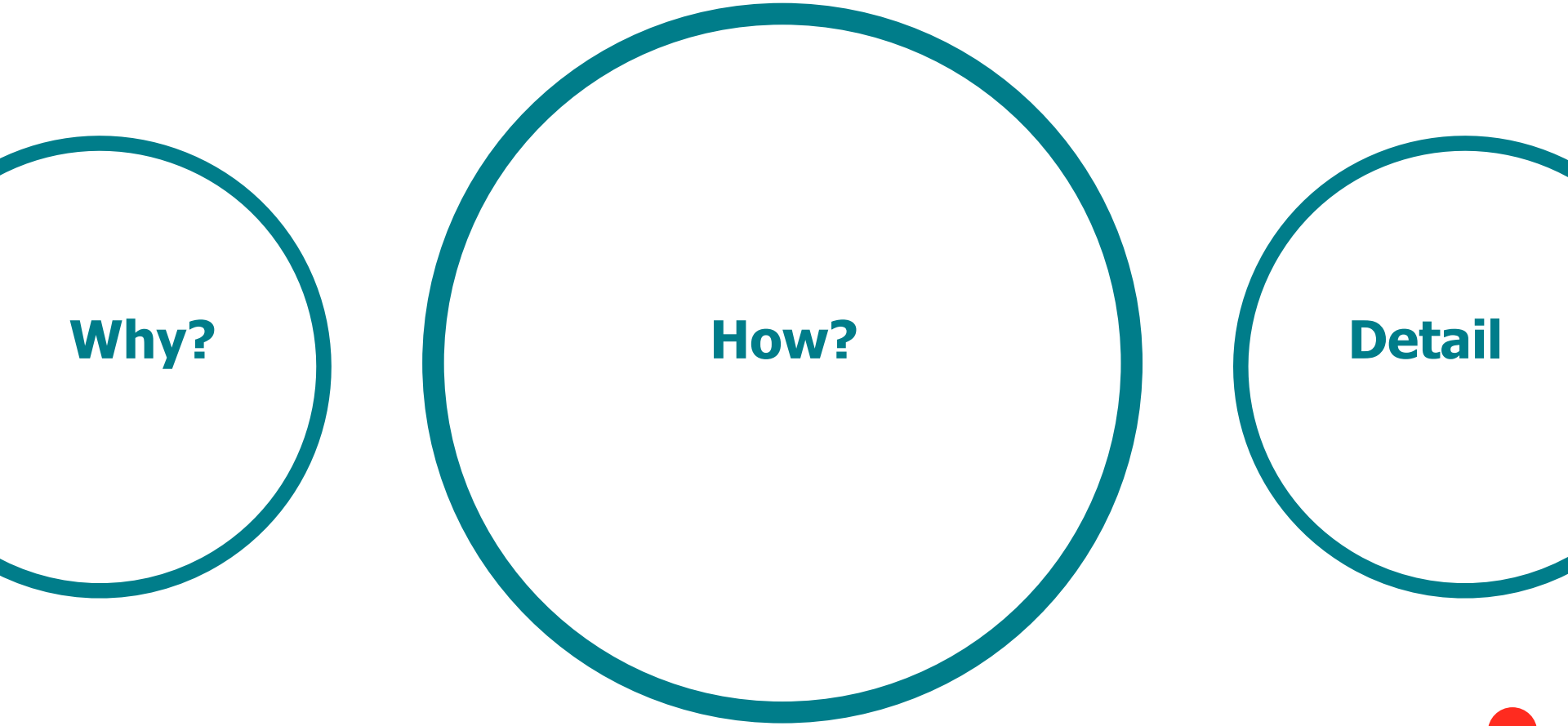
- Assessing OT environments is important
- Successful pwnage of OT systems can have a big impact
- Safety and availability are key in OT
- How might we approach OT assessments to maintain safety and availability of systems?

bsi.

$ whoami

- Current Global Head of Technical Direction at BSI Cybersecurity and Information Resilience
- 7 years+ of pentest experience, always with an eye on SCADA / OT
- Delivered large numbers of pentesting and governance work on SCADA / OT
- Owner of SCADA service line at previous consultancies
- Ex-SCADA design engineer before moving into infosec
- Know a fair bit about SCADA / OT

bsi.



Why?

Triton is the world's most murderous malware, and it's spreading

ode can disable safety systems designed to
phic industrial accidents. It was
Middle East, but the hackers behind it
mpanies in North America and
world, too.

bsi.

OT Security Landscape - 2019

- In 2019 the OT security landscape is still broken
- Many OT environments have not been designed with security in mind
- New directives introduced recently - NIS
- Further convergence of OT and IT
- Increased complexity and connectivity

bsi.

Priorities

IT	OT
Confidentiality	Safety
Integrity	Availability
Availability	Integrity
	Confidentiality

bsi.

Safety is Number One Priority

Safety is Number One Priority

Availability is Number Two Priority

Safety is Number One Priority

Availability is Number Two Priority

Where are confidentiality and integrity?

Assessing OT

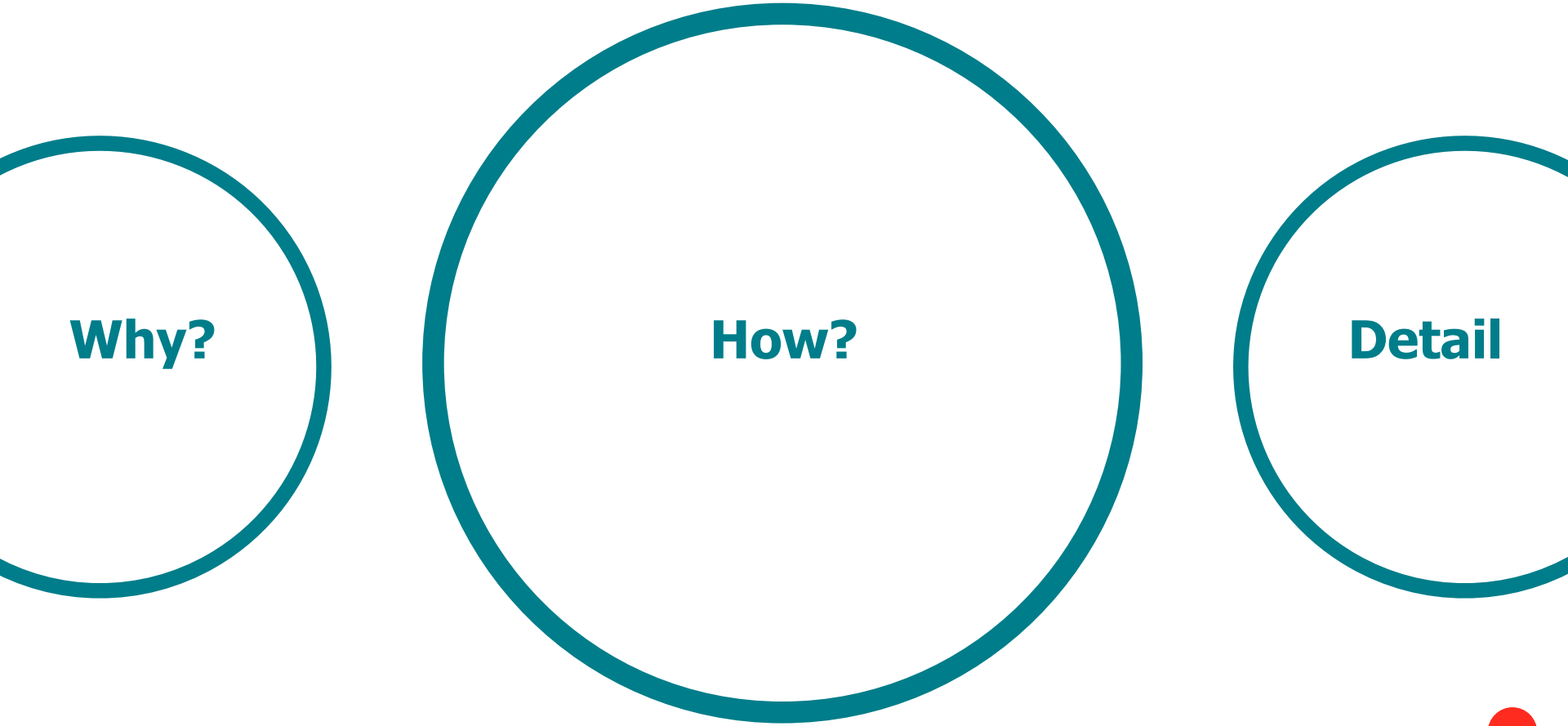
- The impact of a compromise can be huge
- So we must identify the real-world risk of that happening
- Technical testing is one way, but it has its problems...

bsi.

Offensive Testing Risks

1. Risky by nature – makes buy-in for active testing difficult
2. Safety and availability must be maintained
3. Testing environments rarely exist and usually are not representative
4. NIS Directives mean OT systems cannot be ignored

bsi.



Develop a robust and bespoke hybrid approach to assessing OT systems

Approach

Governance

- NIS Directive
- BSI OT Risk Assessment Framework

Testing

- Test Environment / Test Bed
- Testing with familiar techniques
- Controlled Production Testing

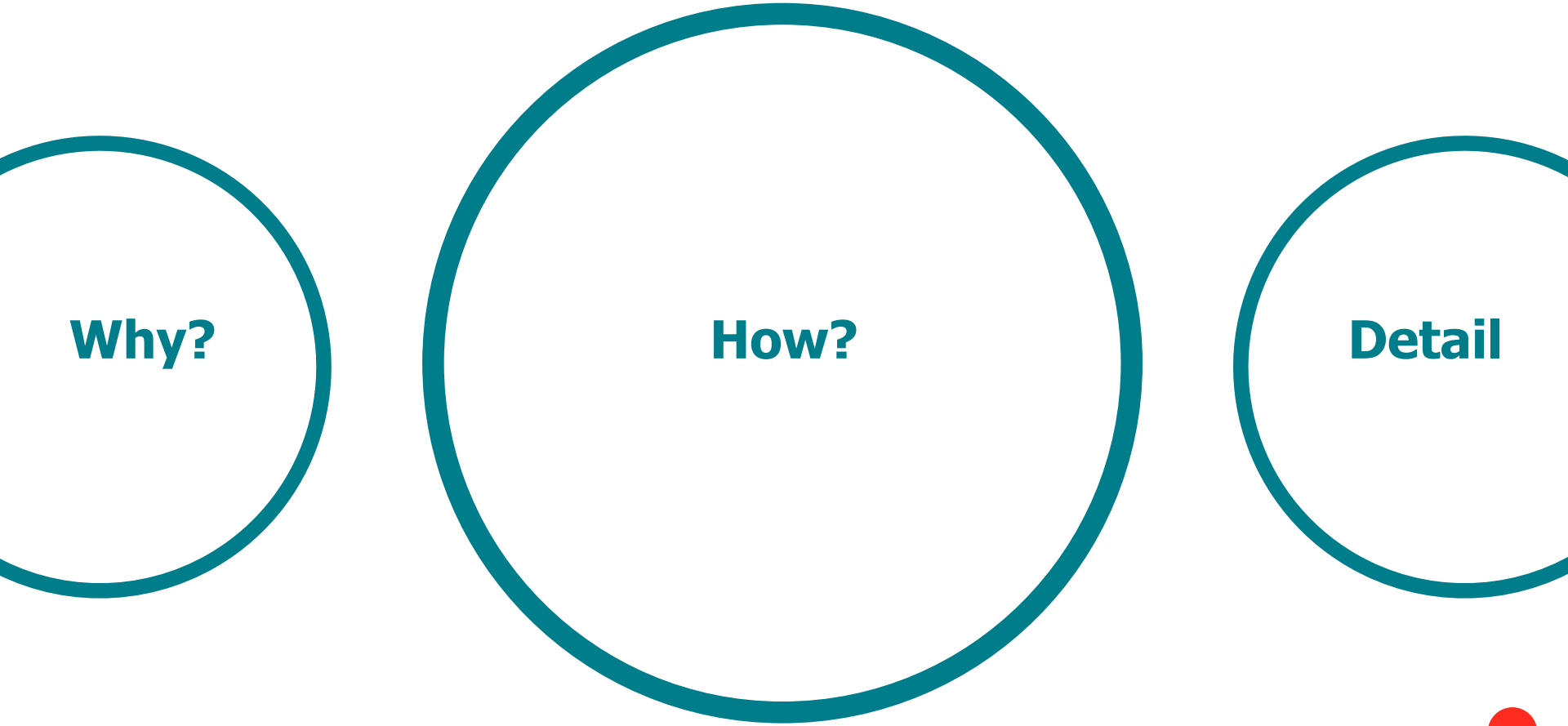
Approach

Governance

- NIS Directive
- BSI OT Risk Assessment Framework

Testing

- Test Environment / Test Bed
- Testing with familiar techniques
- Controlled Production Testing



NIS Directive

Important for Operators of Essential Services – Utilities, Telco etc

Objective A:
Managing security risk

Objective B:
Protecting against cyber attack

Objective C:
Detecting cyber security events

Objective D:
Minimising the impact of cyber security incidents

BSI OT Risk Management Framework

- Bespoke OT Risk Management Framework development and assessment for the OT environment. Calling on existing frameworks and guidelines:
  - Uses IEC62443/ISA99 principles, NIST 800-82 guideline and ISO 27001 framework
  - Very low risk approach
  - Holistic high level view of the wider OT environment
  - Emphasis on security being a continual process based on simple controls

BSI OT Risk Management Framework

- IEC62443 / ISA99 Principles
  - Aim to improve safety, availability, integrity and confidentiality of components or systems used in OT / SCADA
  - Full version provides defined security levels
  - We use the “zones” and “conduits” principles to break up the OT
  - Risk assess against the zones and conduits
  - Grouped risk treatment

BSI OT Risk Management Framework

- NIST 800-82:
  - Guideline document
  - How to secure ICS and SCADA systems
  - Very in-depth
  - We use it to provide detail around what a good environment looks like

BSI OT Risk Management Framework

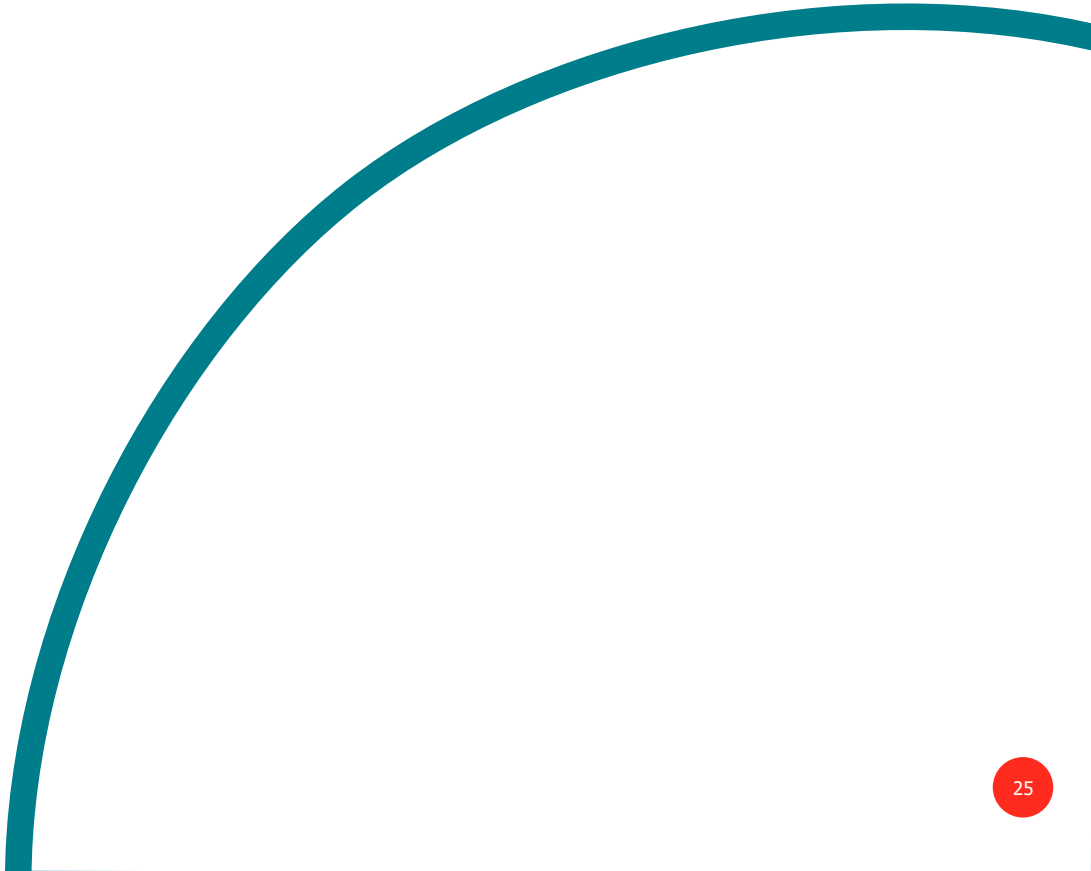
- ISO 27001 Standard
  - Originally a BSI standard before being used by ISO
  - We all know this standard, is widely accepted as a good, thorough standard for **IT** and gives a good **measurable benchmark**
  - It does contain a lot of useful controls relevant to OT
  - Used in the OT Risk Management Framework with irrelevant sections removed and new domains created
  - In-depth physical security is a key area which we have added

BSI OT Risk Management Framework

Intended Outcome

- Holistic assessment
- Highlights key risk areas
- Encompassing many domains of the environment
- Outwards-in – assessing the layers
- Combines with NIS directive

Case Study



Energy Provider – OT Risk Assessment

- Challenge around baselining and focussing future efforts in security
- Task:
  - Develop bespoke OT Risk Management Framework
  - Assess against the framework and tie into NIS
  - Provide analysis on findings and NIS compliance overview
- Helping to shape the future direction of OT security

Approach

Governance

- NIS Directive
- BSI OT Risk Assessment Framework

Testing

- Test Environment / Test Bed
- Testing with familiar techniques
- Controlled Production Testing

Test Environment / Test Bed

- Safest way to performing testing
- Not connected to production systems
- Often as systems are built and in FAT / SAT
- Allows us to do “dangerous” testing:
  - Fuzzing
  - Buffer overflows
  - Vulnerability hunting
  - Bounds testing

Testing with Familiar Techniques

- Report by Dragos[1] – 443 CVE's – only 34% covered industrial-specific protocols
- Many threat actors and ICS malware utilise "live-off-the-land" techniques
- OT environments can often look very familiar to us
- OT testing is not scary in itself, the impact of doing it wrong can be
- Fall back to what we know and test within the zones and the conduits

bsi.

[1] - https://dragos.com/wp-content/uploads/yir-ics-vulnerabilities-2018.pdf

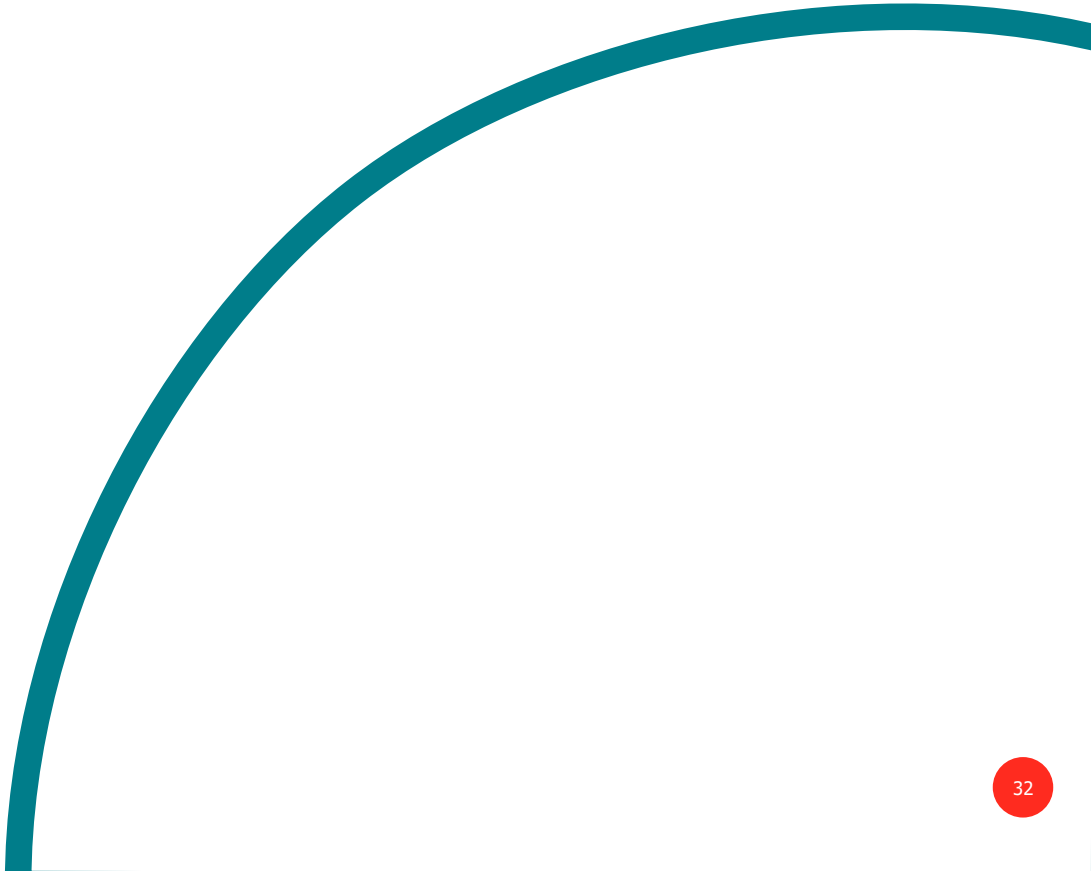
Controlled Production Testing

- Not for everyone!
- Quite risky in nature, but we can manage it:
  - Test non-critical processes
  - Implement additional safety measures
  - Test with a process engineer who knows the environment and can react
  - An appreciation for the whole process is key

Further Steps?

- Attack Simulation is achievable on OT
  - Needs significant buy-in and planning
  - Allows for testing of defensive capabilities

Case Study



Gas Operator - Pentesting

- Challenge was to identify the impact of a compromise on the SCADA network
- Task:
  - Pentest the SCADA / OT production system
  - OT system was segregated from IT but did allow some traffic
  - Pentested from control network perspective (simulated an attacker gaining a foothold – phishing, via corporate network, physical implant
  - Segregation controls between zones in the OT were strong
  - Visited sample sites to perform localised tests to simulate an adversary gaining physical access to a site – segregation and testing devices
  - Pwned the domain and then pwned the control system via that means – numerous issues

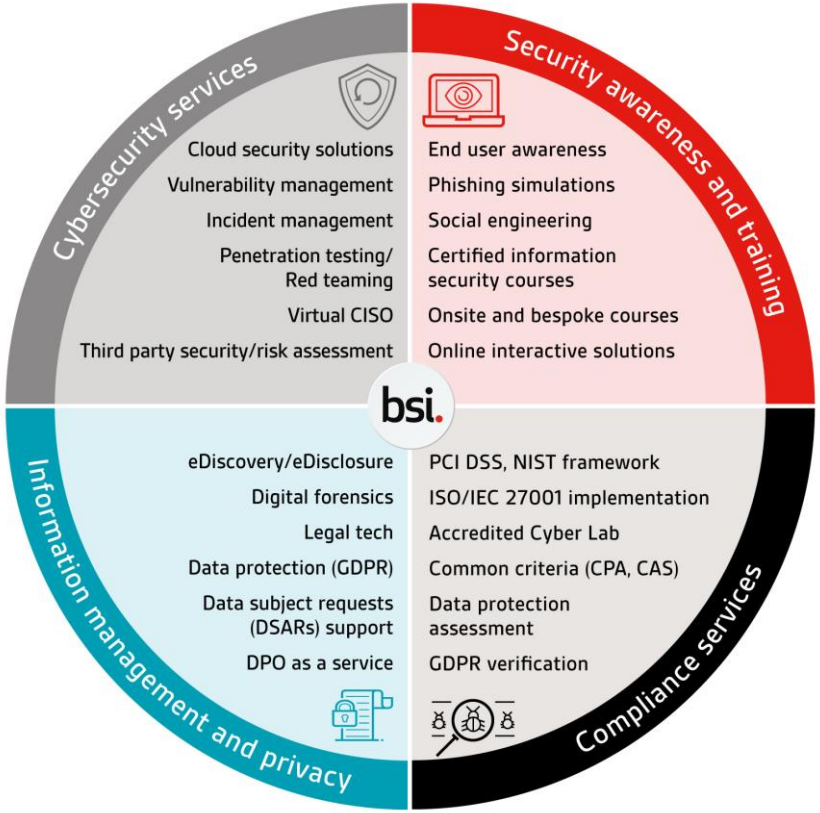
bsi.

Further Information

- More details and in-depth information can be found on our website:

https://www.bsigroup.com/en-GB/our-services/Cybersecurity-Information-Resilience/Resources/Whitepapers/ICS-Cybersecurity-Assessment-Framework/

BSI CSIR


Cybersecurity services
Cloud security solutions
Vulnerability management
Incident management
Penetration testing/ Red teaming
Virtual CISO
Third party security/risk assessment
Security awareness and training
End user awareness
Phishing simulations
Social engineering
Certified information security courses
Onsite and bespoke courses
Online interactive solutions
bsi.
Information management and privacy
eDiscovery/eDisclosure
Digital forensics
Legal tech
Data protection (GDPR)
Data subject requests (DSARs) support
DPO as a service
Compliance services
PCI DSS, NIST framework
ISO/IEC 27001 implementation
Accredited Cyber Lab
Common criteria (CPA, CAS)
Data protection assessment
GDPR verification

bsi.

For more information

Contact	UK	Ireland & International	Italy	The Netherlands
	+44 345 080 9000	+353 1 210 1711	+39 02 66 79 091	+31 20 346 0780
	bsigroup.com/cyber-uk	bsigroup.com/cyber-ie	bsigroup.com/it-it	bsigroup.com/nl-nl
	cyber@bsigroup.com	cyber.ie@bsigroup.com	cyber.ie@bsigroup.com	cyber.ie@bsigroup.com

Q&A


Thank you!