dull.

SANS Institute Five Critical Controls

Spotlight on Secure Remote Access

Tim Jackson - Head of Solutions Engineering, **Dull**

IT vs OT Security

Different Networks and Systems

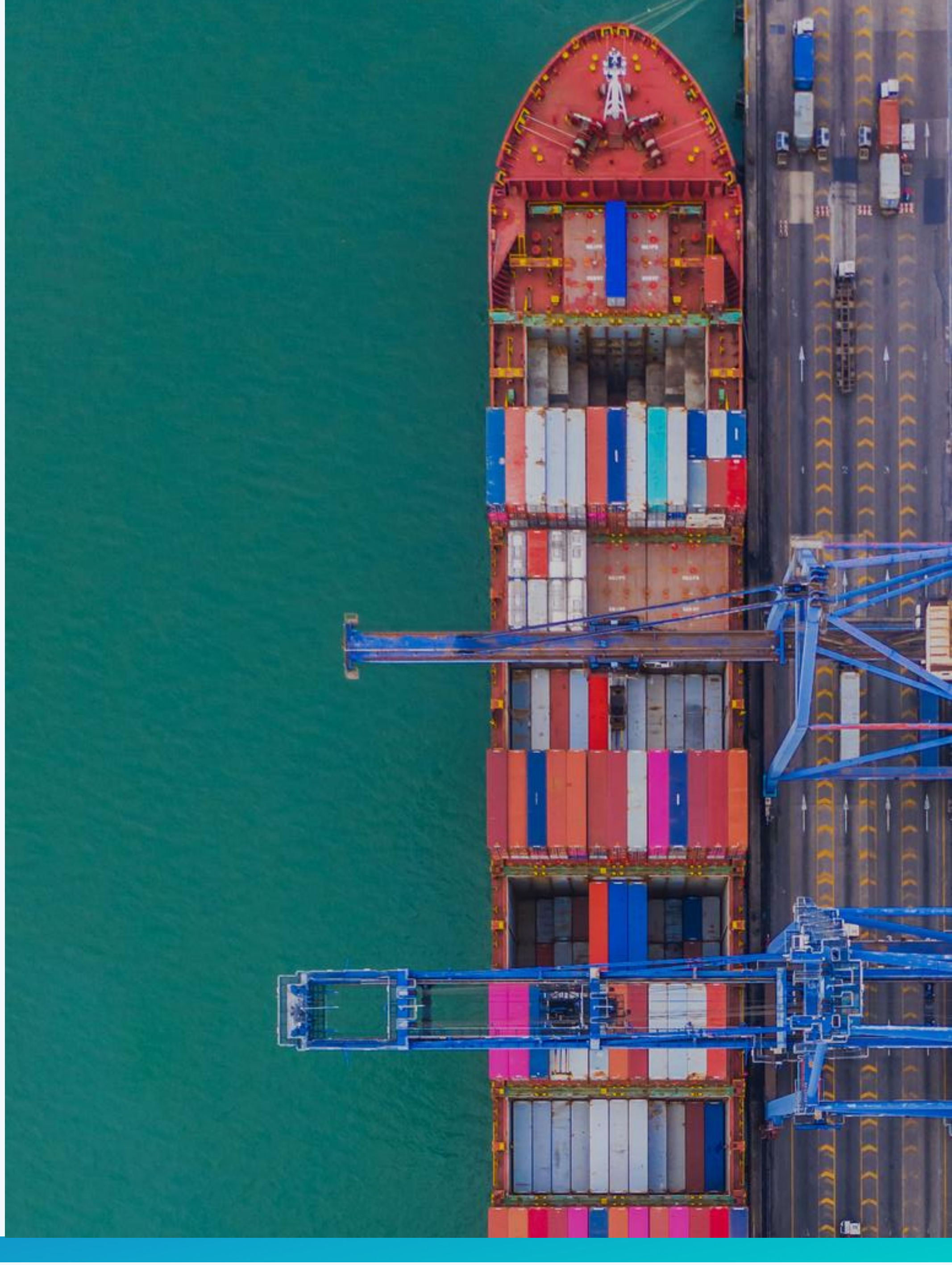
Understanding the assets that need to be protected

Specialised Threat Actors

Sub-dividing networks into isolated zones based upon risk level

Physical Safety Consequences

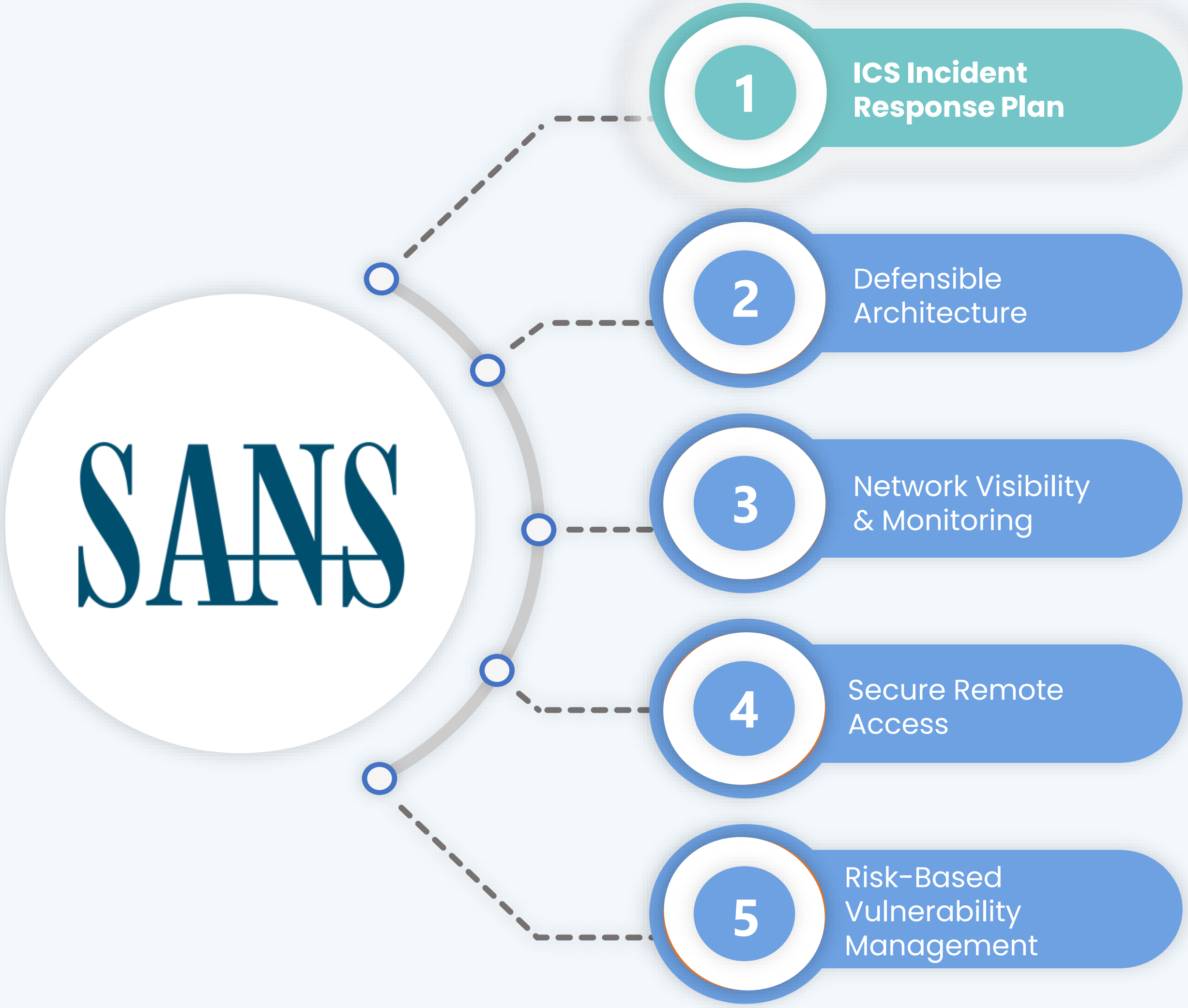
Using IEC 62443 and NIST 800-82 as guiding standards



dull.

SANS Institute ICS Five Critical Controls

SANS Five ICS Critical Security Controls

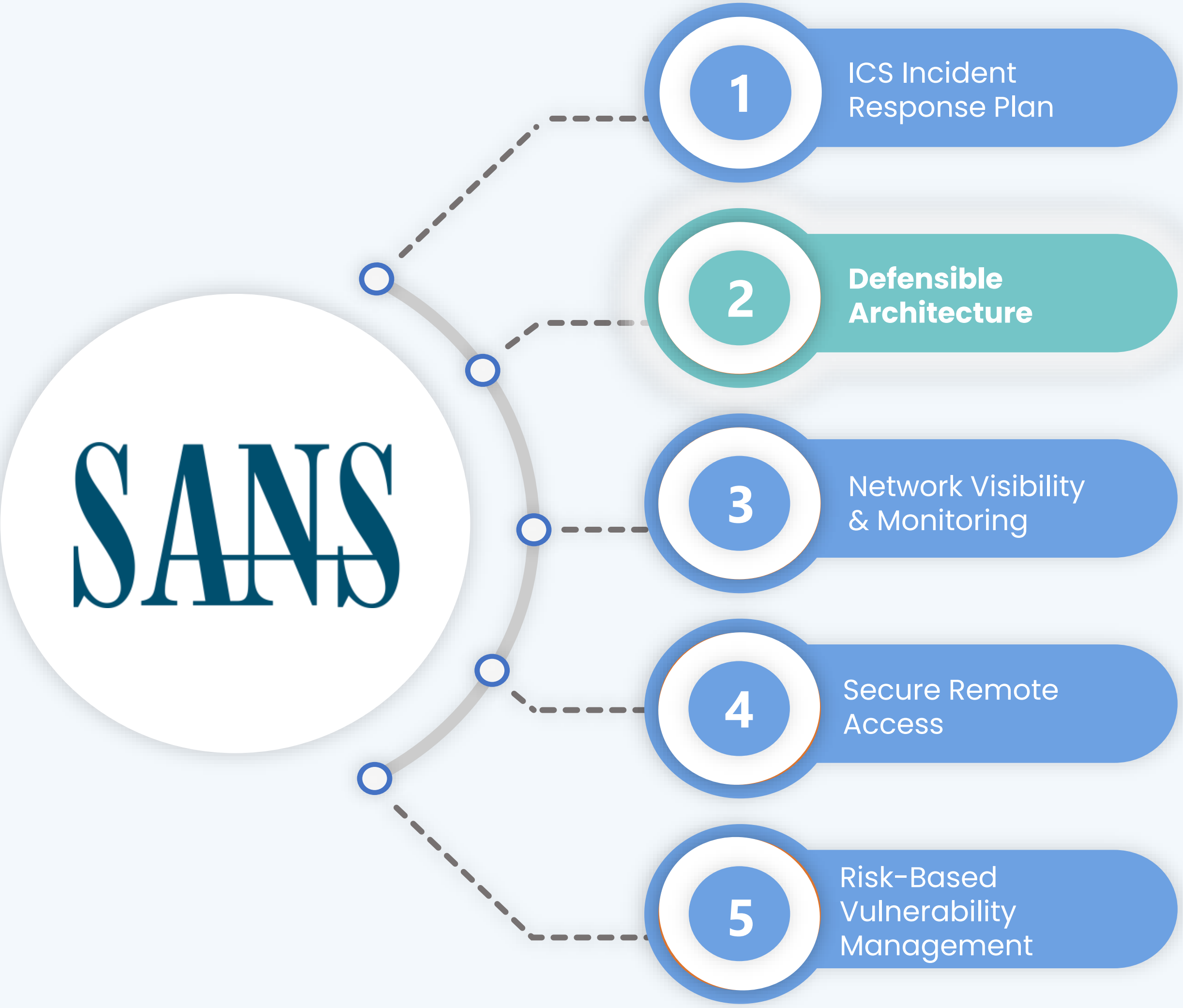


1. **ICS Incident Response Plan**
2. Defensible Architecture
3. Network Visibility & Monitoring
4. Secure Remote Access
5. Risk-Based Vulnerability Management

Develop a comprehensive incident response plan specifically designed for ICS environments.

This plan should encompass procedures for the detection, reaction, and recovery from cybersecurity incidents.

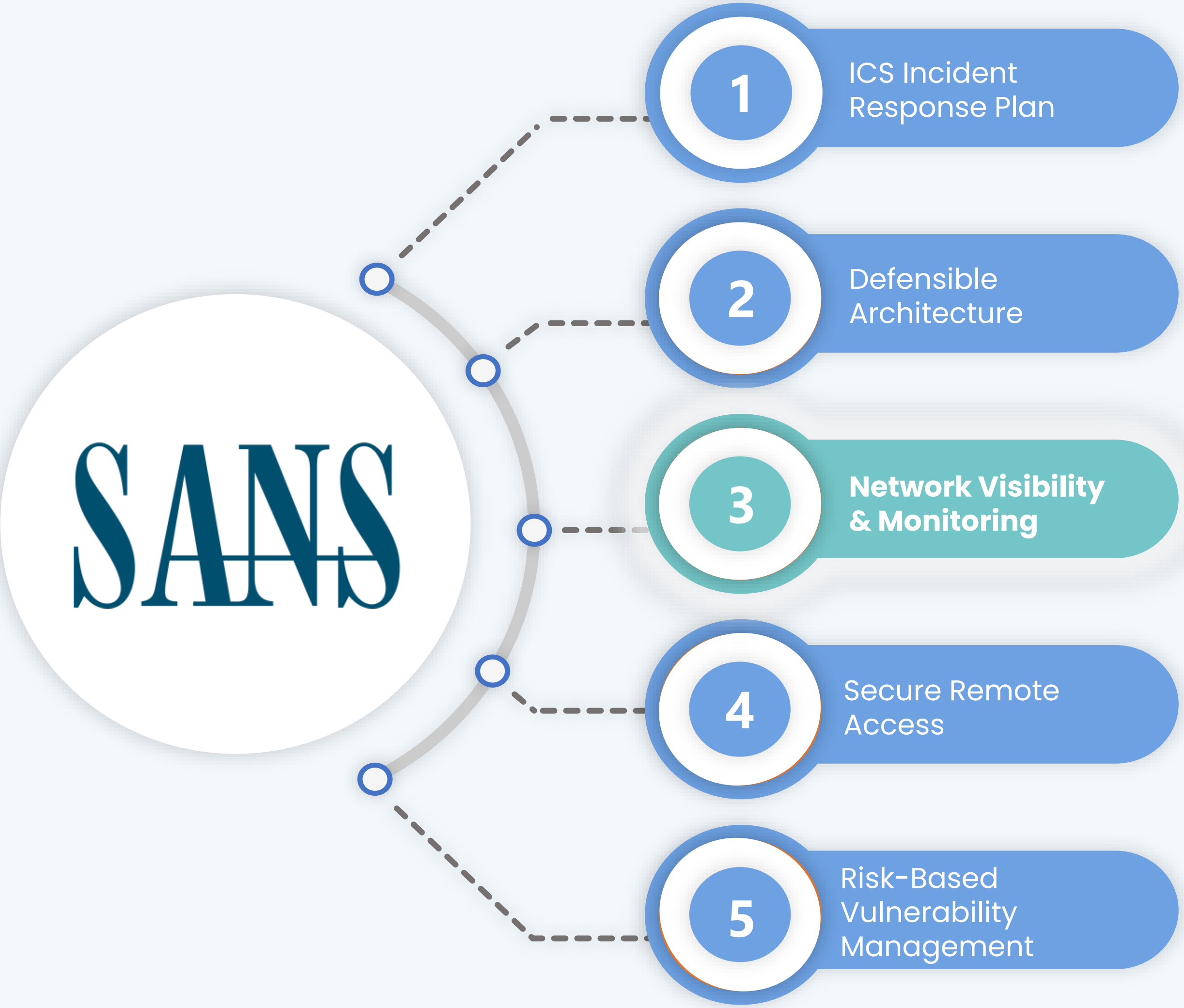
SANS Five ICS Critical Security Controls


SANS
1
ICS Incident Response Plan
2
Defensible Architecture
3
Network Visibility & Monitoring
4
Secure Remote Access
5
Risk-Based Vulnerability Management

Construct a network architecture that effectively segments and isolates critical systems.

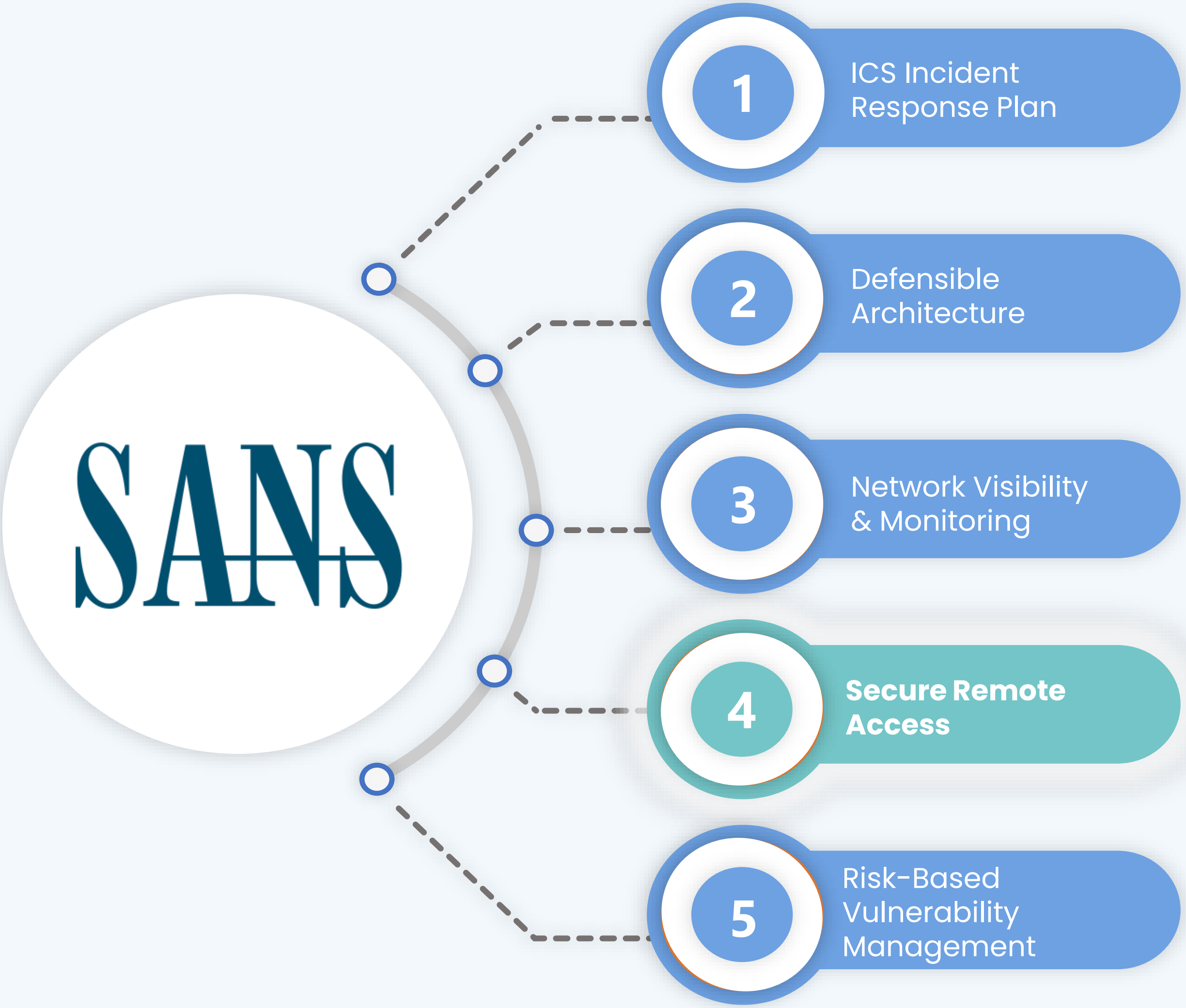
The goal is to minimise the attack surface and reduce the potential impact of cyber incidents.

SANS Five ICS Critical Security Controls


SANS
1
ICS Incident Response Plan
2
Defensible Architecture
3
Network Visibility & Monitoring
4
Secure Remote Access
5
Risk-Based Vulnerability Management

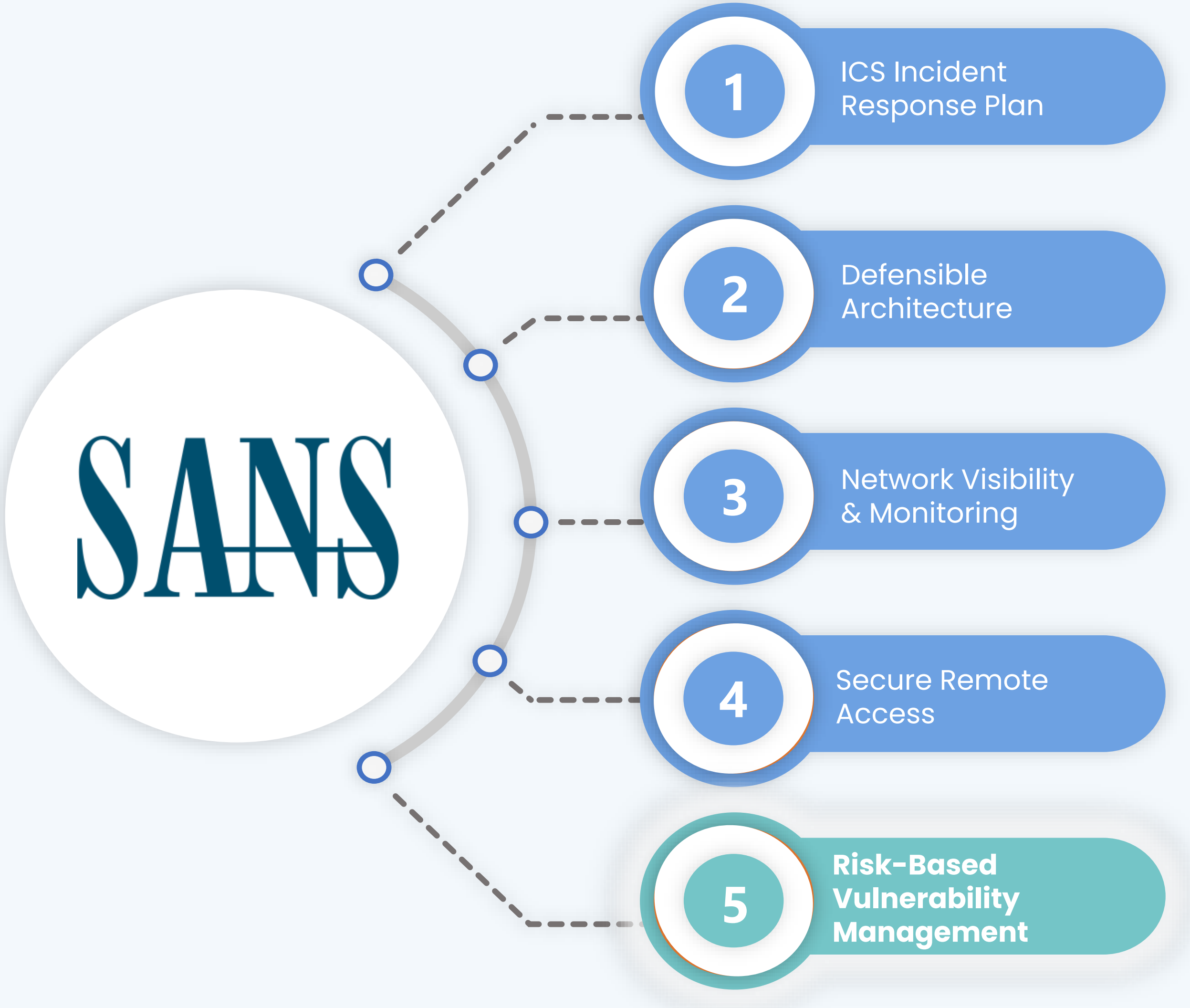
Achieve continuous monitoring of ICS networks to promptly detect anomalies and potential threats.

SANS Five ICS Critical Security Controls


SANS
1
ICS Incident Response Plan
2
Defensible Architecture
3
Network Visibility & Monitoring
4
Secure Remote Access
5
Risk-Based Vulnerability Management

Implement secure, controlled remote access solutions to manage and monitor access to ICS environments effectively.

SANS Five ICS Critical Security Controls



1 ICS Incident Response Plan

2 Defensible Architecture

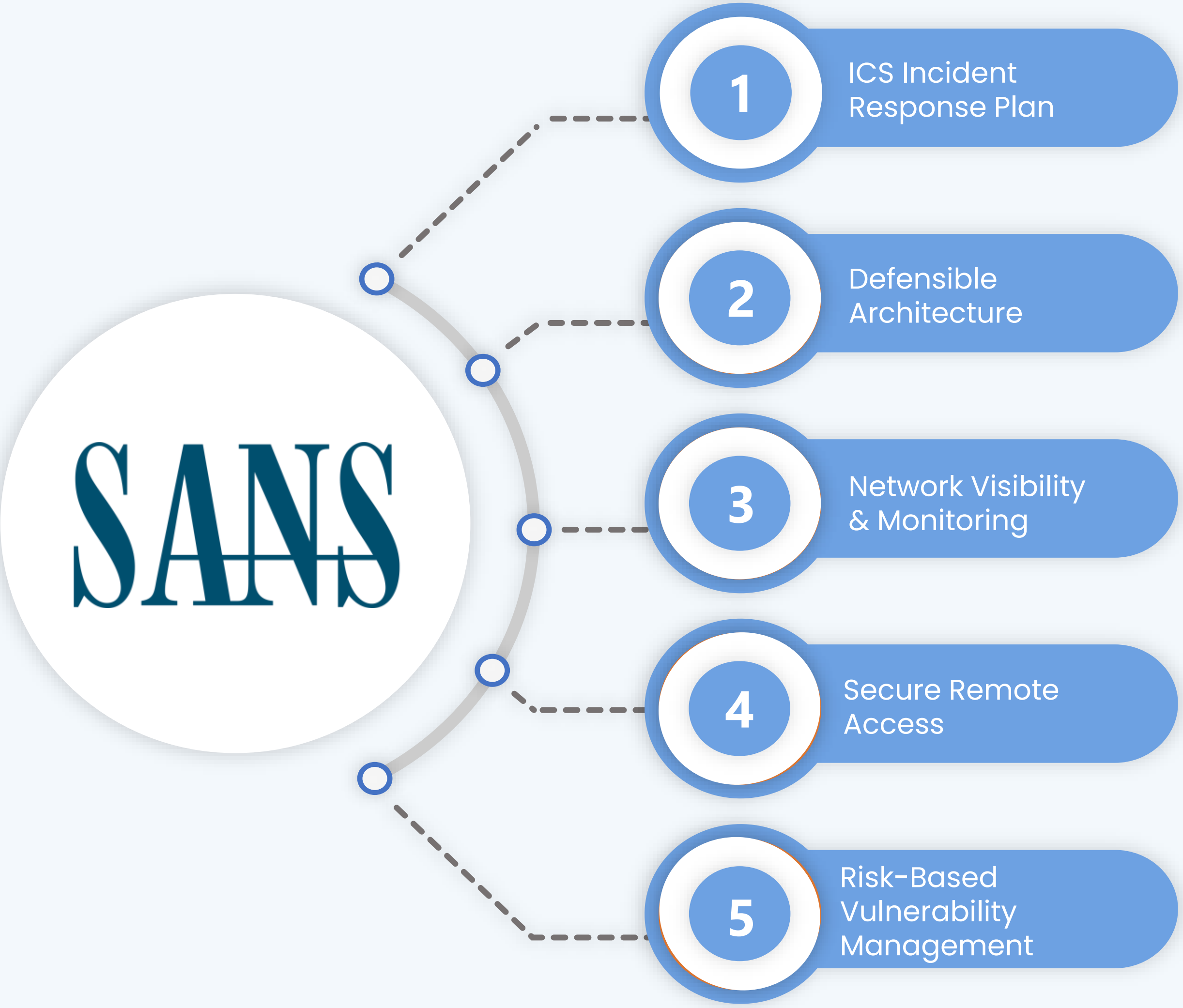
3 Network Visibility & Monitoring

4 Secure Remote Access

5 Risk-Based Vulnerability Management

Conduct systematic vulnerability assessments and prioritise remediation based on the potential impact on critical systems.

An Interconnected Approach

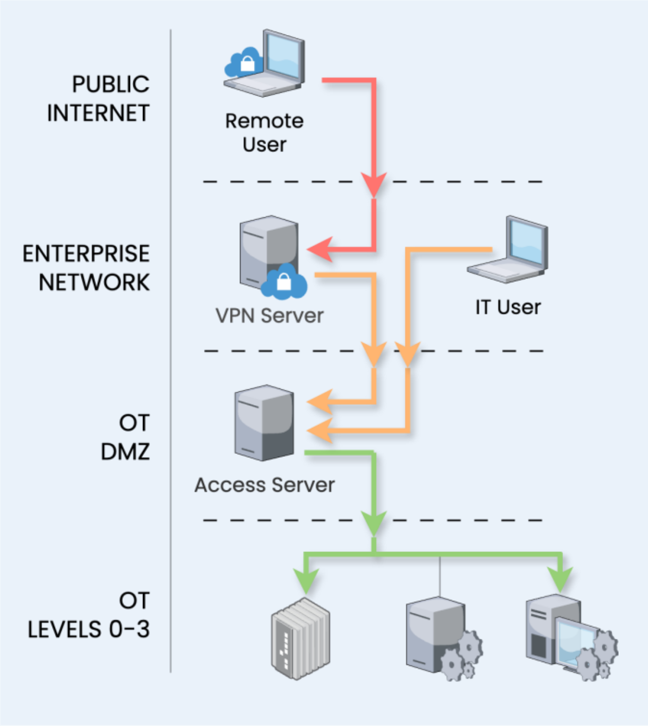


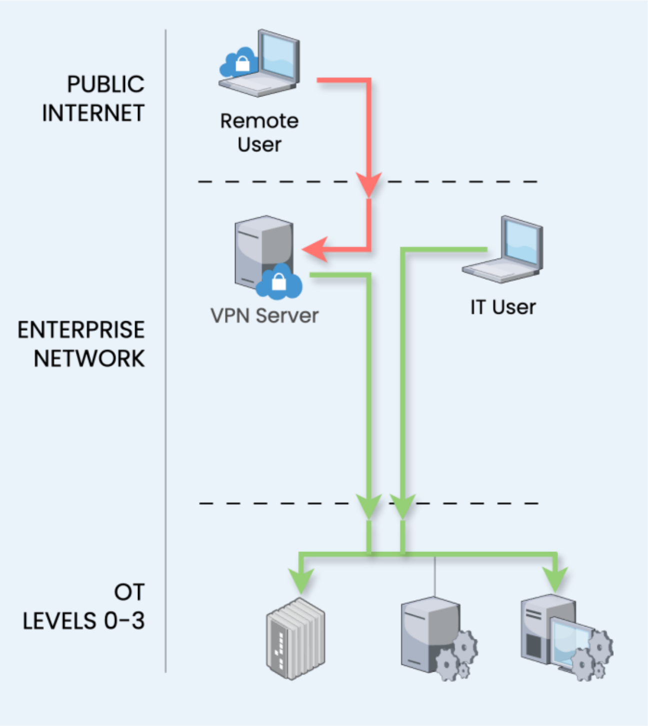
1. ICS Incident Response Plan
2. Defensible Architecture
3. Network Visibility & Monitoring
4. Secure Remote Access
5. Risk-Based Vulnerability Management

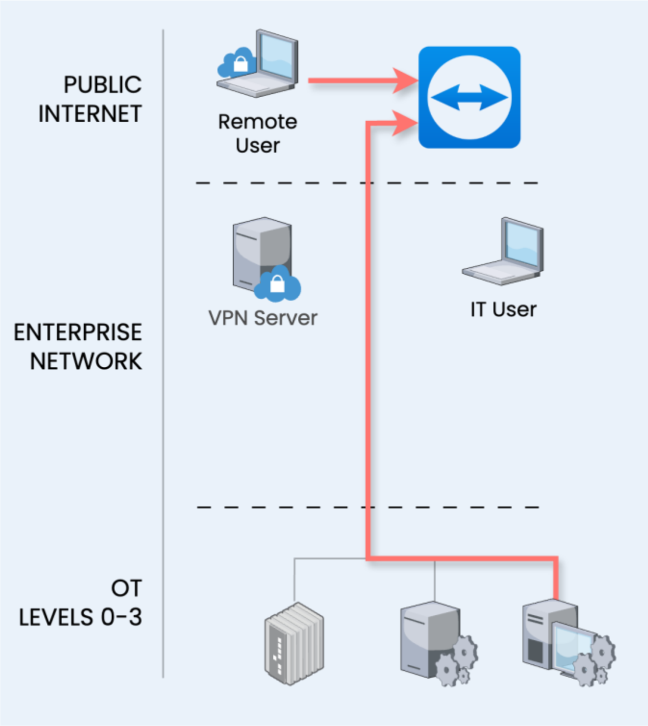
dull.

Secure Remote Access

Typical Remote Access Architectures





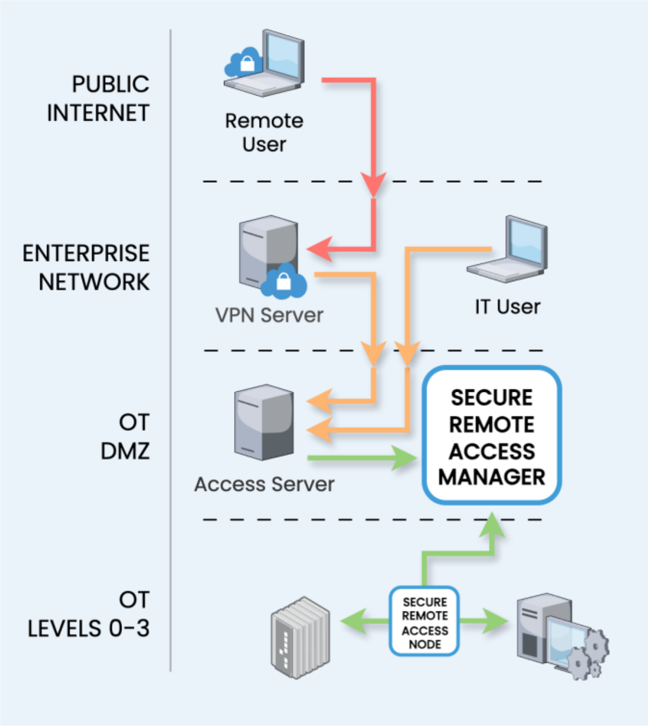


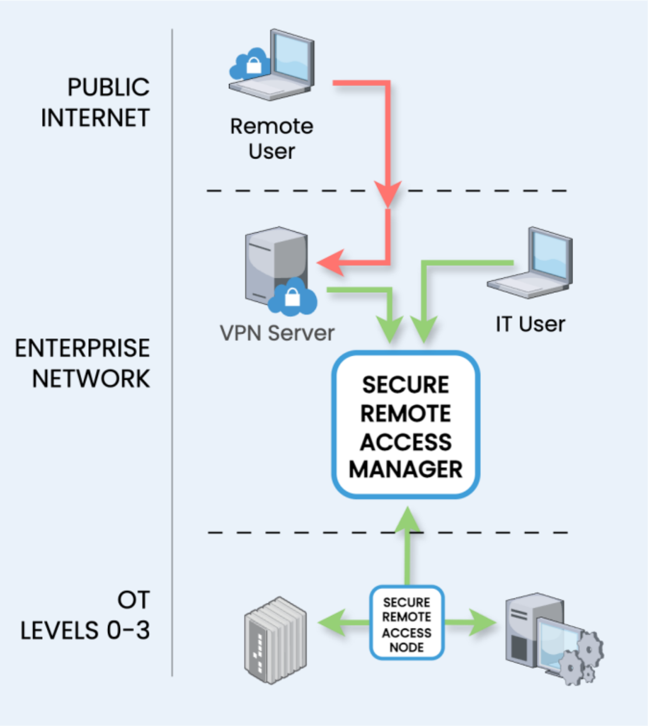
Mature environments that require **multiple hops** before access to the OT environment is granted

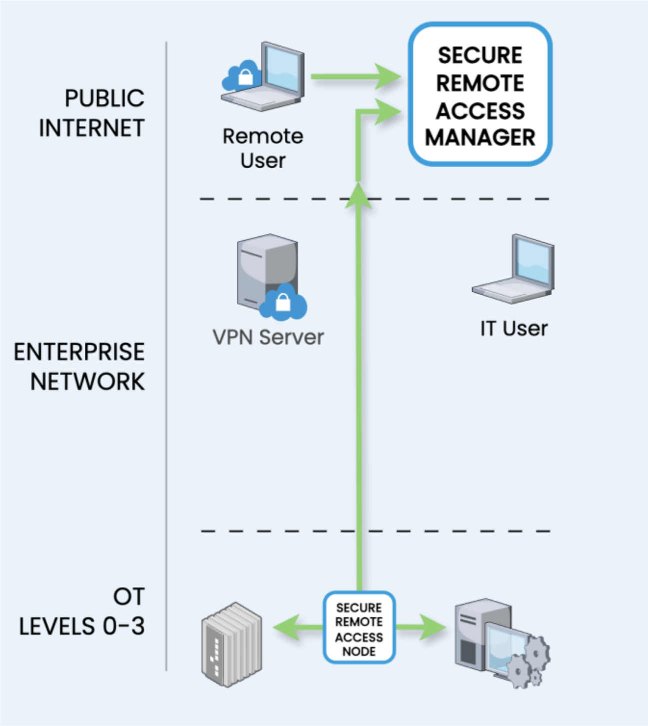
Supporting a **defence-in-depth posture**, but with unregulated access to OT from the Enterprise Network

Using IT **remote support software**, such a Teamviewer, to access OT workstations

Implementing Secure Remote Access







Removing porosity across the OT DMZ boundary and **decreasing administrative overhead**

Standardising OT access and **enforcing Zero Trust controls** from a central policy enforcement point

Maintaining the **seamless access** associated with TeamViewer, while **supporting OT protocol connectivity**

dull.

Thank You

Tim Jackson

tim.jackson@dull.net