Privasec | RED
RED TEAMING & ADVANCED ETHICAL HACKING

Critical Infrastructure (SCADA) Security
Fact Sheet v2.2

WHAT ARE SCADA SYSTEMS?

Critical infrastructure is a term used to describe the assets, physical facilities, supply chains, information technologies and communication networks, which if destroyed, degraded or rendered unavailable for an extended period, would significantly impact on the social or economic wellbeing of the nation, or affect Australia's ability to conduct national defence and ensure national security. Systems managing operational aspects of that critical infrastructure are commonly known as SCADA (Supervisory Control and Data Acquisition) systems.

WHY CARE NOW?

Historically, security in the world of SCADA was managed by the principles of "security by obscurity" and what is referred to as "the air gap".

As these systems used proprietary obscure protocols that not many people other than specialist engineers understood and were isolated from other networks, an air gap existed that reduced the risk of SCADA systems being compromised and exploited. Security was never a consideration due to their isolation and the focus on process control, safety and reliability.

However, connectivity to corporate IT networks is now increasing due to use of common technology standards and network protocols such as IP connectivity, data requirements to enable better decision making, and improved management capabilities through the leveraging of corporate IT management platforms and staff.

With this increased connectivity comes increased risks and opportunity for a security breach of the SCADA network, or adverse and unintended consequences due to accidental human error.

WHY ARE SCADA ASSESSMENTS DIFFERENT ?

The following table demonstrates why traditional IT security controls and assessment may not work or be as effective:

Category	SCADA	Corporate IT
Confidentiality	Low	High (where determined by data classification)
Integrity	Very High	Low to Very High (depending on specific system)
Availability	• Rebooting and momentary downtime usually not acceptable. • Operates on philosophy of seven nines (99.99999%)	• Rebooting acceptable in specified time windows • Outages may be tolerated (as determined by business impact)

Category	SCADA	Corporate IT
Impact of System Failure	Regulatory noncompliance, environment, loss of life or serious injury, production or service delivery failure affecting the territory served	Business operations (as determined by Business Impact Assessments related to the specific system)
Time-Criticality	Response to human interaction and emergency situations is critical	System dependent, but generally less time critical
Performance	Must be "real-time" Latency and jitter are not acceptable Moderate throughput	Must be consistent Latency and jitter may be acceptable High throughput may be required
Prioritising Risk Controls	Safety always takes priority Process protection (integrity and availability) are the next primary factors Fault tolerance is essential	Protecting data confidentiality and integrity are primary Fault tolerance less important

HOW WE CAN HELP

We offer a range of services which are specifically tailored to assist your organisation in applying a risk based approach to secure your critical infrastructure.

Our services include:

- Security Assessments based on Australian Government and Industry Security Standards.
- SCADA Security Assurance Testing specifically designed to take all the precautions when performing vulnerability scanning and penetration testing.
- Network Architecture Reviews performed in accordance with Critical Infrastructure's Good Practices Guides (GPGs)

WHAT YOU GET

We will provide you with a concise report that:

- Describes current cyber threats and risks for your SCADA network.
- Identifies and prioritises the key findings observed.
- Includes a strategy and a roadmap to reduce your cyber risks and help build cyber resilience capabilities.

PREPARE FOR YOUR SCADA ASSESSMENT

The following people may be asked to provide information during the workshops:

- Key business stakeholders involved in managing and operating your IT operations.
- Information Security Manager or staff responsible for SCADA management.
- Administrators of the systems and network(s) processing, containing and/or supporting SCADA operations.
- Third party SMEs who may be involved in your operations and ongoing management.

NEXT STEP

Call us now to discuss how we can help to secure your critical/SCADA environment discussion.

Privasec

GRC GOVERNANCE AND INFORMATION SECURITY PARTNERS

RED RED TEAMING & ADVANCED ETHICAL HACKING

+61 1800 996 001 (AU)
+65 6610 9597 (SG)
+64 9 222 4725 (NZ)

info@privasec.com

www.privasec.com

New South Wales Office
Level 12, 234 George Street
Sydney 2000
NSW, Australia

Victoria Office
Level 6, 276 Flinders Street
Melbourne 3000
VIC, Australia

Queensland Office
Level 6, 200 Adelaide Street
Brisbane 4000
QLD, Australia

New Zealand Office
Level 4, 17 Albert Street
Auckland CBD 1010
New Zealand

Singapore Office
10 Anson Road
International Plaza #34-06
Singapore 079903

Malaysia Office
B-5-8 Plaza Mont Kiara
Mont Kiara 50480
Kuala Lumpur, Malaysia