Sellafield Ltd Performance Evaluation Overview and Lessons Learned

Presented by:

Scott Anderson

Chris Reid

Purpose of this presentation

1. High level discussion on the Sellafield Ltd security performance evaluation methodology.
2. Share our experiences and lessons learned in security performance evaluation.
3. Discuss our Physical Security Vulnerability Assessment Process.

Sellafield Site Background

Categorisation of NM in terms of Theft and Sabotage

- Categorisation by Theft
  - 13 Category I Facilities
  - 7 Category II Facilities
  - 50 Category III Facilities
  - 21 Category IV Facilities

- Categorisation by Sabotage
  - 23 High Consequence Vital Areas
  - 2 Vital Area Facilities
  - 66 Baseline Facilities

WINS Performance Evaluation Workshop

Security Assessment Framework

Step 1 Material Inventory (Categorisation for Theft)

Step 2 Malicious Actions Assessment (Categorisation for Sabotage)

Step 3 Physical Security Vulnerability Assessment

Step 4 Define Operational Requirements

Step 5 Deliver Functional Requirements

Step 6 Update local Facility Security Plan

Step 7 Assurance Cycle

Physical Security Vulnerability Assessment (PSVA) Overview

The Physical Security Vulnerability Assessment (PSVA) has three main purposes:

1. Identify and address security weaknesses.
2. Validate the Physical Protection System (PPS) Design against attack scenarios through effective counter measures.
3. Inform the Duty Holder / Responsible Person on those weaknesses and counter measures for risk management purposes.

Physical Security Vulnerability Assessment (PSVA) Overview

The Physical Security Vulnerability Assessment (PSVA) has three parts:

1. Adversarial Threat Scenarios.   (be Threat Informed)
2. Facility Characterisation.   (be Consequence Driven)
3. Assessment Output Report.   (Overall Assessment)

Establish Ground Rules

External Adversary – Reach to Breach (facility)

An external adversary will always start from the attack side of your initial

security boundary.

Insider – Reach to Consequence

An insider already has certain access privileges within your existing security regime.

Establish Ground Rules

Identify the Primary and Critical Points of Detect, Delay and Assess.

- Primary Points are the **First** opportunity to Detect, Delay and Assess an Adversary (external or Insider). This initiates your response to the event.

- Critical Points are the **Final** opportunity to Detect, Delay and Assess an Adversary (External or Insider) to **successfully** achieve your required response to an event.
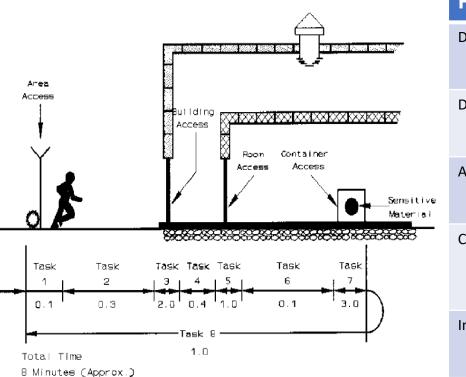
Part 1 - Adversarial Threat Scenario Definition

Define the 'Threat-Informed' aspects of the assessment.

Part 2 – Facility Characterisation

Example of forced entry external intruder

Example of Physical Protection System Functions

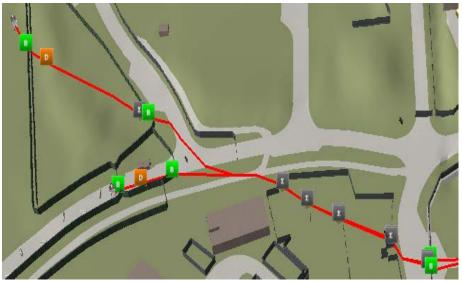| Function	Posture	Objective
Detect	Layers enabling immediate Detection.	Provide immediate detection of unauthorised access into sensitive areas.
Delay	Barriers against persons or vehicles.	Provide delay after detection enough for response personnel to neutralise the adversary.
Assess	Timely threat assessment.	Provide immediate assessment of detection.
Control of Access	Barriers denying unauthorised access.	Provide access controls that effectively prevents unauthorised access to sensitive areas.
Insider Mitigation	minimising unauthorised activity	Ensure trustworthiness and reliability of authorised persons.

Part 3 – Assessment Output Report

1. To identify and address security weaknesses.

2. To validate the Physical Protection System Security Outcome and demonstrate it achieves its required effect.

3. To inform evidence based security decision-making.

4. To inform the end user/asset owner on the considerations and the recommendations made to provide a fit-for-purpose Physical Protection System.

Sellafield Ltd

Security Modelling Capability

Decision support tool, identify adversary pathways, visualisation of security breaches, compute probability of successful attacks and measure effectiveness of site security through Design Verification.

- Questions?