National Nuclear Security Administration

Module 8

Vulnerability to Intrusion System Analysis (VISA) Methodology

A tabletop approach to systematically evaluate effectiveness of MPC&A through the use of Subject Matter Experts

Description

- Used at critical facilities operated by DOD, DOE, NASA, and other US agencies
- Scenario based
- Subject Matter Expert driven
- Results can be based on:
  - Documented values
  - Professional judgment
  - Combination of both
- Very flexible
  - Can be used for all types of facilities and systems
  - Can address all types of threats and targets for both insiders and outsiders
- Quality depends heavily on capabilities of experts involved

Two Variations

- Quantitative
  - Numerical calculation of system effectiveness
  - More accurate, but hand calculations can be cumbersome
  - Calculated results can falsely imply greater accuracy than available data supports
- Qualitative
  - Intuitive approach using logic process
  - Easier and quicker, but less accurate
- For this workshop, we will focus on the qualitative approach

VISA Process Overview

- Develop scenario
- Expand scenario into logical steps (detection opportunities)
- Analyze System Effectiveness for each step
- Develop System Effectiveness for scenario
- Document in a tabular format

Scenario Development

- **Exploit potential weaknesses**
- **Credible scenario that gives adversary best chance for success**
- **Develop description of adversary plan**
  - **Example:**

Adversaries use trees and buildings adjacent to the site perimeter to bridge over perimeter sensors and then use explosives to breach the building and storage room doors. After obtaining material and loading it into backpacks, the adversaries exit the site along the same path they entered.

Scenario Breakdown

- Expand scenario into sequence of logical steps
- Develop timelines
- Evaluate each step as if the proceeding step had been successful
- Each step represents a potential opportunity to detect, assess, engage, and neutralize the adversary

Scenario Table

Cuml. = cumulative time
Rem. = remaining time

Step	Step Time	Cuml. Time	Rem. Time	Step Description	P_D	P_A	P_E	P_N	Step Score
1	30	30	100	Bridge across the site perimeter					
2	25	55	75	Enter target building door					
3	25	80	50	Penetrate material storage room door					
4	15	95	35	Open containers, gather material					
5	15	110	20	Exit building					
6	20	130	0	Cross back over perimeter					
Adversary timeline = 130 seconds **Response Force Time = 50 seconds**								System Effectiveness:	

P_D = Probability of Detection
P_A = Probability of Assessment
P_E = Probability of Engagement
P_N = Probability of Neutralization

VL = Very Low
L = Low
M = Moderate
H = High
VH = Very High

Elements of System Effectiveness

- **Probability of Detection (P_D) – sensing the activity of the adversary**
  - **security sensors, local alarm, observation, inventory discrepancy**
- **Probability of Assessment (P_A) – correctly determining that the detected activity is an adversary act requiring a response**
  - **CCTV, automatic response, investigation of discrepancies**
- **Probability of Engagement (P_E) – ability of the responders to reach and engage adversaries prior to adversaries completing their mission**
  - **Response time from when alarm received shorter than adversary task time remaining after alarm**
- **Probability of Neutralization (P_N) – ability to overcome the adversary and prevent the adversary from completing the mission**
  - **Response force numbers and capabilities superior to adversary**

Evaluating Detection

- Examples of detection methods
  - Sensors
  - Guards
  - Site personnel
  - Procedures
- Determining detection values
  - Performance tests
  - Published data
  - Professional judgment
- Impact of nuclear security culture on detection
  - Adherence to procedures
  - Maintenance, testing, calibration of equipment

Evaluating Assessment

- Types of Assessment
  - Cameras
  - Guards
  - Site personnel
  - Procedures
- Determining assessment values
  - Performance tests
  - Published data
  - Professional judgment
- Impact of nuclear security culture on assessment
  - Willingness to report abnormal behavior and events
  - Adherence to procedures
  - Acknowledgment of threat

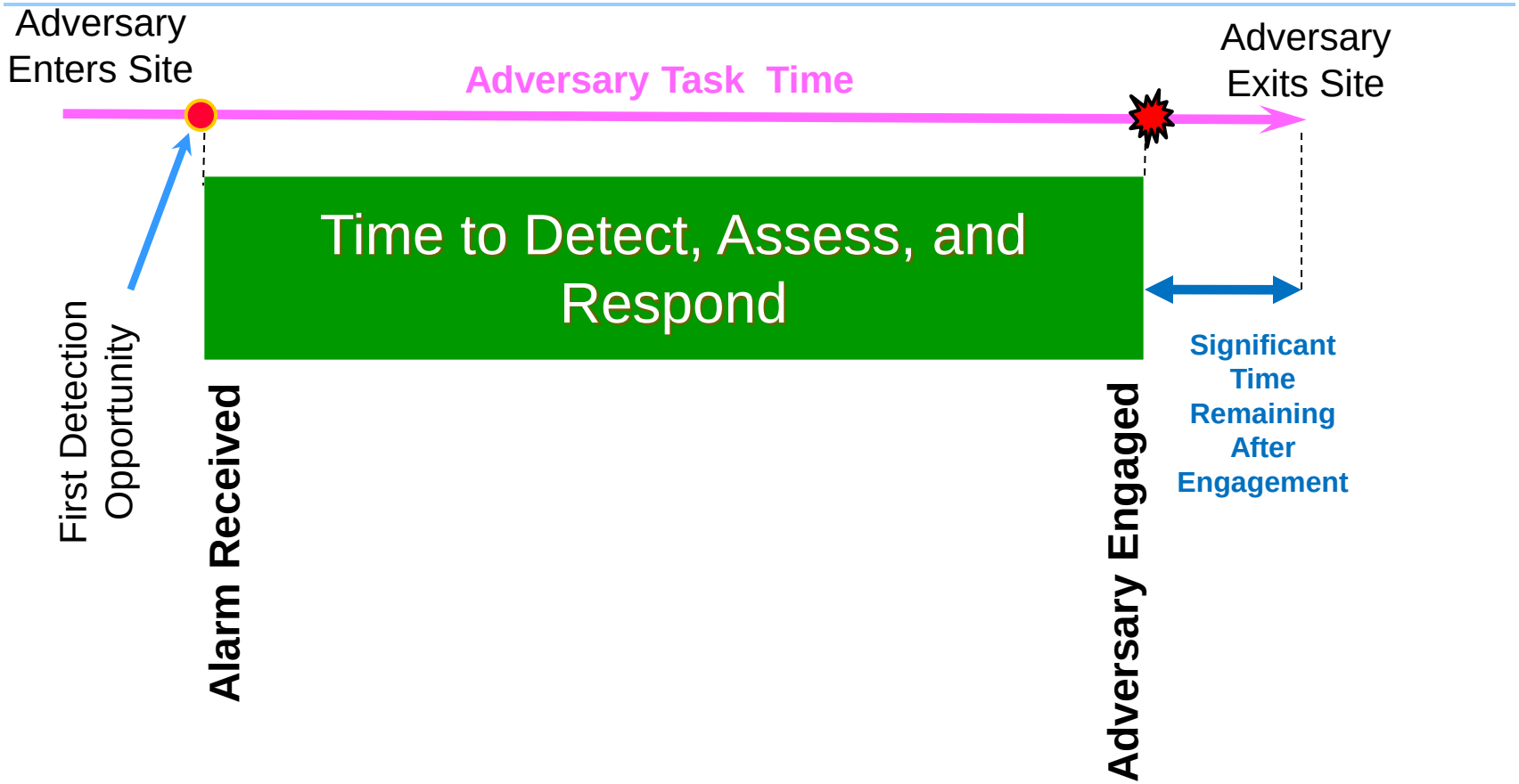
Evaluating Engagement

- Adversary timeline
  - Task times
    - Published delay values
    - Performance tests
    - Subject Matter Expert estimates
    - Deployment times (foot, vehicle)
- Response timeline
  - Can be based on performance test data
  - Can be estimated
    - CAS operator assessment and reporting time
    - Response force muster time
    - Deployment time (foot, vehicle)
- Impact of nuclear security culture on engagement
  - Frequency of drills
  - Adequacy of training
  - Acknowledgment of threat

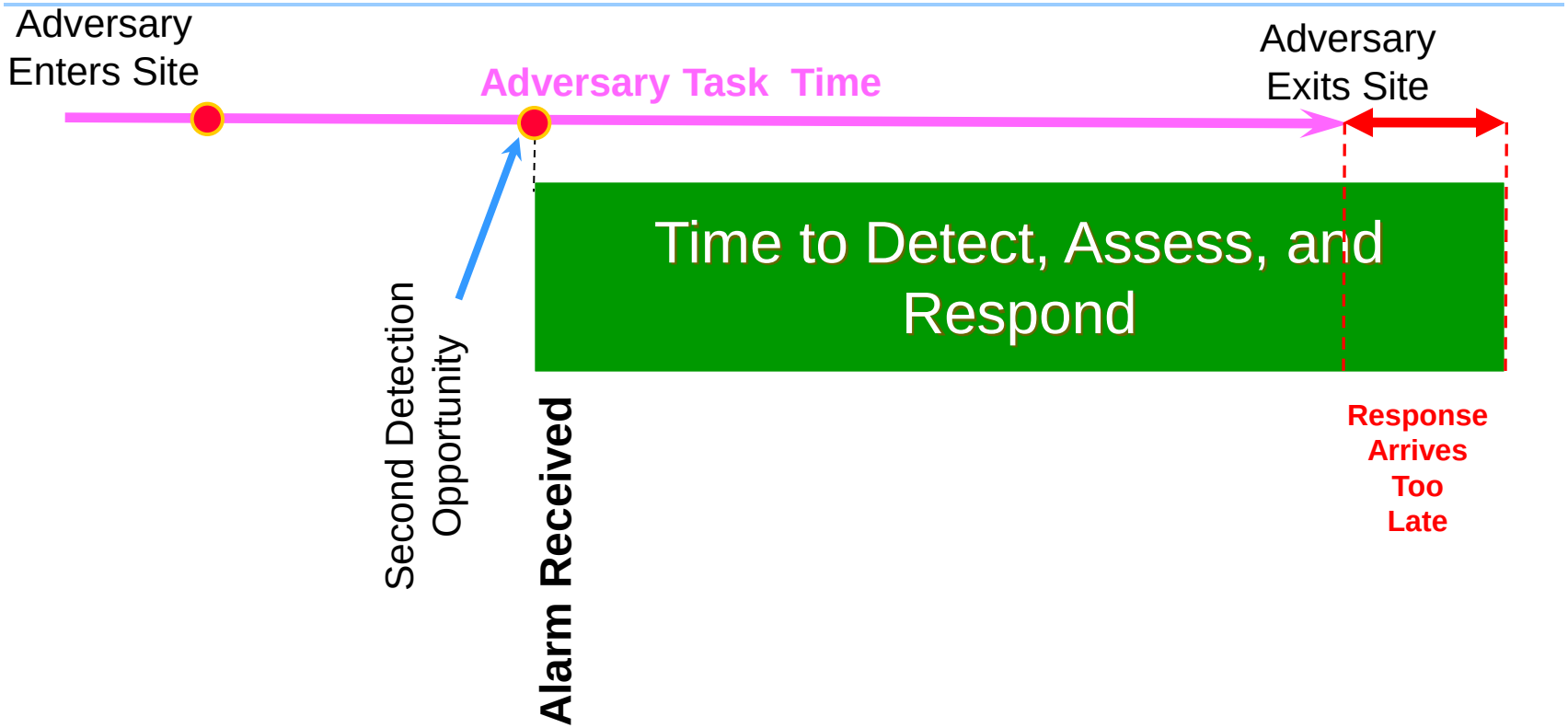
Response Force Timeline Example

Response Force Timeline (seconds)	
Activity	Time
CAS operator assesses alarm	
CAS operator notifies head of shift	
Head of shift dispatches team of responders	
Responders don gear (vests, helmets, weapons)	
Responders exit CAS building	
Responders move tactically 135m to target building	
Total Response Force Time (RFT)	

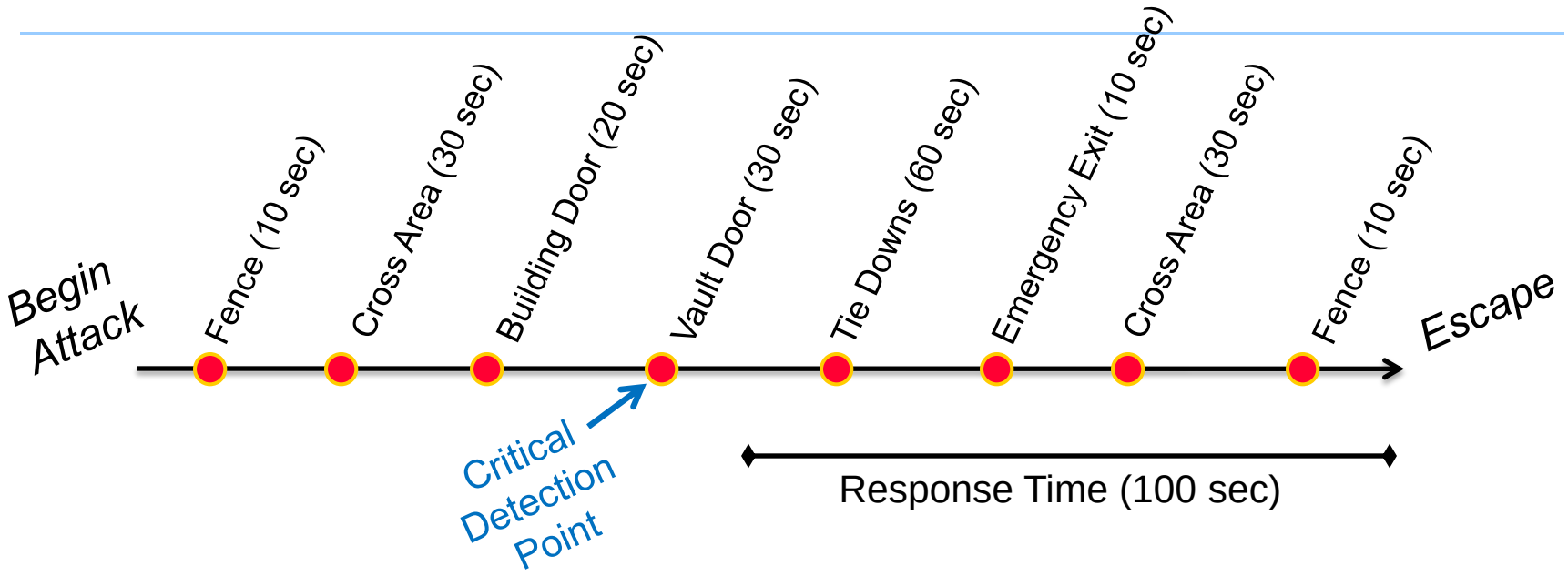
Task Time versus Response Time:
Very High Probability of Engagement



Task Time versus Response Time:
Very Low Probability of Engagement



Critical Detection Point



Delay and Time Element (working backwards)	Cumulative Time
10 seconds to exit over fence	**10**
30 seconds to cross area to fence	**40**
10 seconds to exit through emergency exit	**50**
60 seconds to defeat tie downs	**110**

Evaluating Neutralization

- Capability to neutralize adversary
- Often scenario specific
- Performance test results
- Computer modeling
- Estimates
  - Number of attackers versus number of defenders
  - Skills, training, equipment, weaponry, and motivation of each side
  - Adversary tactics versus response tactics
- Impact of nuclear security culture on neutralization
  - Adequate staffing
  - Planning and analysis
  - Troop support (equipment, housing, morale)
  - Acknowledgement of threat

Evaluating Steps

- **Within a step, evaluate each element individually**
  - **P_A is probability of assessment <u>given</u> detection of that step**
  - **P_E is probability of engagement** in the scenario **<u>given</u> detection and assessment of that step**
    - **Detection and assessment are step dependant, engagement is timeline dependant**
  - **P_N is probability of neutralization** in the scenario **<u>given</u> detection and assessment of that step and engagement in the scenario**

Evaluating Steps (cont.)

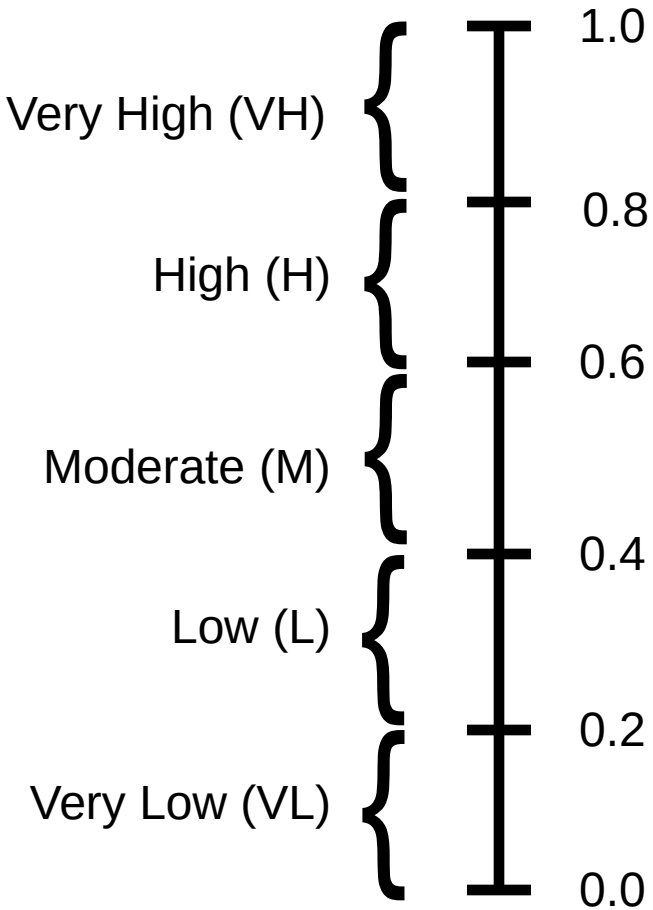
- **Detection, Assessment, Engagement, and Neutralization are a chain of events, each of which must occur to stop the adversary***
- **Within a step, elements of system effectiveness are dependent**

Detection → Assessment → Engagement* → Neutralization*

- **Intuitive approach**
  - **Weakest link in the chain**
- **Step score is the <u>lowest</u> qualitative value assigned for the step elements**

** Note: nonviolent insider scenarios generally only involve Detection and Assessment, and do not include Engagement and Neutralization*

Qualitative Ratings



Step Evaluation Example

Cuml. = cumulative time
Rem. = remaining time

Lowest Value

Step	Step Time	Cuml. Time	Rem. Time	Step Description	P_D	P_A	P_E	P_N	Step Score
1	30	30	100	Cross the site perimeter	M	L	VH	H	L
2	25	55	75	Enter target building door	H	M	H	H	M
3	25	80	50	Penetrate material storage room door	H	L	M	H	L
4	15	95	35	Open containers, gather material	L	VH	L	H	L
5	15	110	20	Exit building	H	VH	VL	H	VL
6	20	130	0	Cross back over perimeter	H	M	VL	H	VL
Adversary timeline = 130 seconds **Response Force Time = 50 seconds**							System Effectiveness:		

P_D = Probability of Detection
P_A = Probability of Assessment
P_E = Probability of Engagement
P_N = Probability of Neutralization

VL = Very Low
L = Low
M = Moderate
H = High
VH = Very High

Scenario Evaluation

- **Step scores are independent**
  - **If <u>any</u> step in scenario has sufficient detection and assessment (and for the outsider, enough time remaining for engagement and neutralization) to stop adversary, system wins**

Example: outsiders are able to cross the perimeter undetected (step 1), but are detected and assessed at the building entrance (step 2) with sufficient time remaining to engage and neutralize them prior to exiting site with material. System win is based on step 2 in this example.

Scenario Evaluation (cont.)

- **Intuitive approach: System Effectiveness is driven by:**
  - **Strongest point in the system**
  - **Weakest point for adversary**
- **Scenario System Effectiveness is the highest step score**

Scenario Evaluation Example

Cuml. = cumulative time
Rem. = remaining time

Lowest Value

Step	Step Time	Cuml. Time	Rem. Time	Step Description	P_D	P_A	P_E	P_N	Step Score
1	30	30	100	Cross the site perimeter	M	L	VH	H	L
2	25	55	75	Enter target building door	H	M	H	H	M
3	25	80	50	Penetrate material storage room door	H	L	M	H	L
4	15	95	35	Open containers, gather material	L	VH	L	H	L
5	15	110	20	Exit building	H	VH	VL	H	VL
6	20	130	0	Cross back over perimeter	H	M	VL	H	VL
								System Effectiveness:	M

Highest Value

Adversary timeline = 130 seconds
Response Force Time = 50 seconds

P_D = Probability of Detection
P_A = Probability of Assessment
P_E = Probability of Engagement
P_N = Probability of Neutralization
VL = Very Low
L = Low
M = Moderate
H = High
VH = Very High

Insider Considerations

- **Nonviolent insider**
  - **Will stop when confronted**
  - **May not want to be identified**
  - **Typically only evaluate detection and assessment**
- **Violent insider**
  - **Willing to kill to avoid capture**
  - **Evaluate detection, assessment, engagement, and neutralization**

Scenario Evaluation NV Insider Example

Lowest Value

Step	Step Description	P_D	P_A	Step Score
1	**The insider gains access to storage area.**	VL	**L**	**VL**
2	**The insider obtains material from a storage container.**	VL	**VH**	**VL**
3	**The operator carries the stolen material out of the storage area.**	**VH**	VL	**VL**
4	**The insider carries material out through the building entry control point.**	M	**H**	M
5	**The insider carries material out through the site entry control point.**	VL	**L**	**VL**
			System Effectiveness:	M

Highest Value

P_D = Probability of Detection
P_A = Probability of Assessment

VL = Very Low
L = Low
M = Moderate
H = High
VH = Very High

System Upgrade Evaluation

Steps

1. Identify system weaknesses (vulnerabilities)
2. Identify upgrades (technical and procedural) that address each weakness
3. Logically group upgrades into packages
4. Prioritize upgrade packages factoring in cost-benefit analysis

Upgrade Considerations

Potential Weaknesses

- Detection
  - Poor sensor coverage
- Assessment
  - Dispatch delay, inclement weather, poor communication
- Delay
  - Minimal delay requires shorter response times
- Response Force Times
  - Long distances, poor communication, low numbers
- Neutralization
  - Effectiveness of weaponry, tactics, training, vehicles, numbers, fighting positions

Reanalyze Scenarios

- Analyze potential upgrades
  - Determine effect on System Effectiveness
    - Existing scenarios
    - New scenarios
- Prioritize Upgrade Options
  - Greatest impact
  - Cost effective

Nonviolent Insider Example

Threat Description

- Single individual with access to site
- Willing to misuse access and/or authority to steal material
- Not willing to use violence or force
- Willing to attempt abrupt or protracted theft

Example Facility and Target

- Site perimeter consists of single fence with vibration sensor
- Site entry control point (ECP) does not have radiation portal monitor or metal detector
- Building has an ECP equipped with a radiation portal monitor and metal detector that is staffed during the day
- The building has a material storage room adjacent to the processing area that is opened at the beginning of the shift and not secured until the end of the shift
- Samples are carried by the process operator to another building for analysis
- Target is HEU metal stored in simple containers in the material storage room

Scenario

The process operator enters the material storage room during a break and removes material from a container. When the operator carries a sample out of the building to be measured, he hides the material along the way. At the end of the day, the operator retrieves the material and exits the site through the site ECP.

Scenario Steps

Step	Step Description
1	**The insider is at work in the process area. During a break, while other personnel are out of the area, the operator enters the material storage room.**
2	**The operator opens a container and places material in a bag that the insider can hide under their coat.**
3	**The operator carries the stolen material together with a sample out through the building ECP.**
4	**The operator hides the stolen material on the way to the measurement lab**
5	**At the end of the day, the operator retrieves the stolen material.**
6	**The operator exits with the material through the site ECP**

Scenario Evaluation

Step	Step Description	P_D	P_A	Step Score
1	**The insider is at work in the process area. During a break, while other personnel are out of the area, the operator enters the material storage room.**	**VL**	**L**	**VL**
2	**The operator opens a container and places material in a bag that the insider can hide under their coat.**	**VL**	**VH**	**VL**
3	**The operator carries the stolen material together with a sample out through the building ECP.**	**VH**	**VL**	**VL**
4	**The operator hides the stolen material on the way to the measurement lab**	**L**	**L**	**L**
5	**At the end of the day, the operator retrieves the stolen material.**	**L**	**L**	**L**
6	**The operator exits with the material through the site ECP**	**VL**	**L**	**VL**
			System Effectiveness:	**L**

P_D = Probability of Detection
P_A = Probability of Assessment

VL = Very Low
L = Low
M = Moderate
H = High
VH = Very High

Example Upgrades

- Implement two-person rule that requires two people to actively participate in any activity in the storage room
- Install a gate on the entrance to the storage room that requires badge reads from two persons on both entry and exit that is activated during the day
- Use a separate organization on site for transferring samples to the measurement laboratory

Upgrade Evaluation

Step	Step Description	P_D	P_A	Step Score
1	**The insider is at work in the process area. During a break, the operator enters the material storage room. Access controls on day gate require operator to enter with another person.**	**VL**	**L**	**VL**
2	**The operator opens a container and places material in a bag that the insider can hide under their coat. Detection and assessment is provided by other person.**	**VH**	**VH**	**VH**
3	**The operator carries the stolen material together with a sample out through the building ECP. Detection and assessment provided by radiation monitor combined with violation of sample transfer procedure.**	**VH**	**VH**	**VH**
4	**The operator hides the stolen material on the way to the measurement lab**	**L**	**L**	**L**
5	**At the end of the day, the operator retrieves the stolen material.**	**L**	**L**	**L**
6	**The operator exits with the material through the site ECP**	**VL**	**L**	**VL**
			System Effectiveness:	**VH**

P_D = Probability of Detection
P_A = Probability of Assessment

VL = Very Low
L = Low
M = Moderate
H = High
VH = Very High

Outsider Example

Example Threat

- Five adversaries with military-style training
- Equipped with automatic weapons, grenades, and breaching charges
- Highly motivated, willing to kill and be killed to ensure success of mission
- Passive insider supplies outsiders with information about security measures, building and site layout, target locations, etc.

Example Facility and Target

- Site perimeter consists of single two meter high fence with vibration sensors and cameras
- Site ECP does not have radiation portal monitor or metal detector
- Target building is located 60 meters from the perimeter.
- Building main entry door is a single hollow core metal door locked with a key lock and equipped with a sensor (magnetic switch) but no camera
- The building has a material storage room with a hardened door locked with a key lock and equipped with a sensor (magnetic switch) but no camera
- Target is HEU metal stored in containers in the material storage room. Two containers are a goal quantity for the adversary

Example Response Force

- Fifteen responders
- Well-trained, well-motivated
- Equipped with body armor, automatic weapons
- Total time from receipt of alarm to arrival at target building is 140 seconds

Scenario

The adversaries pull up to the outside of the perimeter at night in a large truck. The adversaries use a ladder from the top of the back of the truck to bridge over the perimeter fence. The adversaries use breaching charges to penetrate the building ECP door and the storage room door, load material containers into backpacks, and return off site along the same path.

Scenario Steps

Step	Step Description
1	Adversaries attack at night. Adversaries park truck next to perimeter near target building. Four adversaries use a ladder from the top of the truck to cross over the perimeter fence (10 seconds) while one adversary remains behind with the truck.
2	Adversaries cross 60 meters to the building (20 seconds) and use breaching charges to penetrate the main entry door (25 seconds). Two adversaries enter the building while two adversaries remain outside to engage any responders.
3	Adversaries move through the building (20 seconds) and use breaching charges to penetrate the material storage room door (25 seconds).
4	Adversaries grab two containers and load them into backpacks (5 seconds).
5	Adversaries move back through the building and exit the main entry door (20 seconds).
6	Adversaries cross back to the perimeter (20 seconds) and cross the perimeter fence using the ladder (10 seconds). Adversaries depart in the truck.

Scenario Evaluation

Response Force Time = 140

Step	Step Time	Cuml. Time	Rem. Time	Step Description	P_D	P_A	P_E	P_N	Step Score
1	10	10	145	Adversaries attack at night. Adversaries park truck next to perimeter near target building. Four adversaries use a ladder from the top of the truck to cross over the perimeter fence (10 seconds) while one adversary remains behind with the truck.	VL	VH	H	VH	VL
2	45	55	100	Adversaries cross 60 meters to the building (20 seconds) and use breaching charges to penetrate the main entry door (25 seconds). Two adversaries enter the building while two adversaries remain outside to engage any responders.	VH	L	VL	VH	VL
3	45	100	55	Adversaries move through the building (20 seconds) and use breaching charges to penetrate the material storage room door (25 seconds).	VH	L	VL	VH	VL
4	5	105	50	Adversaries grab two containers and load them into backpacks (5 seconds).	VL	L	VL	VH	VL
5	20	125	30	Adversaries move back through the building and exit the main entry door (20 seconds).	VL	L	VL	VH	VL
6	30	155	0	Adversaries cross back to the perimeter (20 seconds) and cross the perimeter fence using the ladder (10 seconds). Adversaries depart in the truck.	VL	VH	VL	VH	VL
								System Effectiveness:	VL

P_D = Probability of Detection
P_A = Probability of Assessment

P_E = Probability of Engagement
P_N = Probability of Neutralization

VL = Very Low
L = Low
M = Moderate
H = High
VH = Very High

Upgrades

- **Install CCTV cameras covering the interior and exterior of the building door, the material storage room door, and the interior of the material storage room.**
- **Install a second hardened and alarmed door inside the main entry door to create a person-trap.**
- **Install restraints over containers in the material storage room.**

Upgrades Evaluation

Response Force Time = 140

Step	Step Time	Cuml. Time	Rem. Time	Step Description	P_D	P_A	P_E	P_N	Step Score
1	10	10	230	Adversaries attack at night. Adversaries park truck next to perimeter near target building. Four adversaries use a ladder from the top of the truck to cross over the perimeter fence (10 seconds) while one adversary remains behind with the truck.	VL	VH	VH	VH	VL
2	70	80	160	Adversaries cross 60 meters to the building (20 seconds) and use breaching charges to penetrate the main entry door (25 seconds) and the inner door (25 seconds). Two adversaries enter the building while two adversaries remain outside to engage any responders.	VH	VH	VH	VH	VH
3	45	125	115	Adversaries move through the building (20 seconds) and use breaching charges to penetrate the material storage room door (25 seconds).	VH	VH	VL	VH	VL
4	65	190	50	Adversaries cut through restraints on one container (30 seconds) and restraints on second container (30 seconds), grab two containers and load them into backpacks (5 seconds).	VL	VH	VL	VH	VL
5	20	210	30	Adversaries move back through the building and exit the main entry door (20 seconds).	VL	VH	VL	VH	VL
6	30	240	0	Adversaries cross back to the perimeter (20 seconds) and cross the perimeter fence using the ladder (10 seconds). Adversaries depart in the truck.	VL	VH	VL	VH	VL
								System Effectiveness:	VH

P_D = Probability of Detection
P_A = Probability of Assessment

P_E = Probability of Engagement
P_N = Probability of Neutralization

VL = Very Low
L = Low
M = Moderate
H = High
VH = Very High

System Effectiveness Evaluation

- Determine credibility of scenario
- Combine detection, assessment, engagement and neutralization results for System Effectiveness
- Evaluate acceptable level of System Effectiveness based on adjectival or numeric result
  - What is “acceptable level” of System Effectiveness?