7.3.8 Incidents

7.3.8.1 Detection

Item	Rate
Detection is considered central to incident handling.	
Detection detects all event sequences with potentially serious negative consequences not covered by a prevention mechanism.	
Detection detects prevented event sequences then risk levels warrant it.	
Detection thresholds are set based on consequences and not based on levels of personnel available to handle alarms.	
Alarms give higher priority to higher potential consequences.	
False alarms are controlled by using high quality detection and triage.	
Adequate investigative capability is available to handle investigation of normal levels of alarms.	
Emergency response includes enough capacity to handle increased alarms associated with malicious attack against alarm systems.	
Detection teams are trained in triage of alarm system attacks and practice exceptional situations.	
Total for this area / 8	

7.3.8.2 Response

Item	Rate
Response systems are analyzed for reflexive control attacks.	
Analysis detects and reacts to threshold shifts for non-low risk systems.	
The response system mitigates serious negative event sequences by blocking them before the consequences become significant.	
Thresholds for response are dictated by risk management.	
Well defined circumstances are specified for disaster recovery or business continuity plan invocation.	
All responses are practiced in advance and only practiced and defined responses are used.	
Response regimens are designed to cover all event sequences at a reasonable level of granularity.	
Total for this area / 7	

7.3.8.3 Adaption

Item	Rate
Adaption is oriented toward changing the way classes of incidents are mitigated and is not used to mitigate specific attacks.	
Adaptation is done on 6-month time frames or longer.	
Adaptations involve risk analysis processes that justify the alternative and the cost associated with the changes.	
Adaptation is coordinated across the entire CISO function.	
Total for this area / 4	

7.3.8.4 OODA loops

Item	Rate
OODA loop times are computed based on risk management analysis of losses over time.	
For continuity of services a combination of fast OODA loops and redundant infrastructure is used.	
OODA loops are considered at all levels of the incident handling process and guide approval processes, automation selection, and autonomic responses.	
Timing, sensor placement and design, analytical power and technique, communication infrastructure, and actuator placement and design are jointly analyzed in design.	
Sensitivity analysis for timing deviations is applied to the Boyd cycle to assure resilience under deviations.	
Fail safes are used to break enemy Boyd cycles and passive defenses are preferred to active defenses.	
Total for this area / 6	

Total all totals and divide by 4

Prevention	Detection	Response	OODA Loop	Rate

Startup	*Diligence*	*Typical*	*Excellent*	*Best*
0.5	3	3	5	8