9.4 Attack and defense processes

Rate each item from 0 to 10. Sum the ratings and divide by 6 for a total rating.

Item	Rate
Attack processes are not used to model low risk situations.	
Attack processes at a generic threat, vulnerability, and consequence levels with examples are used to model medium risk situations.	
Detailed attack graph level are used to model high risk situations.	
The generic attack process is considered in the analysis of defenses.	
Defenses focus on severing attack graphs leading to high consequences, not on eliminating all vulnerabilities.	
Defense uses deterrence, prevention, detection, reaction, and adaptation.	
TOTAL (sum the ratings and divide by 6)	

Startup	Diligence	Typical	Excellent	Best
1.8	5	5	7	10

9.4.1 Deter

Rate each item from 0 to 10. Sum the ratings and divide by 15 for a total rating.

Item	Rate
Deterrence reduces the interest of attackers in specific targets.	
Psychological processes are directed at specific threat types.	
Attacker awareness of targets is attempted	
Attacker interest in targets is reduced	
Barriers that increase perceived difficulty.	
High profile prosecutions are used.	
Moral and ethical deterrence is used.	
Top management supports the deterrence efforts.	
Public relations does outreach to deter attackers.	
Corporate communications supports the public relations effort.	
Deception is used to cause attackers to misperceive the object of attacks.	
Training and awareness uses cases of attackers caught and punished.	
Policy provides for sanctions that are clear and uniform and identify those sanctions with specific acts so as to deter those acts.	
Policy requires that these sanctions are read, understood, and agreed to by those who agree to work for the enterprise.	
Awareness of sanction policies and consequences of actions are part of the awareness program goals.	
TOTAL (sum ratings and divide by 15)	

Startup	Diligence	Typical	Excellent	Best
0	2	3	6	9

9.4.2 Prevent

Rate each item from 0 to 10. Sum the ratings and divide by 23 for a total rating.

Item	*Rate*
Prevention is attained by technical safeguards that limit access or function.	
Prevention includes stopping the attacker from finding a target.	
Prevention includes reducing exploitable vulnerabilities.	
Prevention includes preventing expanding or exploiting of privilege.	
Firewalls are used to sever attack graphs from one side of the firewall to another.	
Prevention mechanisms are used between areas with different classifications.	
Firewalls limit the expansion and exploitation of network access by limiting the range of other network locations that can be reached and the manner in which they can be reached.	
Authentication is used to prevent an attacker from doing what an authorized user can do.	
More and more sure authentication techniques are used to increase the level of certainty that the user is who they claim to be as risk increases.	
Authorization associates authorities with authenticated identities.	
Authorization mechanisms include both the technical mechanisms that allow an identified and authenticated user to perform functions with data and the mechanisms used to grant, revoke, and alter those authorities.	
Administrative control over authorities is protected commensurate with risks of false or lost control.	
The principle of least privilege is applied at a granularity suitable to the risk.	
Access control is based on and compliant with enterprise security architecture.	
Use controls make situation-dependent decisions that enforce enterprise security architecture.	
High-speed intrusion prevention systems (IPS) are designed to meet timing and accuracy criteria associated with their use.	
Architecture acts as a preventive measure.	
Separation is a key architectural principle in use.	
Network zoning is used as a key separation mechanism.	
Surety levels are associated with all preventive mechanisms and systems.	
Surety is used as a basis for choosing between measures.	
Surety is commensurate with risk at all levels.	
Defenders favor higher surety at lower cost.	
TOTAL (sum the ratings and divide by 23)	

Startup	*Diligence*	*Typical*	*Excellent*	*Best*
1	5	6	7	9

9.4.3 Detect

Rate each item from 0 to 10. Sum the ratings and divide by 22 for a total.

Item	*Rate*
Detection provides timely notice of event sequences that have potentially substantial negative consequences.	
Detection is used to provide redundancy for preventive techniques.	
Detection rates event sequences by severity, urgency, or similar metrics.	
Detection mechanisms are updated to remain effective.	
Detection operates in a relatively quiet environment with little noise and few attacks to detect.	
Detection is never the primary protection method used.	
Host-based detection is used for exposed hosts.	
Network-based detection is used as a check on network separation mechanisms.	
Known intrusion types are detectable when justified by potential negative consequences.	
Anomaly detection is used in medium and high surety networks to verify proper protection is operable.	
The results of investigations help determine future detection thresholds.	
Automated response is carefully predetermined to assure that it will always result in a fail safe condition.	
Behaviors of systems and people in situations help to detect deviations.	
Situation provides context that is used to determine the acceptability and normalcy of behaviors.	
Patterns are matched with event sequences in context to determine if the events are to trigger a detection.	
Heuristics are developed over time for specific situations in systems.	
History is used to calibrate anomaly detection systems and historical data is recorded and replayed for calibration and testing purposes.	
Authority of users to perform tasks is used to differentiate between legitimate and illegitimate uses as part of detection.	
Identity is mapped into event sequences to differentiate legitimate from illegitimate event sequences.	
Collection, preservation, fusion, analysis, attribution are done in such a fashion as to meet all enterprise privacy and security policies.	
Risk aggregation is considered in detection system design.	
Risk management balances the benefits of detection with the risks.	
TOTAL (add the ratings and divide by 22)	

Startup	*Diligence*	*Typical*	*Excellent*	*Best*
0.2	5	4	7	9.5

9.4.4 React

Rate each item from 0 to 10. Sum the ratings and divide by 20 for a total.

Item	*Rate*
Reaction uses immediate actions to mitigate harm.	
Reaction time is analyzed to determine how reaction is implemented.	
Automated reactions take into account reflexive control attacks.	
Investigation of detected event sequences determines reaction.	
For certain classes of sequences, automated reactions are used.	
Investigative processes start after a timely triage indicates a need for investigation in time to prevent serious negative consequences.	
Investigations are carried out by qualified and properly trained individuals.	
The legal department is contacted at the start of all investigations.	
Investigations are carried out by, through, or in conjunction with legal counsel.	
Assessments are undertaken in response to high-consequence incidents.	
Risk management is verified after all high-consequence incidents.	
Coordination of response processes is undertaken across the enterprise at a management level.	
Physical security and HR coordination are involved when employees or contractors are involved in incident reaction.	
Line management gets involved and coordinates administrative actions.	
Tracking of reported incidents is used to detect coordinated attacks.	
Covering vulnerabilities is commonly used during incident response.	
Disabling of features, capabilities, or select systems is used to mitigate the short-term effects of an attack when the value of the service is outweighed by the damage of the attack.	
Specific strategies and tactics for response are defined and practiced in advance.	
Response strategies and tactics are practiced on test systems only.	
Unplanned reactions are only undertaken after escalation and management approval.	
TOTAL (sum the ratings and divide by 20)	

Startup	*Diligence*	*Typical*	*Excellent*	*Best*
1	5	6	7	9

9.4.5 Adapt

Rate each item from 0 to 10. Sum the ratings and divide by 5 for overall rating.

Item	*Rate*
Adaptation is a strategic response to operating environment changes.	
Adaptation involves architectural and process changes.	
Rezoning is a preferred adaptation approach.	
Processes for adaptations are equivalent to those for new designs.	
Architecture adaptation considers legacy system compatibility issues.	
TOTAL (sum the ratings and divide by 5)	

Startup	*Diligence*	*Typical*	*Excellent*	*Best*
1	1	2	7	10

9.4.6 Roll-up

Area	*Rate*	*Level*	*Startup*	*Diligence*	*Typical*	*Excellent*	*Best*
Deter			0	2	3	6	9
Prevent			1	5	6	7	9
Detect			0.2	5	4	7	9.5
React			1	5	6	7	9
Adapt			1	1	2	7	10
TOTAL / 5			0.7	3	4.2	6.8	9.2

Enter ratings from above and divide by 5 for the total. Rate each area's level by selecting the highest level not exceeding the rating.