Best Practices - Actions

BP-Actions

ACTIVITIES

- 2-3 word phrase for each Best Practice
  - ❑Your words
  - ❑Other’s words
  - ❑Dean’s words
- Matching old & new
  - ❑800-27 to 800-160
  - ❑Is it possible
- LAST Exercise- SP800 analysis

WHY

- You have 100 -150 exam questions
- How do you filter each question down quickly?
- To pass you must stay in the best practices = managerial mode
- You need a practice that is NOT Security & Technology
  - But still includes global concepts, analysis, and best practices
  - Keeping you out of your experiences
- Something you can do after this session
- Spot the other way to say term (SYNONYM GAME)

TOOLS YOU NEED

- Download from my github
  - □ [800-27.pdf]
  - □ [BP-activity-800-160vol2.pdf]
- OR
  - □ Google sheet first 2 tabs
- Advanced practice
  - □ Relate 800-160 term to current BP

Practice- Integrity

	How do you say it 2-3 words	= 800-160?
1	GS:Unaltered information	
2	Information Assurance	broad
3	accuracy	
4	M G: validated reliable information	
5	PRevent unauthorized modification	
6	Pure/ precise/ true	

Practice- Availability

	How do you say it 2-3 words	= 800-160?
1	USABLE DATA	
2	Easy Access	
3	UPTIME	
4	CONTINUITY	
5	ANT:NO INTERRUPTIONS	
6		

Practice- Confidentiality

	How do you say it 2-3 words	= 800-160?
1	Secret	
2	Restricted Access	
3	Not disclosed	
4	right eyes only	
5	compartmentalized	
6		

Establish a sound security policy as the "foundation" for design

	How do you say it 2-3 words	= 800-160?
1	SDLC	
2	~~Covers main issues~~	
3	?	
4	Easy? to apply	
5	Convey Architecture Protections	
6	Policy Drives Design	

Treat security as an integral part of the overall system design

	How do you say it 2-3 words	= 800-160?
1	Secure from start	
2	Security by Design	
3	BAKE IN SECURITY	
4	? common criteria ITSEC / SecDevOps / bottom up method?	
5		
6	Security by Design	

Clearly delineate the physical and logical security boundaries governed by associated security policy

	How do you say it 2-3 words	= 800-160?
1	Security Perimeter Policy	
2	MAKE CLEAR RULES	
3	*TAILORED* SECURITY POLICY	
4	FAIL SECURE	
5	? define scope in policy/Mandatory access control/~~Administrative Controls~~	
6	Isolate on boundaries	

Ensure that developers are trained in how to develop secure software

	How do you say it 2-3 words	= 800-160?
1	SECURITY SKILLED DEVELOPERS	
2	STRIDE / DREAD/ OWASP	
3		
4	Secure Coding	
5		
6	Secure coding practices	

Reduce risk to an acceptable level

	How do you say it 2-3 words	= 800-160?
1	Risk Tolerance Identified	
2	risk management	
3	risk appetite	
4	Security that makes sense	
5	Transfer = insurance/ ~~Regulation required level~~ / risk mitigation / Avoid	
6	Management's Risk appetite	

Assume that systems are insecure

	How do you say it 2-3 words	= 800-160?
1	Zero trust	
2	Assume breach	
3	When, not if	
4		
5	Security through Obscurity / **Potential Vulnerability**	Hug your system
6	Zero Trust Policies	

IDENTIFY TRADE-OFFS BETWEEN REDUCING RISK, INCREASED COSTS, DECREASE OPERATIONAL EFFECTIVENESS

	HOW DO YOU SAY IT 2-3 WORDS	= 800-160?
1	RISK ANALYSIS	
2	PRUDENT MANAGEMENT	
3	NOTHING IS FREE	
4	BALANCED RISK OPERATIONS	
5	JUSTIFIED TOLERANCE	
6	COST OF ASSET > MITIGATION	

Implement tailored measures to meet security goals

	How do you say it 2-3 words	= 800-160?
1	Just enough Security	
2	targeted security controls	
3	Adapted best practices	
4	Customized security solutions	
5	reduce cost / Bespoke Policies / Tailoring and Scoping	
6		

Protect information in process, in transit, in storage (Encryption)

	How do you say it 2-3 words	= 800-160?
1	Secure Data Everywhere	
2	Ensure confidentiality	
3	Data Security	
4	secure at every stage	
5	? ~~chain of custody~~ / **Whole Disk Encryption / DLP**	
6		

CONSIDER CUSTOM PRODUCTS TO ACHIEVE SECURITY

	HOW DO YOU SAY IT 2-3 WORDS	= 800-160?
1	COMMON CRITERIA	
2	BESPOKE DEVELOPMENT	
3	CUSTOMIZED SECURITY	
4	BUSINESS SECURITY DEMAND	
5	? COTS	
6		

Protect against all likely classes of attacks

	How do you say it 2-3 words	= 800-160?
1	THREAT RESILIENCE	
2	*Threat Modelling Result*	
3		
4		
5	? Layered Protection / Control diversity / system hardening / SOC	
6	RISK MITIGATION	

Base security on open standards for portability and interoperability

	How do you say it 2-3 words	= 800-160?
1	Minimal Customization	
2	useful secure products	
3	No Security by Obscurity	
4	Security Compliance	
5	? ~~Use accepted best practices~~ / Elasticity=cloud	
6		

Use common language in developing requirements

	How do you say it 2-3 words	= 800-160?
1	Common Criteria	
2	ITIL - Process	
3	OCTAVE - RISK	
4	SABSA / TOGAF	
5		
6		

Design for regular adoption of new including upgrading process

	How do you say it 2-3 words	= 800-160?
1	ITIL	
2	Flexible	
3	Future proof	
4	CMMI	
5		
6	Change Mgt	

Operational ease of use

	How do you say it 2-3 words	= 800-160?
1	Customer - User friendly	
2	?Internal SecDevOps	
3	Operational Efficiency	
4	User Acceptance	
5	? Training / Automation	
6		

Implement layered security (Defense-in-Depth)

3 cat or types of controls - NO examples

	How do you say it 2-3 words	= 800-160?
1	1) Preventative (2) Detective (3) Corrective Recovery, Deterrent,	
2	Admin / Tech / Phy	
3	Locks - physical, IDS technical, police-admistrative	
4	Compensating = META	
5		

Limit vulnerabilities and be resilient

	How do you say it 2-3 words	= 800-160?
1	Risk Management	
2	Recovery	
3		
4		
5	Continuous monitoring, Periodic review, Hardening, Change Mgmt	
6		

PROVIDE ASSURANCE SYSTEM IS RESILIENT IN FACE OF THREAT

	How do you say it 2-3 words	= 800-160?
1	Survivable Recoverability	
2	Trusted recovery	
3	Redundant	
4	How: Harden	
5	FAIL SECURE FAIL OPEN	
6	OVER TIME Recoverability	

Limit or contain vulnerabilities

	How do you say it 2-3 words	= 800-160?
1	Mitigate / Remediate	
2	patch	
3	Quarantine = compromised host	
4		
5	Lockdown = Isolation / STIG= configure (not patch) - CISECURITY.ORG	
6		

Isolate public systems from mission critical

	How do you say it 2-3 words	= 800-160?
1	Boundary / DMZ	
2	Proxy Server	
3		
4	? ~~Enclaves~~/ process	
5	? VLAN/ Load balance / Zone	
6	Domain	

USE BOUNDARY MECHANISMS TO SEPARATE COMPUTING AND NETWORK

	HOW DO YOU SAY IT 2-3 WORDS	= 800-160?
1		
2		
3		
4		
5		
6		

Audit mechanisms to detect unauthorized use and to support incident investigations

	How do you say it 2-3 words	= 800-160?
1	Monitoring Logs	
2	___Logs	
3	SIEM	
4	Forensics = law	
5		
6		

Develop and exercise contingency procedures for availability.

	How do you say it 2-3 words	= 800-160?
1		
2		
3		
4		
5		
6		

STRIVE FOR SIMPLICITY.

	HOW DO YOU SAY IT 2-3 WORDS	= 800-160?
1		
2		
3		
4		
5		
6		

Minimize elements to be trusted

	How do you say it 2-3 words	= 800-160?
1		
2		
3		
4		
5		
6		

IMPLEMENT LEAST PRIVILEGE

	How do you say it 2-3 words	= 800-160?
1		
2		
3		
4		
5		
6		

Do not implement unnecessary security mechanisms

	How do you say it 2-3 words	= 800-160?
1		
2		
3		
4		
5		
6		

Ensure proper security in shutdown or disposal

	How do you say it 2-3 words	= 800-160?
1		
2		
3		
4		
5		
6		

IDENTIFY AND PREVENT COMMON ERRORS AND VULNERABILITIES.

	HOW DO YOU SAY IT 2-3 WORDS	= 800-160?
1		
2		
3		
4		
5		
6		

Implement security controls physically and logically

	How do you say it 2-3 words	= 800-160?
1		
2		
3		
4		
5		
6		

FORMULATE MEASURES TO ADDRESS MULTIPLE OVERLAPPING INFORMATION DOMAINS

	HOW DO YOU SAY IT 2-3 WORDS	= 800-160?
1		
2		
3		
4		
5		
6		

Authenticate to ensure appropriate access control

DECISIONS

	How do you say it 2-3 words	= 800-160?
1		
2		
3		
4		
5		
6		

Use unique identities to ensure accountability

	How do you say it 2-3 words	= 800-160?
1		
2		
3		
4		
5		
6		

LAST FEW

- Lifecycle – SDLC – 5 steps

COLLECT YOUR WORDS RECOGNIZE / ANALYZE IN SP

- Download & open as we go

Executive summary SP800-113

	BP terms	Page/ Parg.
1		
2		
3		
4		
5		
6		

Executive summary SP800-115

	BP terms	Page/ Parg.
1		
2		
3		
4		
5		
6		

Executive summary SP800-30

	BP terms	Page/ Parg.
1		
2		
3		
4		
5		
6		

Executive summary SP800-35

	BP terms	Page/ Parg.
1		
2		
3		
4		
5		
6		

Executive summary SP800-40

	BP terms	Page/ Parg.
1		
2		
3		
4		
5		
6		

Executive summary SP800-49

	BP terms	Page/ Parg.
1		
2		
3		
4		
5		
6		

Executive summary SP800-51

	BP terms	Page/ Parg.
1		
2		
3		
4		
5		
6		

Executive summary SP800-55

	BP terms	Page/ Parg.
1		
2		
3		
4		
5		
6		

EXECUTIVE SUMMARY SP800-60

	BP TERMS	PAGE/ PARG.
1		
2		
3		
4		
5		
6		

Executive summary SP800-61

	BP terms	Page/ Parg.
1		
2		
3		
4		
5		
6		

Executive summary SP800-64

	BP terms	Page/ Parg.
1		
2		
3		
4		
5		
6		

Executive summary SP800-70

	BP terms	Page/ Parg.
1		
2		
3		
4		
5		
6		

Executive summary SP800-94

	BP terms	Page/ Parg.
1		
2		
3		
4		
5		
6		

Executive summary SP800-97

	BP terms	Page/ Parg.
1		
2		
3		
4		
5		
6		

THANK YOU

Questions