CIS CRITICAL SECURITY CONTROLS

BY

MELANIE MCKEAN
CHRISTOPHER ROBINSON

Acknowledgements

Jeopardy presentation slides provided by:
Educational Technology Network. www.edtechnetwork.com 2009

Answers and Questions extracted from:
SANS Implementing and Auditing the Critical Security Controls – In Depth

Companies that appear within questions of this presentation are included as an example of why an organization should implement these controls. It is generally not the case that these companies engaged in gross negligence or did not know the right thing to do.

In General	Guiding Principles	Devices and Software	Secure Configurations	Vulnerability Assessment
100	100	100	100	100
200	200	200	200	200
300	300	300	300	300
400	400	400	400	400
500	500	500	500	500

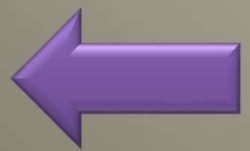
In General– 100 Points

Answer:

This council is the official home of the Critical Security Controls.

Question:

What is the Council on CyberSecurity?



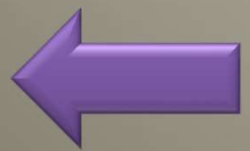
In General– 200 Points

Answer:

These are the three families in which the controls are listed.

Question:

What is System, Network, and Application?



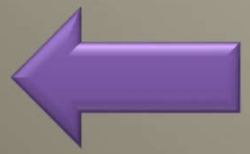
In General– 300 Points

Answer:

This is the order by which the critical security controls are listed.

Question:

What is priority?



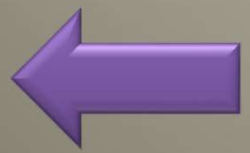
In General– 400 Points

Answer:

Appendix B of the APT1 report describes this.

Question:

What is the average lifecycle of an advanced or dedicated attack against a company?



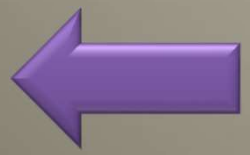
In General– 500 Points

Answer:

This threat model is distributed by the Center for Internet Security with contributions from over 150 different international organizations.

Question:

What is The Open Threat Taxonomy (OTT)?



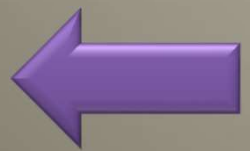
Guiding Principles– 100 Points

Answer:

•According to the guiding principles, defenses should focus on this.

Question:

•What are the most common and damaging attack activities occurring today, and those anticipated in the near future?



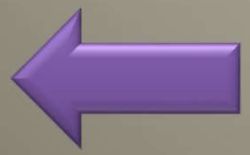
Guiding Principles– 200 Points

Answer:

•According to the guiding principles, enterprise environments must ensure this in order to effectively negate attacks.

Question:

•What is consistent controls across an enterprise?



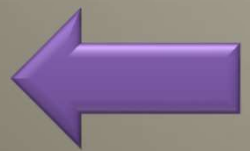
Guiding Principles – 300 Points

Answer:

- According to the guiding principles, defenses should include these two activities.

Question:

- What is automation and periodic or continuous measurement?



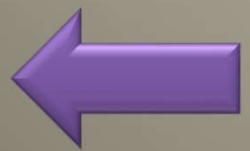
Guiding Principles – 400 Points

Answer:

- According to the guiding principles, a variety of these type of activities should be used to address current attacks occurring on a frequent basis against numerous organizations.

Question:

- What are technical activities?



Guiding Principles – 500 Points

Answer:

- According to the guiding principles, these should be established to provide a common language to communicate about risk.

Question:

- What are measures?

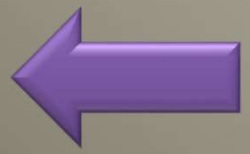
Devices and Software – 100 Points

Answer:

This can be deployed to ensure that only **authorized applications** are allowed to execute.

Question:

What is application whitelisting?



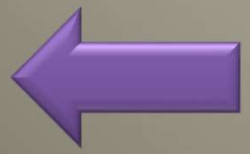
Devices and Software – 200 Points

Answer:

This company was breached due to an insecure version of Oracle Java running on internal workstations.

Question:

Who is Facebook?



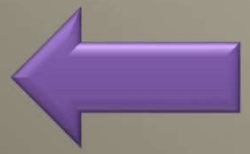
Devices and Software – 300 Points

Answer:

This whitelisting vendor was breached due to the fact that they did not install controls on machines that were not in their inventory.

Question:

Who is Bit9?



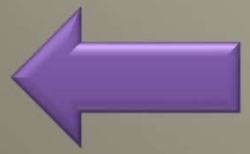
Devices and Software – 400 Points

Answer:

This is an attack tool that provides a graphical front end to many common attack tools, most importantly to Metasploit.

Question:

What is Armitage?



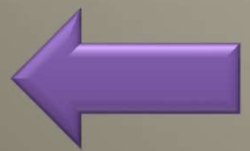
Devices and Software – 500 Points

Answer:

New devices and software should detected within this time frame.

Question:

What is 24 hours?



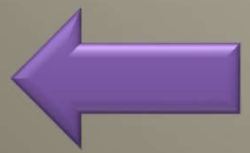
Secure Configurations – 100 Points

Answer:

These should be established for your operating systems and software applications.

Question:

- What are standard secure configurations?



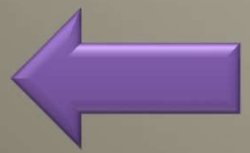
Secure Configurations – 200 Points

Answer:

This is a possible location where master images could be stored.

Question:

What is offline machines, air-gapped from the production network?



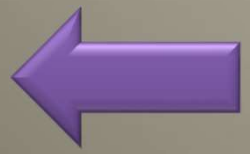
Secure Configurations – 300 Points

Answer:

These two organizations website credentials were stolen due to poor configuration of the hashing mechanism.

Question:

Who are LinkedIn & eHarmony?



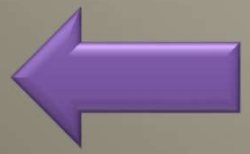
Secure Configurations – 400 Points

Answer:

This Windows command line utility can be automated or scripted to help with the implementation of this control.

Question:

What is WMIC or Windows Management Instrumentation Command-line?



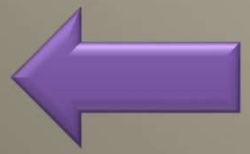
Secure Configurations – 500 Points

Answer:

An unauthorized configuration change should be blocked/quarantined within this amount of time when detected.

Question:

What is an hour?



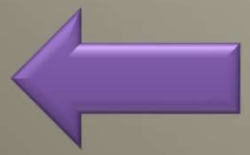
Vulnerability Assessment – 100 Points

Answer:

A vulnerability scanner should look for these two types of vulnerabilities.

Question:

What are code-based and configuration-based?



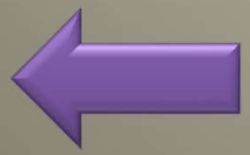
Vulnerability Assessment – 200 Points

Answer:

This can be done to keep vulnerability scanners up-to-date with the latest vulnerabilities.

Question:

What is subscribe to vulnerability intelligence services?



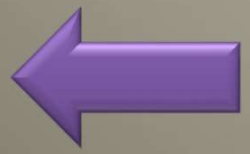
Vulnerability Assessment – 300 Points

Answer:

This organization was exploited by targeting a flaw in Internet Explorer 6 SP1. The malware used in this attack was later named “Operation Aurora”.

Question:

Who is Google?



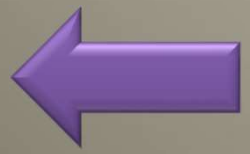
Vulnerability Assessment – 400 Points

Answer:

This protocol was developed to scan information systems in a standard way.

Question:

What is Security Content Automation Protocol (SCAP)?



Vulnerability Assessment – 500 Points

Answer:

The two most common SCAP protocols for measuring weaknesses identified during vulnerability scanning.

Question:

What are Common Vulnerability Scoring Systems (CVSS) and Common Configuration Scoring System (CCSS)?