



Policy-Based Controls

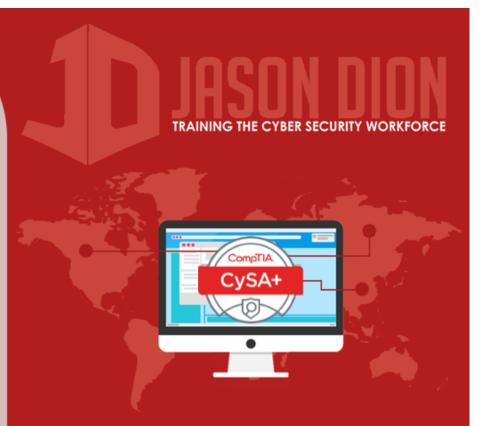
Security Architecture & Tool Sets

Policy-Based Controls

 Policies provide the control objectives the organization wants to achieve

 This is the desired end state, not the method or activities to accomplish them

- Security controls are used to achieve the control objectives
 - Physical Controls
 - Logical Controls
 - Administrative Controls



Physical Controls

Controls that impact the physical world

Examples:

• Fences, gates, locks, lighting, alarm systems, fire suppressions systems, etc.







Logical Controls

 Technical controls to enforce confidentiality, integrity, and availability

Examples:

ACLs in firewalls and routers, encryption schemes





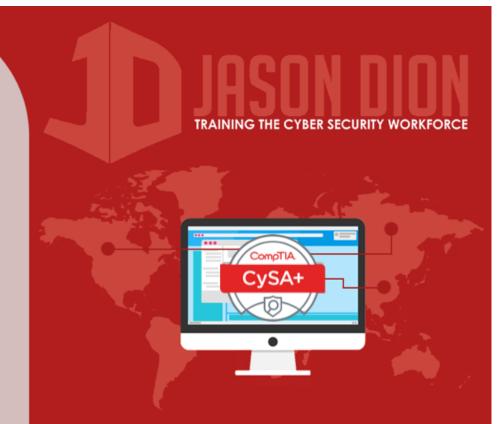
Administrative Controls

 Procedural controls to implement good cybersecurity practices

Examples:

 Separation of duties, background checks, reviewing of log files, etc.

•	9 '	,	0.0.			
LogTime	Computer	Protocol Type	Source IP	Destination IP	Access type	Attack
11.16/2015 03:14:30 PM	CISCO-ASA	UDP	182 72 211 60/35445	192.163.2.34/467	interface interface_name	
11.16/2015 03:14:30 PM	CISCO-ASA	UDP	182 72 211 .61/789	192.168.1.26/233		
11.16/2015 03:14:30 PM	CISCO-ASA				for iomp	
11.16/2015 03:14:30 PM	CISCO-ASA	UDP	182 72 211 .60/35445	192.163.2.34/467	interface interface_name	
11.16/2015 03:14:30 PM	CISCO-ASA				for icmp	
11.16/2015 03:14:30 PM	CISCO-ASA	UDP	182 72.211.61/789	192.188.1.26/233		
11.16/2015 03:14:30 PM	CISCO-ASA	UDP	182 72 211.61/789	192.188.1.26/233		
11:16/2015 03:14:31 PM	CISCO-ASA	CVP	10.4.1.2	10 2.1.1	interface druz	
****8/2015 03:14:31 PM	CISCO-ASA	UDP	10.1.1.1	192.183.1.1	interface outside	Snork attack
11:16/2015 03:14:31 PM	CISCO-ASA	ICMP	10.4.1.2	10 2.1.1	interface druz	
11:16/2015 03:14:31 PM	CISCO-ASA	UDP	10.1.1.1	192.163.1.1	interface outside	Snork attack
11:16/2015 03:14:31 PM	CISCO-ASA	CMP	10.4.1.2	10.2.1.1	interface driz	
11:16/2015 03:14:31 PM	CISCO-ASA	UDP	10.1.1.1	192.163.1.1	interface outside	Snork attack
11:16/2015 03:14:31 PM	CISCO-ASA	CVP	10.4.1.2	10.2.1.1	interface driz	
11.16/2015 03:14:31 PM	CISCO-ASA	UDP	10.1.1.1	192.163.1.1	interface outside	Snork attack
11:16/2015 03:14:31 PM	CISCO-ASA	CMP	10.4.1.2	10.2.1.1	interface druz	
11:16/2015 03:14:31 PM	CISCO-ASA	UDP	10.1.1.1	192.163.1.1	interface outside	Snork attack
11.16/2015 03:14:31 PM	CISCO-ASA	UDP	10.1.1.1	192.168.1.1	interface outside	Snork attack
11.16/2015 03:14:31 PM	CISCO-ASA	UDP	10.1.1.1	192.163.1.1	interface outside	Snork attack
11.16/2015 03:14:31 PM	CISCO-ASA	CMP	10.4.1.2	10 2.1.1	interface druz	
11.16/2015 03:14:31 PM	CISCO-ASA	CVIP	10.4.1.2	10 2.1.1	interface druz	



Combining Control Objectives

 Physical, Logical, and Administrative controls are most effective when they are combined together

Example:

- To prevent theft of the data from a server
 - Physical controls for building access
 - Logical controls like encryption
 - Administrative controls like requiring two people

