Applying Strategic Thought to Digital Security

Richard Bejtlich
@taosecurity

Traditional Security

Board and CEO

CEO/CIO

⇧

Budget Requests
Security Briefings

CISO or
security director

Tactics

Security staff

⇩

Tools

Vendors

FireEye™

Program Goals

Board and CEO

Minimize loss due to intrusions

CEO/CIO

CISO or security director

Tactics

Security staff

⇓

Tools

Vendors

FireEye

Program Goals	Board and CEO	Minimize loss due to intrusions
⬇		
Strategies	CEO/CIO	
		Rapid detection, response, and containment
	CISO or security director	
Tactics		
⬇	Security staff	
Tools	Vendors	

FireEye

Program Goals	Board and CEO	Minimize loss due to intrusions
⇩		
Strategies	CEO/CIO	
⇩		Rapid detection, response, and containment
Operations/Campaigns	CISO or security director	
⇩		Match and hunt for intruders
Tactics	Security staff	
⇩		
Tools	Vendors	

FireEye

Program Goals	Board and CEO	Minimize loss due to intrusions
⇩		
Strategies	CEO/CIO	
⇩		Rapid detection, response, and containment
Operations/Campaigns	CISO or security director	
⇩		Match and hunt for intruders
Tactics	Security staff	
⇩		Collect, analyze, escalate and resolve incidents
Tools	Vendors	

FireEye

Strategic Security 5 of 5

Program Goals   Board and CEO   Minimize loss due to intrusions

⇩

Strategies   CEO/CIO

⇩

Operations/Campaigns

Rapid detection, response, and containment

CISO or security director

⇩

Tactics

Match and hunt for intruders

Security staff

⇩

Tools   Vendors

Collect, analyze, escalate and resolve incidents

Various software

FireEye™

Thank you

- The Practice of Network Security Monitoring
  - Published July 2013
  - www.nostarch.com/nsm
  - 30% of with code **NSM101**
- Network Security Monitoring 101
  - Black Hat Training
  - www.blackhat.com
  - December 8-9
  - Near Washington, DC
- Contact
  - @taosecurity
  - Richard.Bejtlich@fireeye.com
  - taosecurity.blogspot.com

8