NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Planning for the (Un)expected

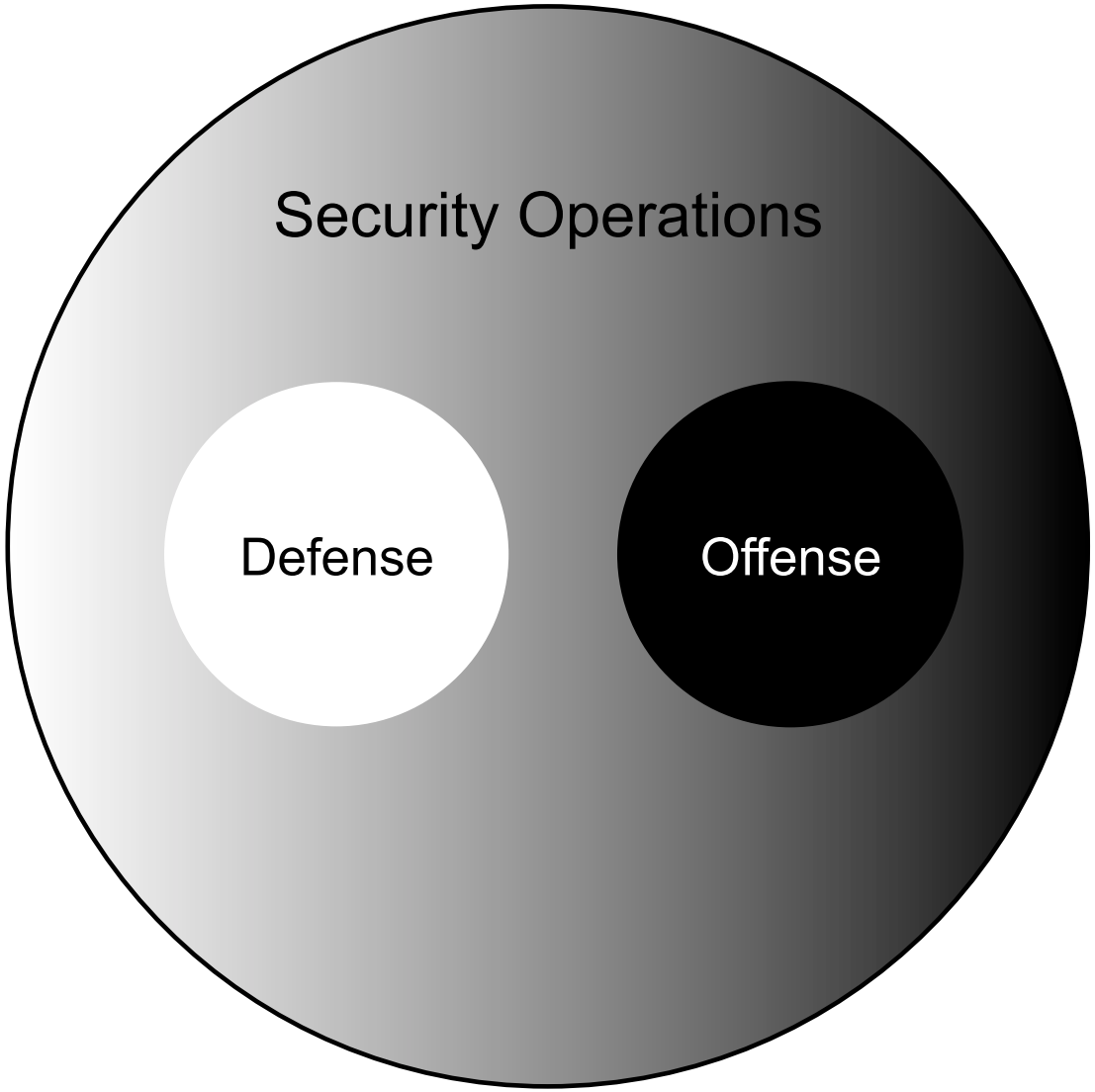
Ben.miller@nerc.net

4/19/2012

RELIABILITY | ACCOUNTABILITY




Premise



"**Security Operations**" is how I refer to the idea that both offensive and defensive teams are in a constant competition. IMO, it's a good working mental model for defenders.

Characteristics of a good plan

- Creates a common language and understanding among various teams
- Creates possibilities, doesn't reduce them
- Creates "knowledge" to feed into your Risk Mgmt program

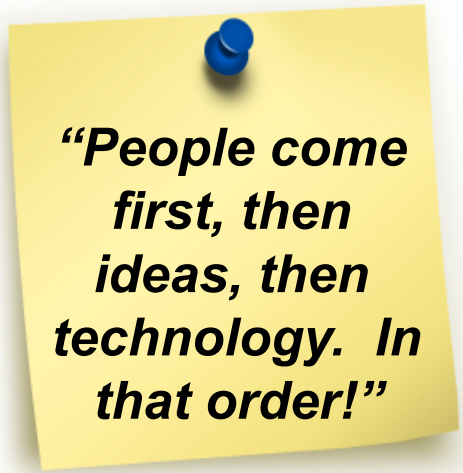
Learning

• Technical

- On The Job Training
  - Mentorship
  - Data Pivoting and Root Cause Analysis
- Drills
  - Technical Challenges (competition, or co-op CCTF)
  - Case Studies
- Books and Blogs
  - Both a physical and virtual bookshelf
- Conferences
  - Hacker Cons
  - Security Training
  - Security Conferences

• Procedural

- Case Study
  - Historical
  - What If?
  - Multi-party
- Table Top Exercise (TTX) Scenario



Structure of a TTX :: Structure of a Broadway Play

Moves -> Acts

Events -> Scenes

Injects -> Dialog

Roles in a TTX include:

- **Players** representing their team
- **Facilitators** to 'narrate' and guide the moves
- "**White cell**" to represent other teams as needed
- **Observers** who simply watch the scenario play out

Designing

An ideal design team will:

- Use an Attacker Mindset
- Represent each player team accurately
- Create appropriate injects and accurate back story
- Have excellent presentation and polish

Date Time	Event	Evidence / Artifacts/Potential Injects
4/15/11 13:41	Attacker A uses google searches to locate a series of employee email addresses	Screenshots of google hits
4/16/11 08:41	Attacker A sends a crafted phishing message to the identified email addresses	SMTP email gateway logs
4/16/11 8:45	Victim B erroneously clicks malicious link / successfully compromises PC “DougH”	HTTP gateway log Windows prefetch entry File: C:\windows\tasks\svchost.exe
4/16/11 8:46	PC “DougH” establishes C2 with example1.dyndns.org: 443	HTTP gateway log
4/16/11 8:46	PC “DougH” downloads p.zip from rapidshare.com/	HTTP gateway log File: c:\windows\tasks\p.zip c:\windows\tasks\p.exe
4/16/11 8:46	PC “DougH” executes p.exe (pwdump) and transfers results via FTP to example2.dyndns.org	Windows prefetch entry

Example MSEL

	Move 3			
	3.1		3.2	
	Game Time: Wed 7am-Noon	Real Time: 60 minutes	Game Time: Wed Noon-5pm	Real Time: 45-60 minutes
Scenario Description	Incident closing actions Facilitators should be alert to poor communications at this point. Did each team keep a clear log of events for post-incident analysis?		Post incident analysis and reporting (NERC, etc) Facilitators should be alert to poor communications at this point. Did each team keep a clear log of events for post-incident analysis? Do the teams begin their own post-op debrief? Facilitators should push for communications between groups Groups create their post-incident reports to deliver to the group.	
Injects	3.1-03 – ITC		None	
On Demand Injects	3.1-04a – SA 3.1-05a – SA			
Ad Hoc Injects	N/A			

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Example MSEL #2

EXPECTED PLAYER ACTIONS		
	Move 3.1	Move 3.2
IT – Corporate (IT-C)	Rewrite firewall rules to prevent ICMP outbound Order a review of all firewall rules, and tighten them up	Prepare a post-incident report for management Should communicate with other teams to get a picture of the whole incident
Management (M); Incident Response; Physical Security	Direct rebuild of appropriate systems Direct firewall reviews and changes Recognize the extension of the network into the field, and the need for appropriate physical controls to match electronic controls Recognize need for alarms on Sub-stations Understand relationship between Physical Sec and IT Sec, and formulate training program accordingly	Prepare a post-incident report for X, Y, Z if appropriate Prepare a post-incident report for Sr Management Should communicate with other teams to get a picture of the whole incident Prepare post-incident report for the rest of the groups

Sample Move

Move 1.1

Tuesday, 22 November, 0000 hrs Eastern through Wednesday, 30 November, 2359 hrs Eastern

- General Media
  - Widespread electrical outage in Brazil reported due to network infiltration at Empresa de Pesquisa Enrgetica covered by CNN, BBC, and other major news sources
  - News Interviews:
    - Senator X pledges to introduce tough new security regulations for "smart grid" technology to "ensure the US doesn't end up like Brazil, where they can't even keep the lights on."
    - Senator X claims over-regulation creates bureaucratic confusion in Brazilian power transmission industry, resulting in the failure.
- Weather
  - Temps: Lows in the high 20s; Highs in the mid 30s
  - Outlook: Large winter storm forming in the West expected to impact the Great Lakes region early this week.

Example Inject

EXERCISE EXERCISE EXERCISE

Inject: 1.2-10a
Received by: IT– ON DEMAND ONLY (This inject will be presented on demand in move 1.2, or on schedule in move 2.1 if it has not already been distributed)

Communication Server has modified settings

After checking the X Communication Server for slow response times, the administrator finds some anomalies.

- The system log files show many invalid login attempts for the Administrator account between 24 and 18 hours ago
- Processors appear to be running about 8% higher than normal, but that is just a "gut feel" on the part of the administrator – the processor load is within the normal range.

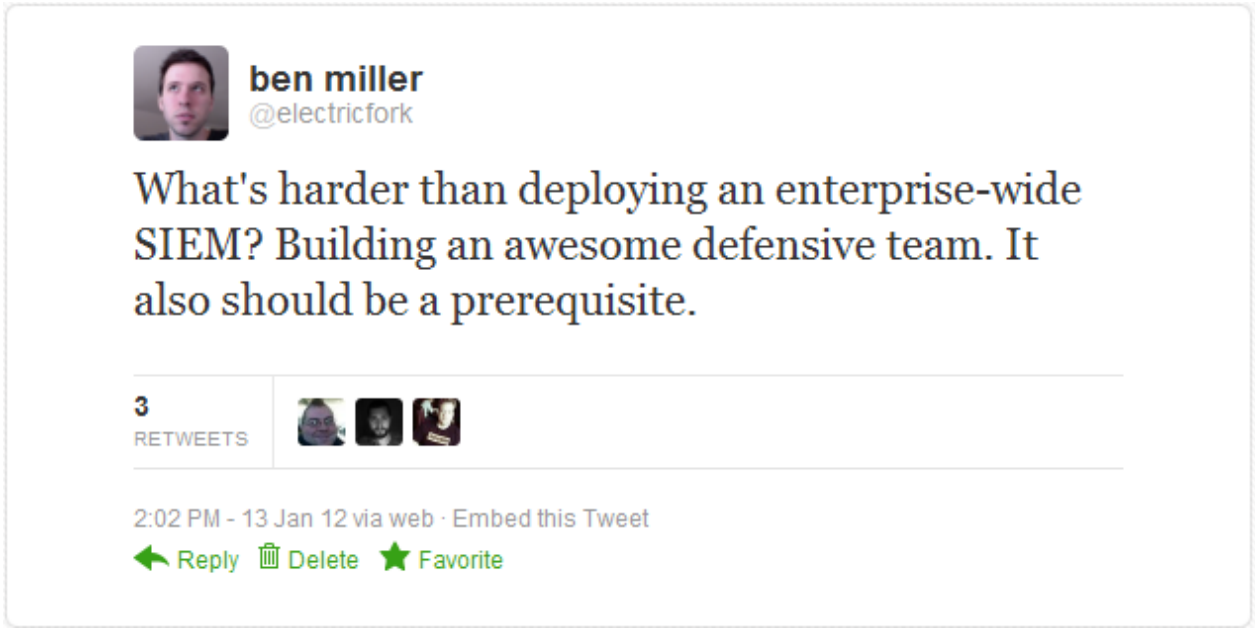
Otherwise, the process list looks normal, and the network stack appears normal.

EXERCISE EXERCISE EXERCISE

Example Agenda for a TTX

- 0830 – 0845 Breakfast, Opening Remarks and Introductions
- 0845 – 0915 Exercise Overview and In-brief
- 0915 – 0945 Move 0
- 0945 – 1030 Move 1
- 1030 – 1045 Break
- 1045 – 1230 Move 2
- 1230 – 1300 Lunch
- 1300 – 1445 Move 2 cont'd
- 1445 – 1500 Break
- 1500 – 1530 Move 3
- 1530 – 1615 Overview of Exercise from an attacker perspective
- 1615 – 1630 Open Discussion and Observations
- 1630 – 1700 Close out of exercise

Thank You


ben miller
@electricfork
What's harder than deploying an enterprise-wide SIEM? Building an awesome defensive team. It also should be a prerequisite.
3
RETWEETS
2:02 PM - 13 Jan 12 via web · Embed this Tweet
Reply
Delete
Favorite

~
~
~
:wq