

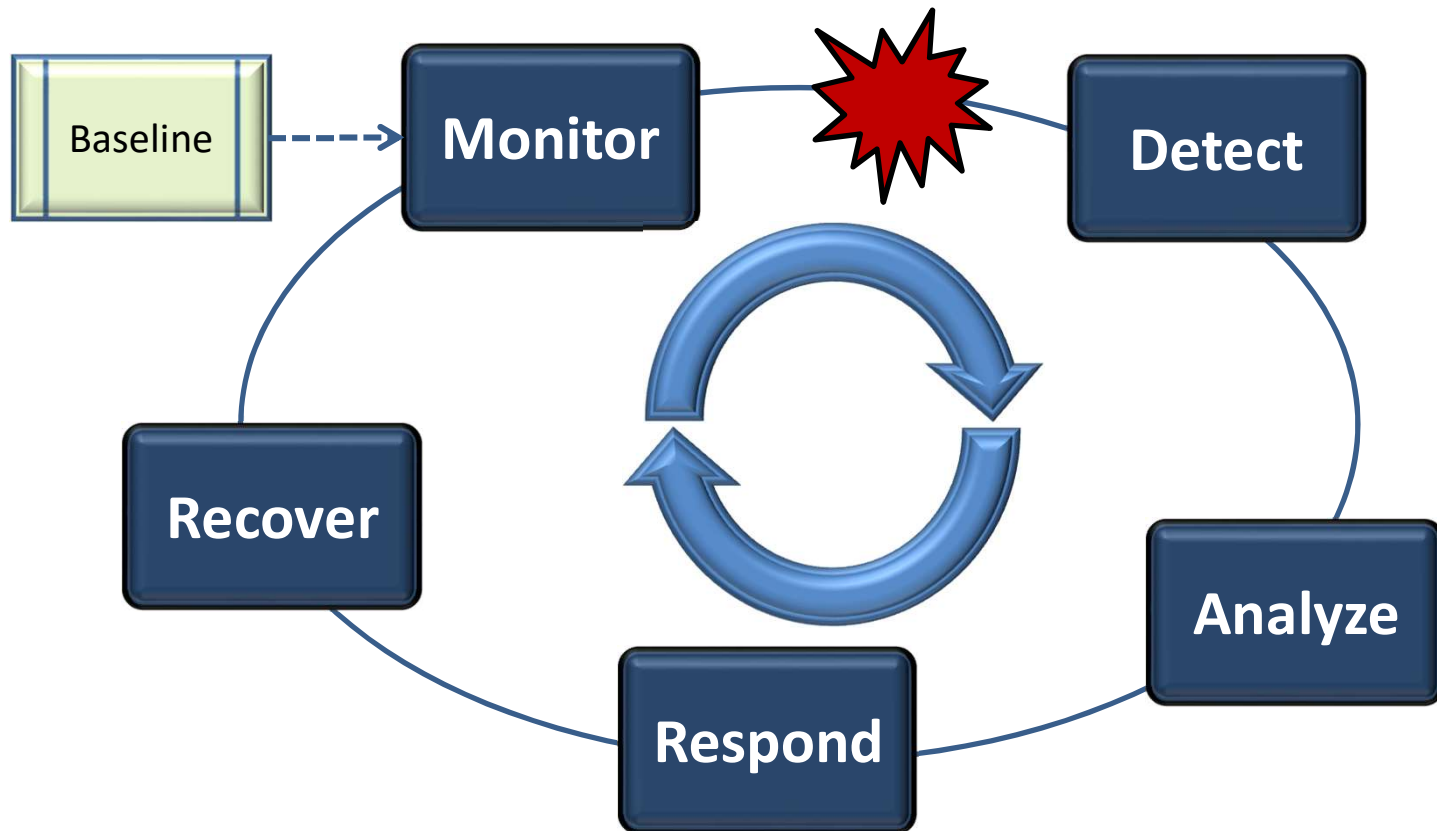


Overview

- The Secure Operations Framework
- Establishing a Baseline
- Monitoring & Detecting Attacks
- Analyzing Attacks
- Responding to & Recovering from Attacks
- Prioritizing Actions

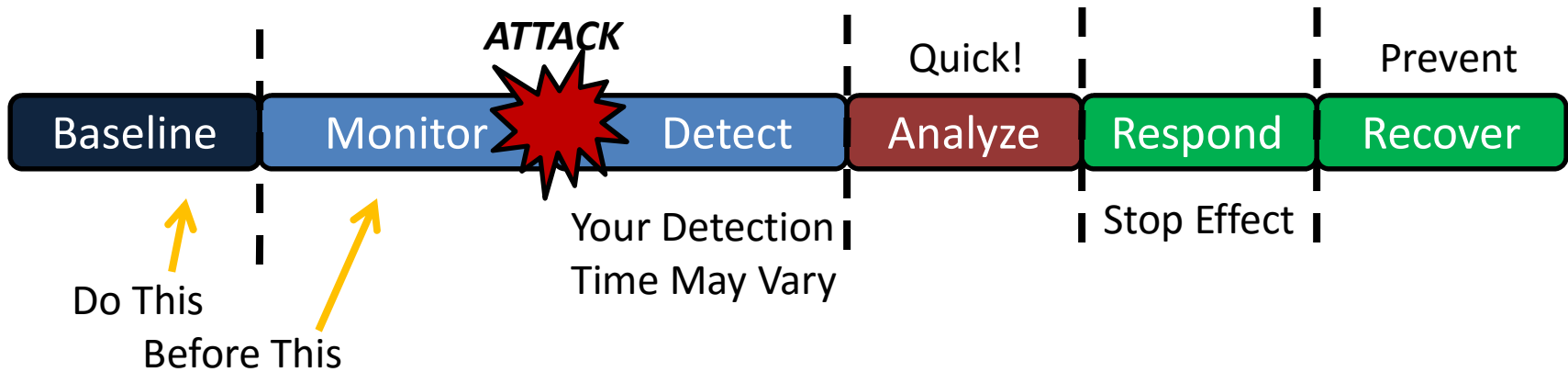
Secure Operations Framework

- A Process for Conducting Secure Operations Within Your Registry



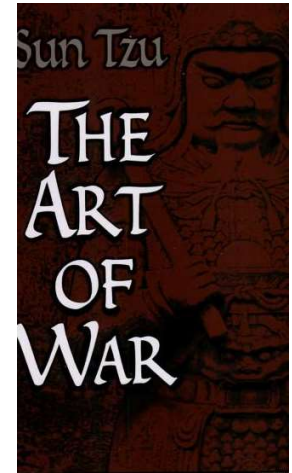
Secure Operations Framework

- Viewed as a Timeline:



Establishing a Baseline

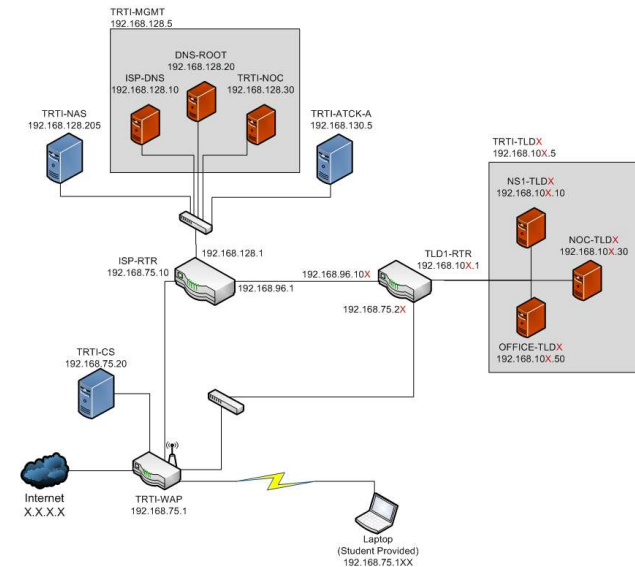
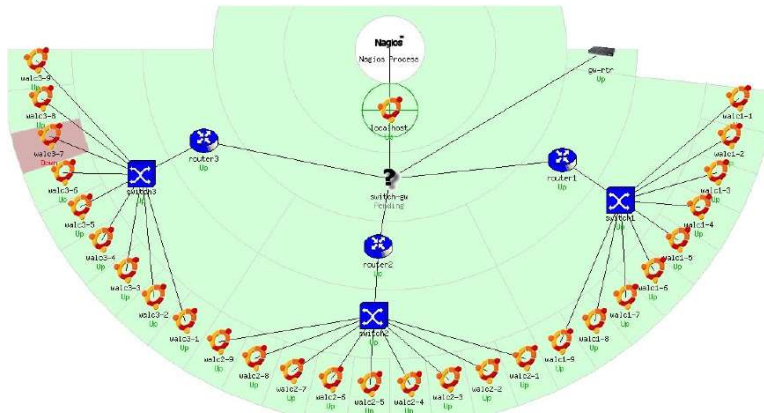
“If you **know the enemy** and **know yourself** you need not fear the results of a hundred battles”



- Secure Operations BEGIN with an understanding of your network -> a Baseline!
- To Establish a Baseline – You Need to Understand:
 - Architecture
 - Traffic
 - People
 - Processes
 - Vulnerabilities

Establishing a Baseline

- Architecture Baseline
 - Hosts, Services, Ports, Connections, Addresses
- This is frequently a network architecture diagram, but could be a text document, or part of your network monitoring solution



Establishing a Baseline

- Architecture Baseline
 - Document your host configurations, operating systems, applications, versions, etc
- Ideally you want something you can reference quickly during attack analysis...
 - e.g. Can you quickly answer the question:

“Is my web server vulnerable to the latest Apache vulnerability?”



Establishing a Baseline

- Architecture Baseline Tools
 - Visio
 - Paper / Pencil!
 - NAGIOS, OpenNMS, HP Openview, etc
- Lots of tools available – the hardest part is actually doing it!



Establishing a Baseline

- Traffic Baseline
 - What kind, how much, source / destination, and usual time
- This is more difficult to capture but is critical to determining if something is expected or not

Establishing a Baseline

- External Traffic Baseline
 - How much traffic (packets per second, megabits per second, etc) is “normal” on your external links?
 - What kind of traffic to external servers (e.g. do you normally have SSH connections to your DNS servers?)
- Internal Traffic Baseline
 - Which hosts or applications communicate?
 - What protocols do they use?
 - How much traffic do they produce?
 - When do they do it?

Establishing a Baseline

- Traffic Baseline
 - Again, ideally, you will have this information readily available during the analysis phase
 - For example, can you easily answer the question:

“Is a SSH connection to my DNS server at 0330 on a Saturday normal?”

Establishing a Baseline

- Traffic Baseline Tools
 - NetFlow
 - Wireshark
 - Tcpdump
 - Iperf, dnsperf
- Again, lots of tools available, the hard part is not only capturing the baseline traffic, but putting it into a format you can reference
 - Graphing and statistical analysis tools can help here!
 - SmokePing, NetFlow Analyzer

Establishing a Baseline

- People Baseline
 - How do your customers interact with your network?
 - Web application for processing registration?
 - Do you typically see people login at 0330?
 - How do your administrators interact with your network?
 - What hosts do they connect to, what protocols do they use, when do they do it?
 - How do your local users interact with your network?
 - What hosts are they supposed to be on, what hosts do they communicate with, when?
 - How do your external users interact with your network?
 - What servers do they connect to, what protocols?

Establishing a Baseline

- People Baseline
 - Again, ideally, you will have this information readily available during the analysis phase
 - For example, can you easily answer the question:

“Should User Jane be Connecting to Users Bob’s Computer at 0330 on Saturday?”



Establishing a Baseline

- People Baseline “Tools”
 - Personnel Interviews
 - How does Bob usually do his job via the network?
 - Administration & User Policies
 - Set policy to guide your administrators and users in what they should and should not do
 - Understand Your Customers
 - How do you interact with your customers?
 - How do your customers interact with you?

Establishing a Baseline

- Processes Baseline
 - Processes typically fuse people and technology
 - Even though the people and technology may not have issues, the processes that pull them together might
 - Processes can be:
 - Business oriented (e.g. processing user registration updates)
 - Operational (e.g. responding to a DDoS attack)
- What processes do you have that interact with your network at one point or another?



Establishing a Baseline

- Process Baseline
 - Creating a baseline of your processes requires an understanding of what you do and how you do it!
 - Again, information should be readily accessible:
 - Can you easily answer this question:

“A new vulnerability was found in our database – what do we need to stop doing until it is patched?”



Establishing a Baseline

- Process Baseline “Tools”
 - Understand your critical business functions and what’s required to provide those functions
 - Walkthroughs & Reviews
 - Personnel Interviews & Surveys
 - See the “Attack & Contingency Planning Course”

Establishing a Baseline

- Vulnerability Baseline
 - Vulnerabilities in Operating Systems & Applications
 - Vulnerabilities in Your Business or Operational Processes
 - Processing registrations, responding to cyber attacks, etc
 - Vulnerabilities in Your People
 - Susceptible to phishing scams
- The procedural or people vulnerabilities are often easier to take advantage of:
 - e.g. do you require validation for updating registrations? Why hack the name server or registry database, when a simple “update” form would work?

Establishing a Baseline

Know Your Enemy...

- Vulnerability Baseline
 - To determine technical vulnerabilities, use automated tools
 - To determine procedural vulnerabilities, think like a “bad guy”
- You MUST make the risk decision on fixing vulnerabilities
 - You may determine that a vulnerability is an acceptable risk!
- Better that you KNOW about vulnerabilities than not
- Again, quick reference during analysis is critical:
 - e.g. Can you quickly answer the question:

“Can this attack take advantage of the vulnerability in our automated registry processing systems?”

Establishing a Baseline

- Vulnerability Baseline Tools
 - Nessus, LanGuard, SuperScan, Retina
 - Process Walkthroughs
 - Take each of your critical processes and step through them attempting to identify weaknesses
 - Network Defense Exercises
 - Test your network operators to determine how effective they are responding to cyber attacks
 - Can your operators see attacks, can they analyze and respond quickly?

Establishing a Baseline

- Other Sources of Baseline Information:



Senior Management



Business Area Managers & Process Owners



Technicians & Support Staff

- Important assets
- Perceived threats
- Security requirements
- Current security practices
- Organizational vulnerabilities

How Can Your Network Fail?

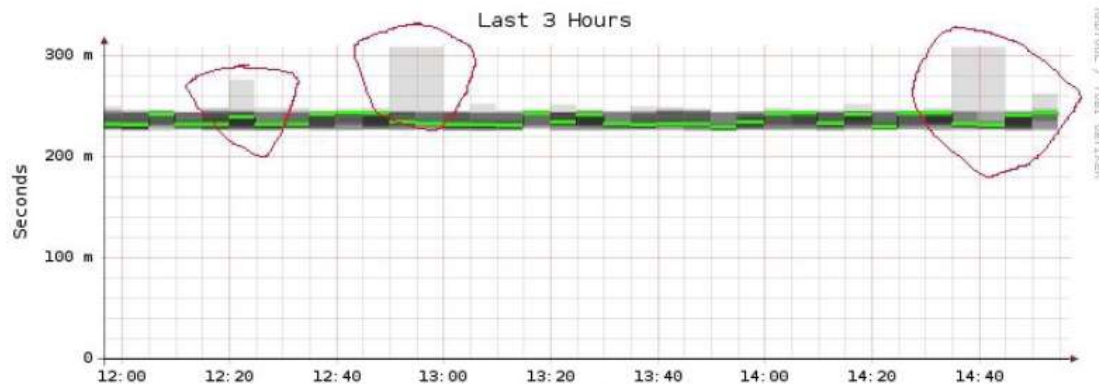
Monitoring & Detecting Attacks

Once You Have a Baseline –
You Can Differentiate “Normal” From “Trouble”

- Regardless of the monitoring tools you use, you ***MUST*** have a baseline to compare it to, otherwise, you are fighting blind

Monitoring & Detecting Attacks

- Monitoring is the notion of having insight into your network and viewing its current (and past) status and performance
- Detecting attacks requires monitoring your network and a comparison of what you see to what is expected



Monitoring & Detecting Attacks

- Network monitoring is best accomplished with automated tools – but can be done manually (not recommended!)
- You must install, configure and operate monitoring tools on your network - without them, how do you know something is happening?
 - Yes - phone calls from customers are a monitoring tool!
- There are many, many tools out there – the challenge is to find those that:
 - 1) Capture the right data
 - 2) Shows that data to you effectively
 - 3) Allows your operation to detect and respond to attacks
 - Personal preference plays a critical part in this – if you're not comfortable with a tool – there's probably another one!



Monitoring & Detecting Attacks

- The tools presented in this course, while not the only ones out there, are recommended for their particular task
- These tools were selected to give you the most “bang for the buck”
- Your particular operation may require something else
 - YOU must spend due diligence in selecting the right tools for your situation

Analyzing Attacks

- Analyzing an attack is the notion of gaining an understanding of what's going on and the extent of the attack
 - What critical business functions are affected
 - What hosts, applications, or services are affected
 - Who is doing it
 - What type of attack is it?
 - How is it being done?
- Arm yourself with the information necessary to develop an effective response to the problem



Responding to Attacks

- Based on your analysis from the previous step, take action!
- You DO have choices here:
 - Stop the attack -> Stops the effect
 - Stop the effect, but not the attack
 - Ride it out and suffer the effects
- Which strategy you chose depends on your response capabilities, your priorities, and your plan!

Responding to Attacks

- Your Plan? – You ***_DO_*** Have a Plan Right?
- Establishing basic actions prior to an attack will allow you to focus on response actions, not the determination of what to do...
- Your contingency response plans should include how to respond to cyber attacks!
 - See Attack & Contingency Response Planning

Responding to Attacks

- This course focuses on the technical response to attacks – but don't forget your customers, the media, and the public!
- Part of an effective response strategy must incorporate crisis communication procedures
 - Consider Communicating:
 - Fact of the disruption or status update
 - Basic steps being taken
 - Estimated impact or down time
 - See the Attack and Contingency Planning Workshop



Responding to Attacks

- The toughest job might be handling the media!



Recovering From Attacks

- Recovery steps are those taken after the attack is over, or at least the effects mitigated
 - Are there any lasting effects which need to be handled?
 - How would you prevent this from happening again?
 - What would you do differently next time?
- May make you reconsider risk decisions
 - Do we need to shut down that service permanently?
 - Do we need a new firewall?
 - Do we need to train our administrators to respond?

Prioritizing Actions

- Understand your critical business functions
- Understand the big picture of what's going on
- Take action based on responding and recovering what's most important to your business
 - Avoid “Building a \$10,000 fence around a stack of quarters”



Balancing Ops & Security

How Many of Your IT Positions are Dedicated to Security?

- You Need to Balance Daily Ops & Security
- A Recommendation – Make Security Part of Ops
- How Much Security you Do Depends on Your Situation?
 - Security is necessary – but is a black hole and will take *everything* you can give to it!
 - Tune your sensors to provide only the amount of information that you can handle – most sensors default to “overwhelm”
- Security Budgeting
 - Convince management of the risk through monitoring & analysis
 - Security takes a constant investment – roll this into your network admin costs when it comes to budget time

QUESTIONS?

- Do you have any questions about ...
 - Cyber Threats
 - Motivations
 - Remediation Strategies

