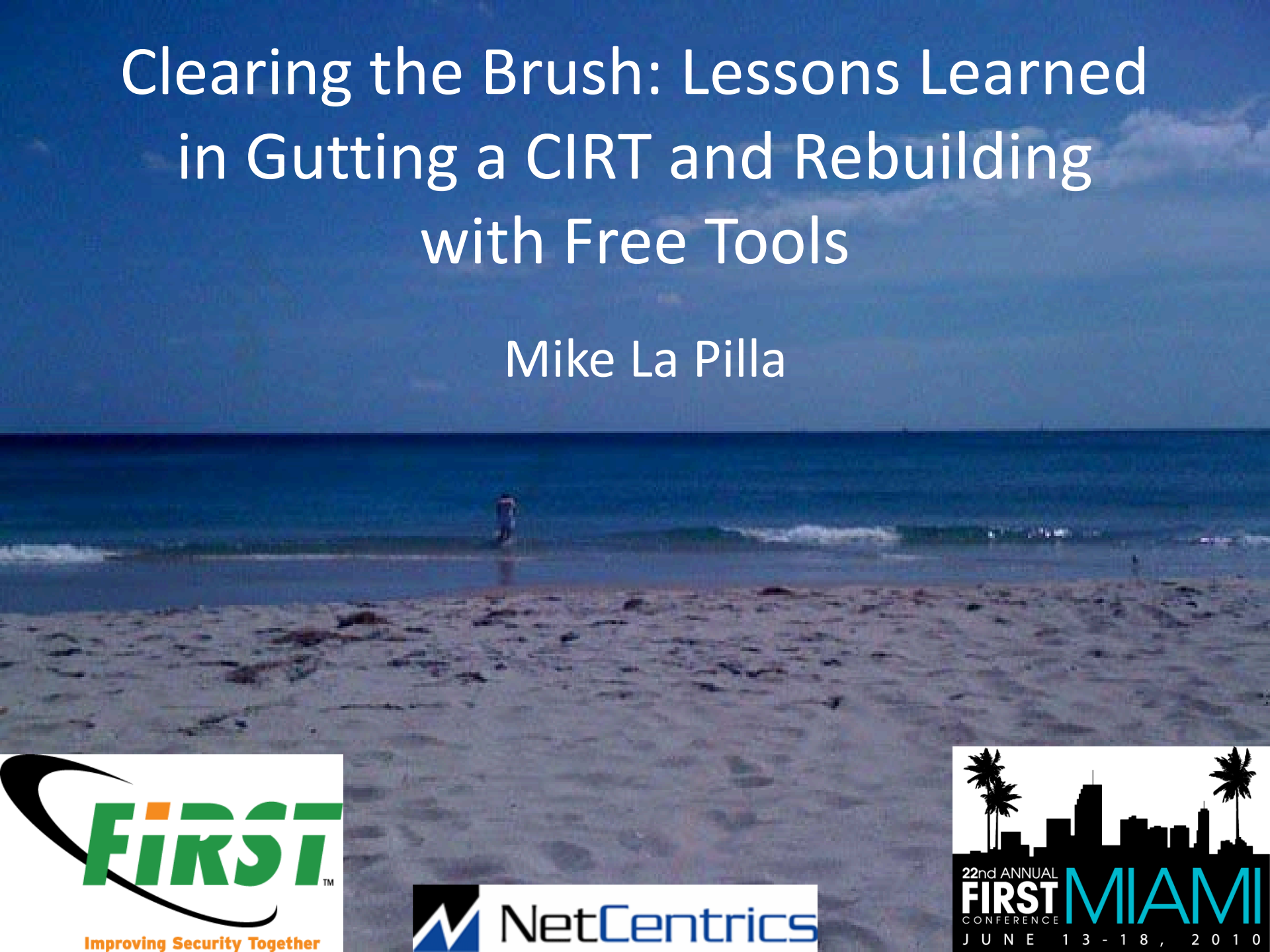
Clearing the Brush: Lessons Learned in Gutting a CIRT and Rebuilding with Free Tools

Mike La Pilla



FIRST™
Improving Security Together

NetCentrics

22nd ANNUAL FIRST CONFERENCE MIAMI
JUNE 13-18, 2010

Slide Warning

- These are draft slides, not the ones presented
- Most images have been removed from draft
- If you are reading these you should check the FIRST portal for the latest ones

About This Presentation

- Everyone Has Their Own Take
- Plenty of Papers on This Subject
- Focus on Building 10 Essential Tools/Systems
  - Preferably without spending money

If You Want Organization and Structure

- http://first.org/resources/guides/
  - CSIRT Setting up Guide
  - CERT-in-a-box
- http://www.sans.org/reading_room/whitepapers/incident/
- Also stuff on Auscert, CERT/CC, GFIRST, etc

Past vs Present

Past vs Present

Preparation by Preservation

- Picture of frozen hard drive

Preparation by Obliteration

- Picture of Bar

Know Your Scope

- Areas of Response
- Actions Allowed
- Contact List

Know Your People

Beware of Certifications

Attack Categories

10 Systems You Need To Build

1: Automatic Malware Analysis System

- Purpose: Automatically process malware samples
- Recommended Features: Fast, Exe and DLL, Memory Dumps

1: Automatic Malware Analysis System

1: Automatic Malware Analysis System

2: Automatic JS Analyzer

- Purpose: Unpack/Analyze/Interpret Javascript
- Recommended Capabilities: Network replay, live site analysis, copy and paste

2: Automatic JS Analyzer

3: Automatic Document Analyzer

- Purpose: Analyze non-executable documents
- Recommended Capabilities: Exploit matching, decompression, javascript/flash parsing

3: Automatic Document Analyzer

4: Document Database

- Purpose: Archive documents
- Recommended Capabilities: Store name, file properties, metadata, link malware info

4: Document Database

5: Malware Repository

- Purpose: Store malware
- Recommended Capabilities: Search, store properties, link to other systems

5: Malware Repository

6: IP and Hostname Tracker

- Purpose: Track network information over time
- Recommended Capabilities: Passive DNS, active checking, search, ASN, GeoIP

6: IP and Hostname Tracker

7: Forensics System/Lab

- Purpose: Forensic analzye drives, memory
- Recommended Capabilities: Scanning, automation, hashing

7: Forensics System/Lab

8: Image Repository

- Purpose: Replicate machines in production environment

8: Image Repository

9: Tiny Tools Server

- Purpose: Collection of scripts and tools that increase efficiency

9: Tiny Tools Server

10: Documentation Portal

- Purpose: Self-explanatory

Recommended Capabilities: Revisions, author tracking

10: Documentation Portal

Final Workflow Diagram

Questions?

- mlapilla@netcentrics.com

References