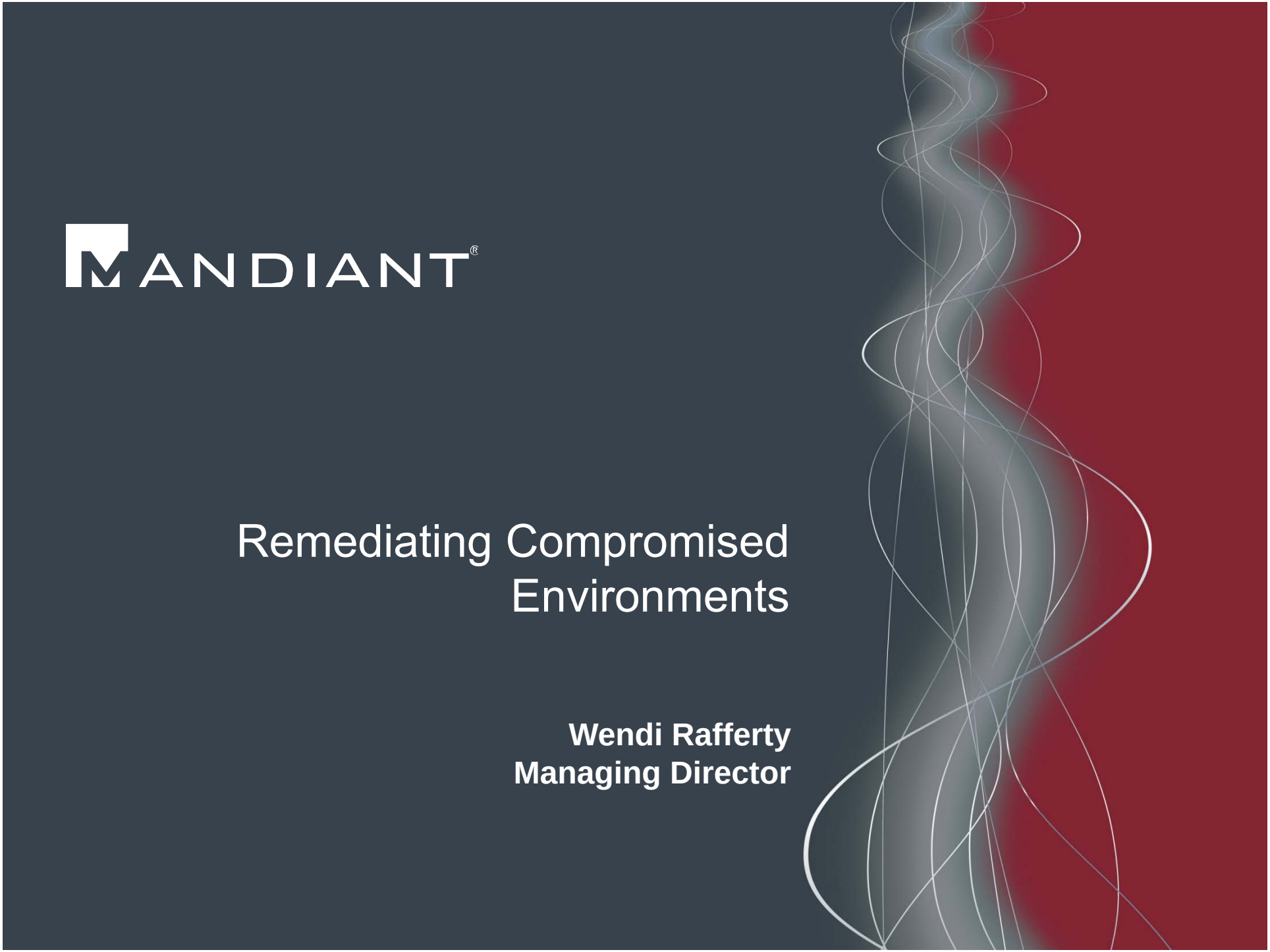


Remediating Compromised Environments

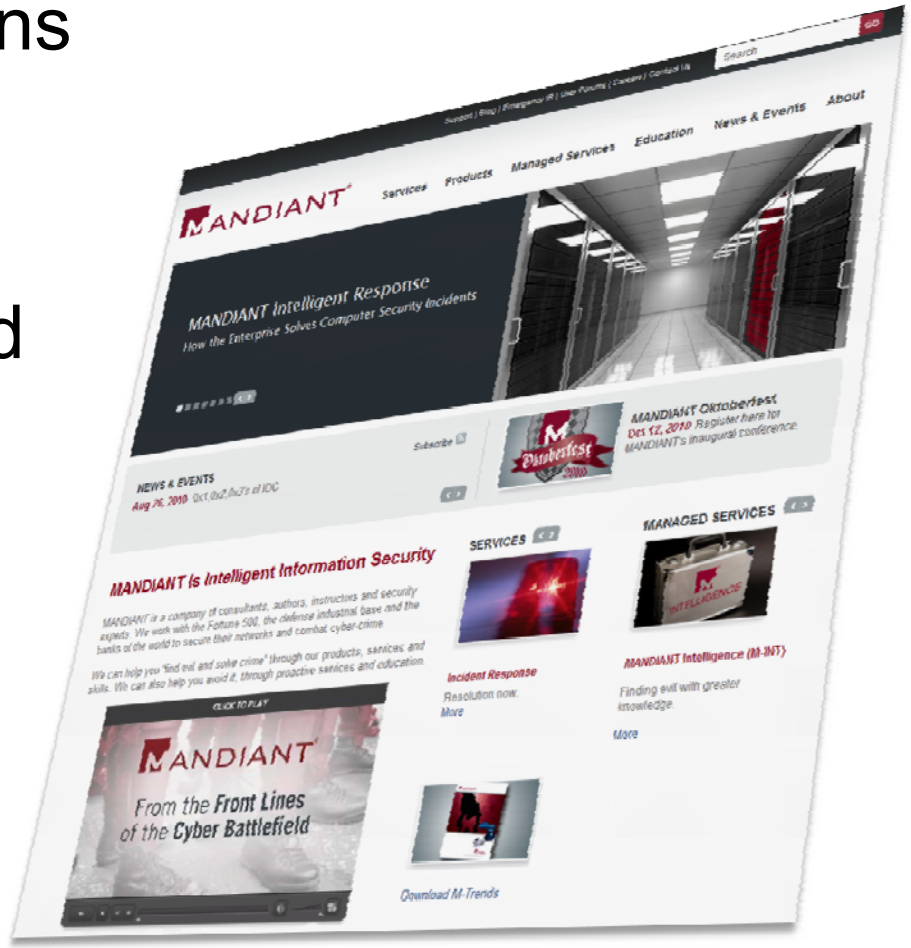
Wendi Rafferty
Managing Director

Agenda

- Introduction
- 2010 IR Investigations
- What is Remediation?
- Visibility and Response
- Two Remediation Case Studies
- Q & A – Current Investigations, Other Topics

MANDIANT

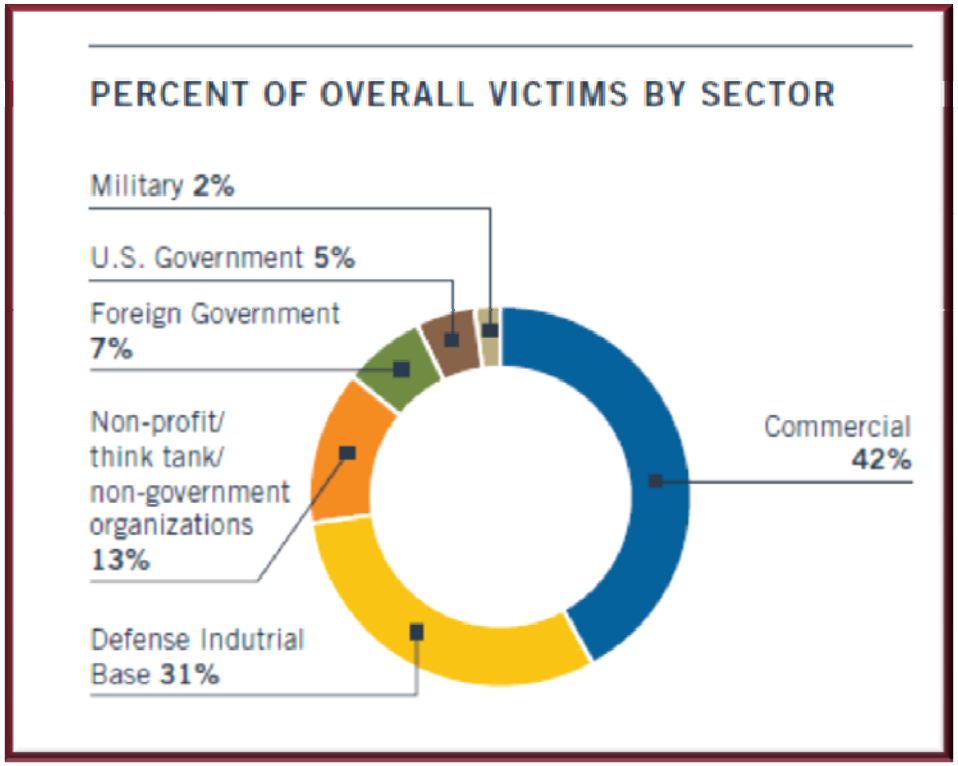
- APT and CDT investigations
- Four U.S. offices
  - DC, NY, LA, SF
- Professional and managed services, software and education
- Customers in
  - 20% of the Fortune 100, 500
  - 60% of the largest defense contractors



About Wendi

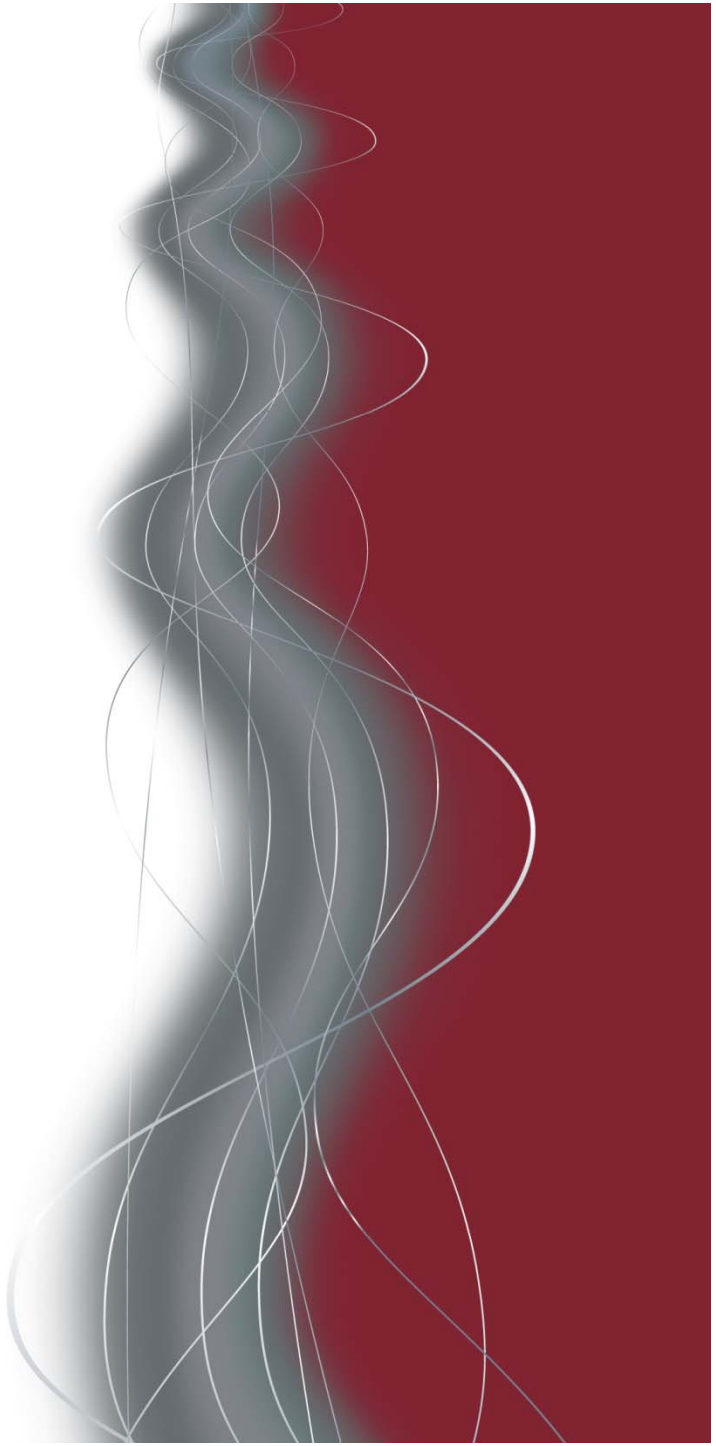
- 4+ yrs @ Mandiant
  - Los Angeles Office
  - Incident Response Background
    - Federal
    - Commercial
- 4+ yrs US Air Force OSI
  - Computer Crime Investigator
  - Forensic Analysis
  - Intrusion Investigations

2010 Mandiant IR Investigations



Commercial Sector Breakdown	
Automotive	2%
Space and Sateallites and Imagery	19%
Cryptograph & Communications	20%
Mining	2%
Energy	18%
Legal	9%
Investment Banking	3%
Media/Public Relations	10%
Hospitality	2%
Chemical	5%
Technology	10%

What is Remediation?



Remediation is (at least) 2 Parts:

MANDIANT

PART 1

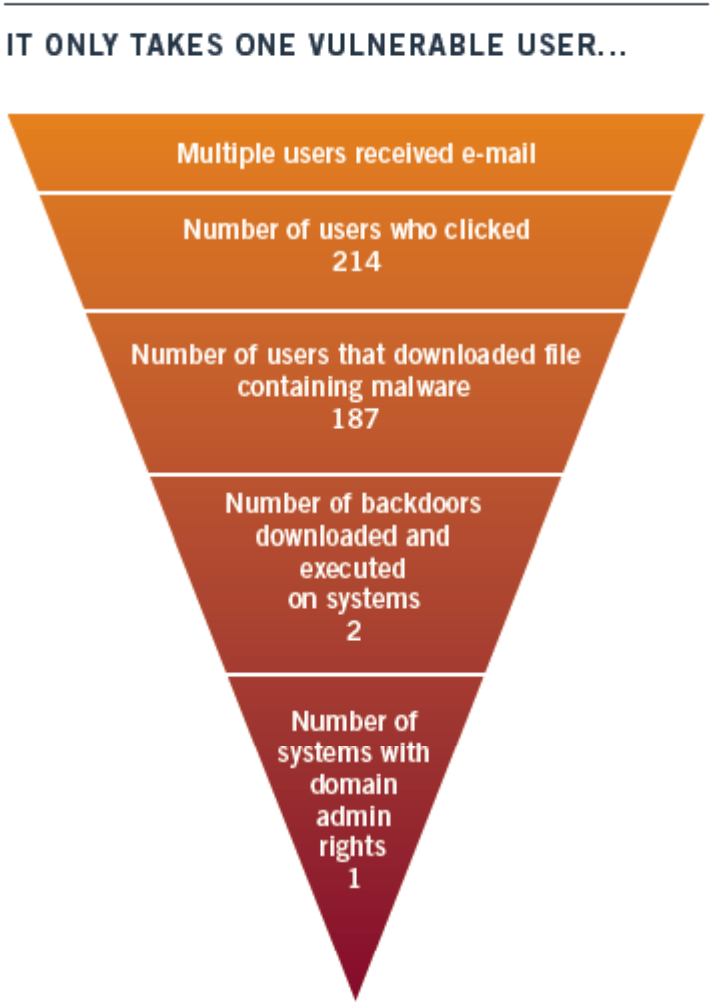
- Successfully removing an attacker from your network by:
  - Identifying their activity
  - Implementing countermeasures

PART 2

- Developing a plan and capabilities to:
  - Successfully detect future attacker activity
  - Respond quickly to future attacks

What Makes Remediating a Targeted Attack Difficult?

- Attackers with access to a lot of malware
- Attackers who escalate behavior based on your response
- Attackers who repeatedly seek to maintain presence once it is lost
- Attackers who target people, not systems
- Attackers who target organizations with sensitive information in mind



Moving Beyond the Basics… What Makes Remediation Successful?

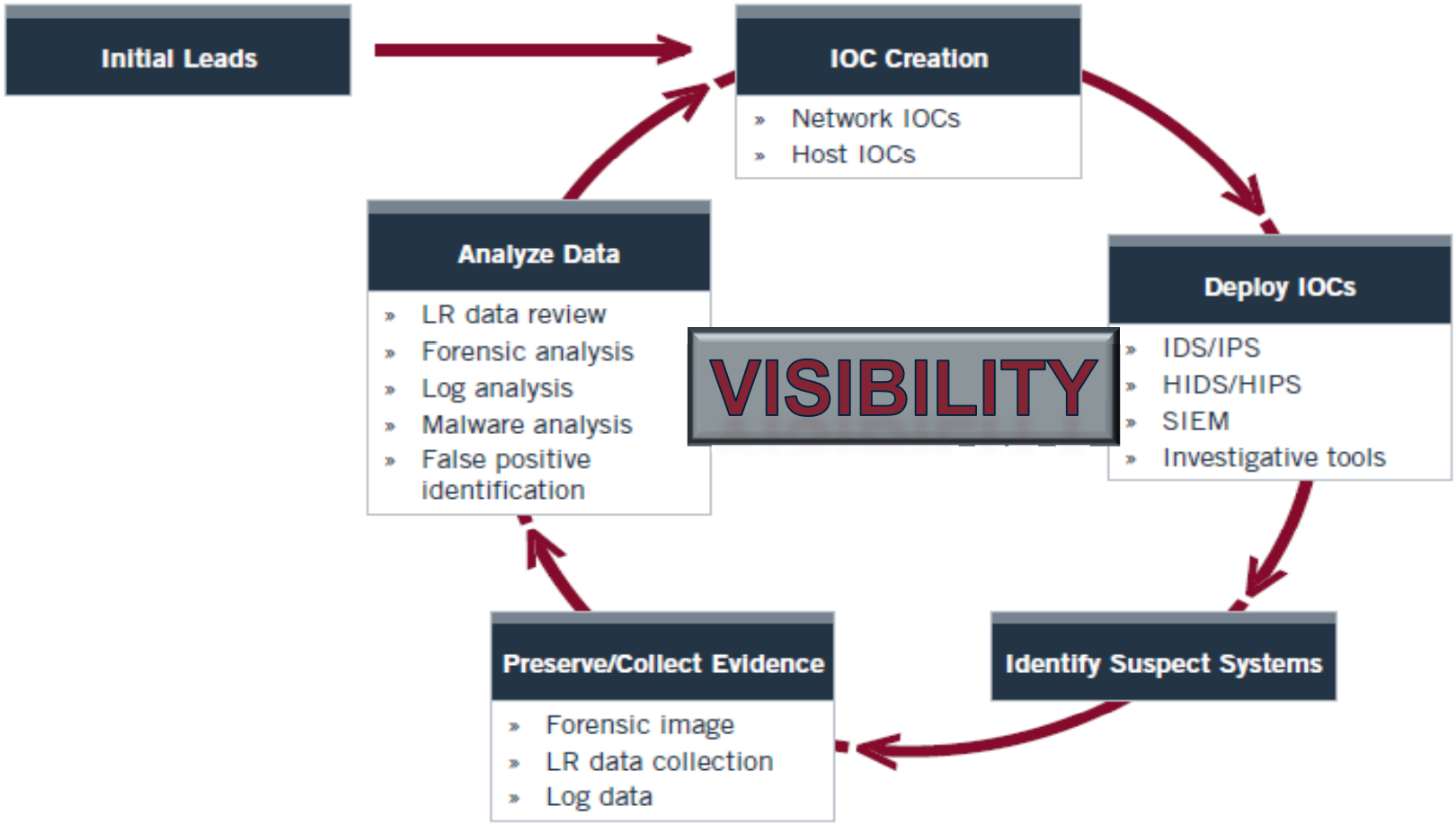
MANDIANT®

Items Needed to Establish Operational Readiness to Respond to the APT	
Total Visibility Across the Enterprise	» Host-based visibility » Network-based visibility » Increased logging » Log aggregation
Actionable Intelligence	Threat intelligence derived internally and from outside sources including: » Relationships with peer organizations » Defense industrial base » Law enforcement » Vendor-specific threat feeds

Visibility -> Detection -> Response

MANDIANT

HIGH-LEVEL INVESTIGATIVE STEPS PERFORMED AT VICTIM X



Understand your network

- List your
  - DNS servers
  - DHCP servers
  - Internet connections
  - VPN concentrators
  - Windows domains
  - Network diagram
  - Firewall rulesets
  - Group policy objects

Centralize logs

- DNS servers
  - Name and query source
- DHCP servers
  - Hostname/address pairs
- VPN servers
  - Hostname/address pairs
  - Users
- Proxies
  - Date, time, hostname / address, URL request
- Windows event logs
  - Big enough
  - Success *and* failure
- HIPS / HIDS
  - Report off-host
- Firewalls
  - Traffic metadata
  - Don't need full packet capture here

Incident management

- Acquire a security information event management (SIEM)
  - At least, copy logs centrally somewhere
  - At best, tailor a commercial offering
- Roll as much data as you can into it
  - Firewall, VPN, DNS, DHCP
- Goal is to make your smartest people faster

There is no One correct way to perform remediation: every environment is different

A Tale of Two Investigations

- Two victim organizations
- Different sizes, strengths, and capabilities
- Both implemented remediation in very different ways
- Both successful in removing the initial attackers and detecting subsequent activity
- Both organizations have detected multiple subsequent attacks

Two Investigations:

	Victim X	Victim Y
Total hosts	< 1,500	> 150,000
Compromised hosts	< 20	< 100
Compromised accounts	5	20
Account types	Domain admin Local admin	Domain admin Local admin Service accounts
Date of initial compromise	> 1 year	>3 years

Two Investigations:

MANDIANT

	Victim X	Victim Y
Distinct pieces of malware	< 10	> 30, including 12 different keyloggers
Malware capabilities	Reverse shell Credential harvesting Host and network recon Pass the hash tools Lateral movement Disable Windows File Protection	Reverse shell Credential harvesting Host and network recon Pass the hash tools Lateral movement Email harvesting Data compression Data transfer

Two Investigations

	Victim X	Victim Y
Email harvested	0 employees	> 50 employees
Lateral movement	Scheduled tasks Compromised host used as gold image	Net use Scheduled tasks At jobs

Victim X: Classic Approach

MANDIANT

STRONG NETWORK VISIBILITY:	TIGHT HOST CONTROL:
▪ 2 Network Egress Points for entire enterprise ▪ Full Packet Capture ▪ DNS logging ▪ Proxy logging and blocking ▪ Aggregation at SIEM ▪ Threat-specific network sensors	▪ Removed Internet access from all users ▪ Conducted traditional remediation event after implementing security best practices ▪ Reintroduced users to Internet access with highly customized Internet isolation application

Victim Y: Iterative Approach

MANDIANT

IDENTIFIED CRITICAL INFRASTRUCTURE:	COMPREHENSIVE VISIBILITY:
▪ Identified hosts and personnel targeted ▪ Hardened critical infrastructure first from the inside out ▪ Removed new credential harvesting capability from attackers ▪ Encrypted communication & identified next victims	▪ Continuous threat-specific monitoring of hosts and network ▪ Continued investigation until new compromises dwindled ▪ Conducted traditional remediation event ▪ In process of building strong response team

Defining the Win

- Company profiled in M-trends *was* re-compromised
- Their win is a matured incident response capability:
  - Faster identification
  - Smaller remediation effort
  - Normal operations vs. surge response
  - Ongoing managed cost vs. uncontrolled emergency expense

Q&A

wendi.rafferty@mandiant.com

Contact

Washington, DC (HQ)
2318 Mill Road
Suite 500
Alexandria, VA

New York, NY
24th West 40th Street
9th Floor
New York, NY 10018

El Segundo, CA
400 Continental Blvd
6th Floor
El Segundo, CA 90245

San Francisco, CA
425 Market Street
Suite 2200
San Francisco, CA 94105

phone: +1.703.683.3141
toll free: 1.800.647.7020
fax: +1.703.683.2891

www.mandiant.com
www.twitter.com/mandiant
http://blog.mandiant.com

M-Trends 2011

Download the full report

http://www.mandiant.com

Point Solutions (Free Tools)

MANDIANT

- Web Historian — browser analysis
- Memoryze — memory forensics
- Audit Viewer — memoryze front end
- Highlighter — log analysis
- Red Curtain — malware identifier
- IOCE — indicator of compromise editor
- OpenIOC — common language to describe IOCs

Two Remediations

	Victim X	Victim Y
Remediation technique	Classic remediation: all passwords changed, compromised systems wiped and reintroduced to network, implemented SIEM with limited host data aggregation but threat specific network monitoring, removed Internet access from users for period of time and reintroduced those capabilities with highly customized Internet isolation solution, limited egress traffic and used an explicit HTTP proxy.	Iterative approach: identified critical infrastructure and personnel, hardened hosts and increased monitoring of both, encrypted communications of targeted personnel and their inner circles, limited attacker use of email stealing through webmail, moved to Server 2008, and increased threat-specific monitoring of both hosts and network… all before conducting traditional remediation event and locking out attackers.