Toward more effective incident response
Portable incident response environment and incident response management

7 October 2012
Disclaimer

Ernst & Young refers to the global organization of member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit www.ey.com.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

This presentation is © 2012 Ernst & Young LLP. All rights reserved. No part of this document may be reproduced, transmitted or otherwise distributed in any form or by any means, electronic or mechanical, including by photocopying, facsimile transmission, recording, rekeying or using any information storage and retrieval system, without written permission from Ernst & Young LLP. Any reproduction, transmission or distribution of this form or any of the material herein is prohibited and is in violation of US and international law. Ernst & Young LLP expressly disclaims any liability in connection with use of this presentation or its contents by any third party.

Views expressed in this presentation are not necessarily those of Ernst & Young LLP.
If your goal is to:

- Collaborate openly
- Collaborate internally or with partners
- Manage incident response (IR) incidents across diverse teams
- Effectively manage your IR team on a single incident

This will help.
(And you don’t need to spend $10m on technology to do it.)
Take-home points

► Use portable, self-contained or well-constrained environments
► Organize people, data and analysis better
► Deliver consistent, high-quality results using less senior staff in a secure, repeatable, auditable manner
I've got a bunch of virtual windows machines networked together, hooked up to an incoming pipe from the net. They execute email attachments, share files, and have no security patches.

Between them, they have practically every virus.

Pretty, isn't it?

What is it?

There are mail trojans, warhol worms, and all sorts of exotic polymorphs. A monitoring system adds and wipes machines at random. The display shows the viruses as they move through the network, growing and struggling.

You know, normal people just have aquariums.

Good morning, Blaster. Are you and W32.Welchia getting along?

Who's a good virus? You are! Yes, you are!
Do adversaries do SIGINT?

To: CISO@client.com (or CISO@youremployer.com)
From: consultant@consulting.com (or you@youremployer.com)
Subject: Remediation weekend

Dear Phil (or Jane, or ....),

Looks like we're on track for doing the remediation weekend on 7 October 2012.
<etc>

-----

But even if the body is just:

MIAGCSqGSi3dQEHA6CAMIAACQAxgewwgekCAQAwUjBFMqsCQYDVQGkEwJBVTETMBGAS1UECBMKU29tZS1TdGF0ZTFhMB8GAIUEChMYSW50ZXJuZXiQgV2IkZ210cyBQdHkgTHRkAgkA7oW81OrifAwDQYJKoZIhvcNAQEBBQAeYCfnqPK/O34DFlIp2zsm+xZQ6R+94BqZHdtEWQN2evrcgtAng+f2ItILxrpcg8bEwDO5uGc+k92uYp2rLKI5BxCGb8fRM4kYC9sHbH2dPaqzUBhMxjgWdMCX6QE130u9MdGaP74Ogw8fN1I3D4sx/0kO2/QwgaukeY7uNhzcABgkq1江西9gwOBBoEwFAYIKoZIhvcNAwcECDrozFSsPnSgoIAEiHmqjSKAwiQbuQGL9w4nKw4I+44WgTkF7mGZWvYY8tOCdmdhDxRSMiLy682Imt+LTZfOLXzuFGTsCGUo742N8AAAAAAAAAAAAAAA
Incident management – the way it is (Excel)

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
<th>G</th>
<th>H</th>
<th>I</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>B</td>
<td>C</td>
<td>D</td>
<td>E</td>
<td>F</td>
<td>G</td>
<td>H</td>
<td>I</td>
</tr>
<tr>
<td>Date / Time</td>
<td>Host</td>
<td>Attributed</td>
<td>Event</td>
<td>Notes</td>
<td>Environment</td>
<td>Location</td>
<td>Exfil?</td>
<td></td>
</tr>
</tbody>
</table>

- **A** - Date / Time
- **B** - Host
- **C** - Attributed
- **D** - Event
- **E** - Notes
- **F** - Environment
- **G** - Location
- **H** - Exfil?

In the Excel sheet, you can see columns for different aspects of incident handling, such as date and time, host details, status, event type, and more. The sheet also includes tabs for timeline info and other relevant categories.
Problem statement

► IR teams are often in the environment rather than outside of it.
► IR often depends on remote tools/services.
► Collaboration is often via inefficient tools.
► Information is poorly contained – multiple email servers and mailboxes, local and shared folders, etc.
► Security is ad hoc or nonexistent.
► Integration is done via manual processes.
► Cannot cleanly archive entire environment.
Drivers

- Faster start-up, more efficient process, cleaner shutdown
  - Less downtime
  - Lower costs
- Repeatability
- Accountability
- Audit trail
- Reduced complexity
  - Less experienced staff can contribute more easily

It is also more elegant, appealing to the geek in all of us.
Proposed solution

- Integrated, portable, flexible, secure environment
- Component-based, plug and play
- Scalable

Supporting

- Integrated collaboration tools
- Secure out-of-band communications
- Databases for malware and incident response management
Advantages

► Secure, efficient collaboration
► Independent of environment being analyzed
► Tools are local to on-site team
► Data constrained to environment
► Communication and at-rest data secured
► Automated integration of data and processes
► Easily duplicated – consistent across organization
► Entire environment easily archived, searched
► Scalable
► Consolidation of scarce resources – Bit9, DeepSight
Components

Generic services
► Network
► Communications
► File services
► Collaboration
► Database services

IR-specific services
► Malware analysis
► Malware management
► Incident response management
► Issue tracking
Core server

► Guest OS – Ubuntu server
  ► Email
    ► Mail + security – http://flurdy.com/docs/postfix/#install
    ► Email – iRedMail (http://iredmail.org/)
    ► Mail + Windows Server + Exchange
  ► Network
    ► DNS/DHCP – http://sourceforge.net/projects/dhcp-dns-server/
    ► NTP, sftp, etc.
  ► Collaboration
    ► MediaWiki
    ► Jabber
    ► SMS
  ► Issue tracking – RTIR (http://bestpractical.com/rtir/)
Network and file services

Network – secure and out of band
- Host-only and NAT VM network
- Dedicated switch
- Cellular modem, dedicated DSL, encrypted tunnel

File
- VM host hard drive
- Direct attach to host, shared via host
- NAS
Communications

► Secure, encrypted, unattributable, out of band
► Segregation of environment enables collaboration among clients, partners and staff
► On-demand (email) and real-time (SMS, encrypted chat) communications integrated in single environment
► Domain with dynamic DNS for each project
► Email – web only, no clients? User choice
Documentation/collaboration

- Documentation – wiki
- Project management – task-tracking system:
- Information management
  - Malware DB front end
  - IR DB front end
- Planning and reporting
  - Database entries generate tickets to manage tasks
  - Template-driven recommended steps for certain issues
  - Generate current status automatically
  - Generate bulk of remediation plan automatically
Components – enterprise servers

- ECAT
- Mandiant Intelligent Response (MIR)
- Carbon Black
- Bit9
- AccessData
- Guidance Software
- SIEM (Q1, ArcSight, Nitro)
- Deep packet inspection tools (NetWitness, Wireshark)
- And others
Putting it all together

Core services

AV console

Qualys

NAS

Free flow

ECAT

Malware analysis

Forensic analysis

Analyst laptops

ArcSight

Mir

Data diode
What do we need to succeed?

► Good people
► Good tools
► Good processes
► Good data
► Good management of all of the above
What is good data?

► Accurate
► Right – i.e., the data you need
► Organized
► Available

A good incident response environment should provide all of these characteristics.
Malware management – the way it should be

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>MD5 hash</td>
<td>795f099a536f118fb4c34fcedfa42165</td>
</tr>
<tr>
<td>SHA-1 hash</td>
<td>c83624b0c3c65abea42305143db7c8619443df3a</td>
</tr>
<tr>
<td>Signed</td>
<td>Yes</td>
</tr>
<tr>
<td>Whitelisted</td>
<td>NSRL/Local</td>
</tr>
<tr>
<td>Bit9 Reputation</td>
<td>Clean</td>
</tr>
<tr>
<td>VirusTotal Report</td>
<td>Yes</td>
</tr>
<tr>
<td>Date found</td>
<td>10 July 2012</td>
</tr>
<tr>
<td>Date submitted</td>
<td>11 July 2012</td>
</tr>
<tr>
<td>Date installed</td>
<td>04 Feb 2012</td>
</tr>
<tr>
<td>Submitter</td>
<td>David Kovar</td>
</tr>
</tbody>
</table>

Manage environment through

Tag to include in timeline

Submit to VirusTotal
Submit to Cuckoo
Submit for human analysis

Search in ECAT
Search in master database
Search in Virus Total

Generate OpenIOC

Go!
Malware collection and analysis

- Either VM with sub-VMs or stand-alone system
  - Shared file storage or network services
- Malware zoo
  - Static analysis VM
  - Dynamic analysis VM
  - Cuckoo sandbox – with sub VMs
    - Run on the host OS or on a distinct machine
- Honeypot system(s)
- ECAT, MIR, Carbon Black, etc.
Malware database in action

**Partners/inputs**
- Batch input
  - Email
  - FTP
  - Web/GUI
- Automated input
  - Honeypot
  - Phish monitoring
  - ECAT
- Incident response
  - Internal IR team
  - External partners
- Threat intelligence
  - Vendors
  - Partnership orgs
  - Open source
- Risk management
  - Risk analysis
  - Business priorities

**Threat intelligence**
- Intel integration
- Threat modeling
- Log analysis
- External feeds
- Collaborative partners
- Vulnerability data analysis

**Human analysis**
- Dead box forensics
- Malware analysis
- Live response

**Static and dynamic analysis**
- PE analysis
- Reputation – Bit9
- YARA
- Hash/fuzzy hash
- Cuckoo sandbox

**Outputs**
- Incident management
  - Tasking
  - Daily reports
  - Remediation planning
  - IR database
- Threat/vulnerability management
  - Forensics analysis
  - Malware reports
  - Forensic summaries
  - IOCs
- Incident response
  - Event detection to IR
  - Tactical fix actions
- Threat intelligence
  - Threat reports
  - Intel database

Page 23
Toward more effective incident response
Outputs – planning and reporting

► Database entries generate tickets to manage tasks
► Template-driven recommended steps for certain issues
► Generate current status automatically
► Generate bulk of remediation plan automatically

 Remember narrative – if it is well written, the facts are easier to discern, the quality of the resulting analysis is higher and the reader is more receptive.
Incident response management

- Collect and manage data
  - Malware and IR databases
- Manage staff and partners
  - Email, ticketing system, collaboration tools
- Report to client, management, other engagements
  - Reporting and archiving
- Build templates to define and manage process
  - Email, issue ticket, wiki pages
Incident response management
Distributed incident management

► Link individual IR environments to central resources
  ► Distributed real-time threat intelligence
  ► Collaboration in real time for IR management
  ► Preservation of data to feed into future engagements
It is all about information management

- Ultimate goal is to produce actionable intelligence
  - Valuable to current incident
  - Valuable threat intelligence for other engagements
- Managing malware is all well and good, but without context, much of the value is lost.
Follow-up items, what you can do next

► Interchange formats
  ► OpenIOC, MAEC

► What you can do to contribute:
  ► Help write code.
  ► Work on YARA or Cuckoo.
  ► Poke holes in this.
  ► Let me know that it helped in some way and what I can do to make it better.
Contact information

For questions, please contact:
David Kovar, Manager
+1 650 278 1774
david.kovar@ey.com