Toward more effective incident response

Portable incident response environment and incident response management

7 October 2012

ERNST & YOUNG
Quality In Everything We Do

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.

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

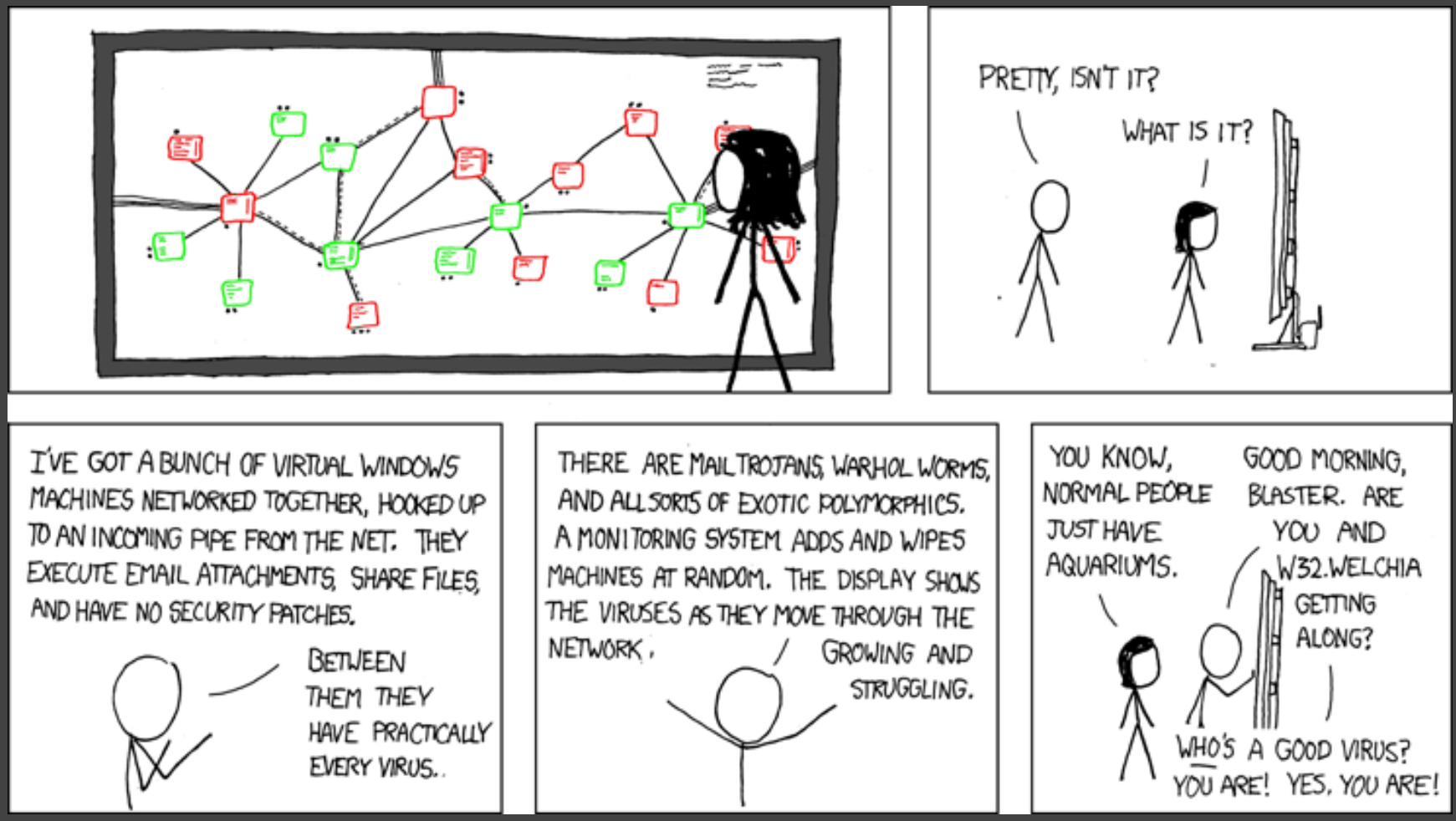
This will help.

(And you don’t need to spend $10m on technology to do it.)

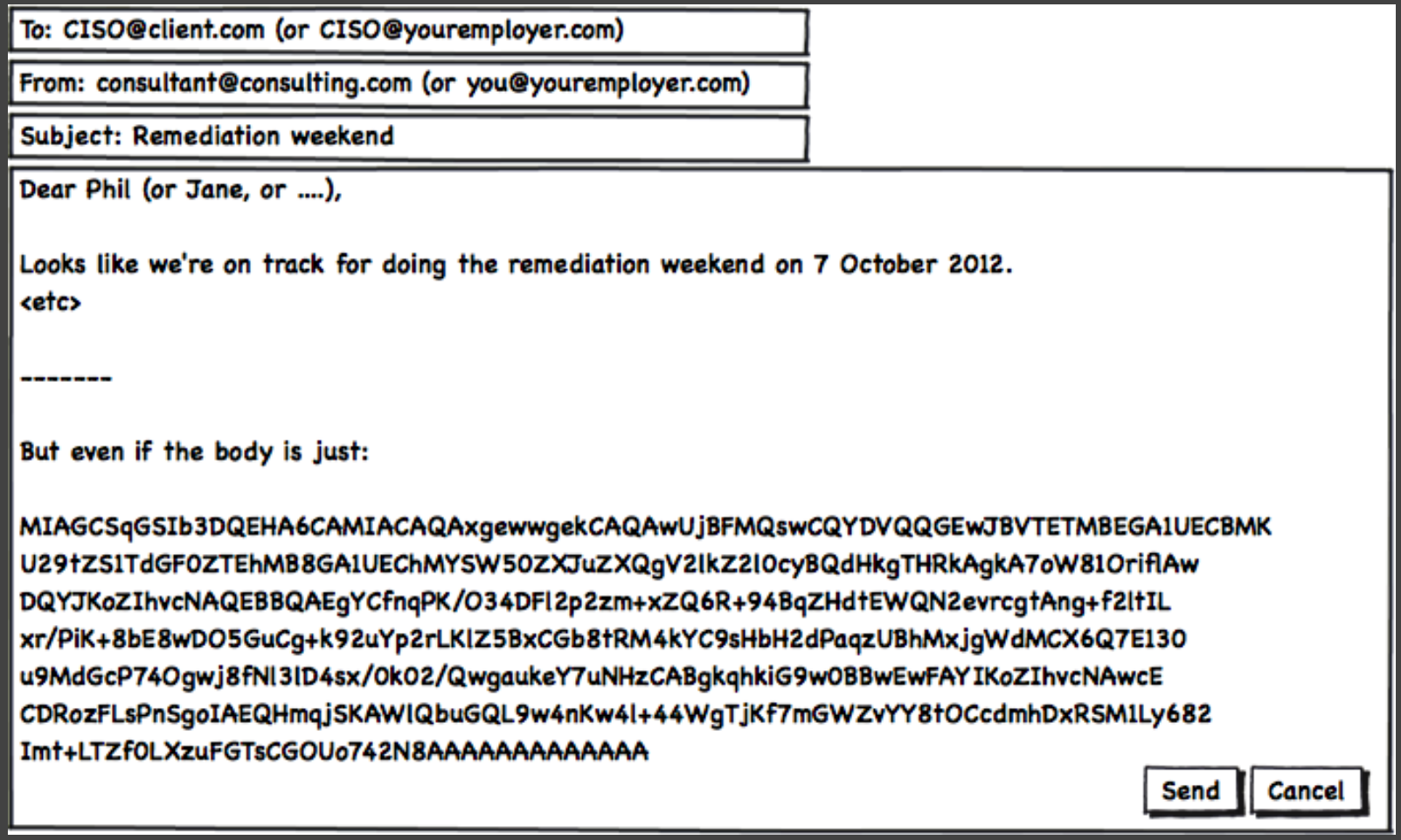
Take-home points

- 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

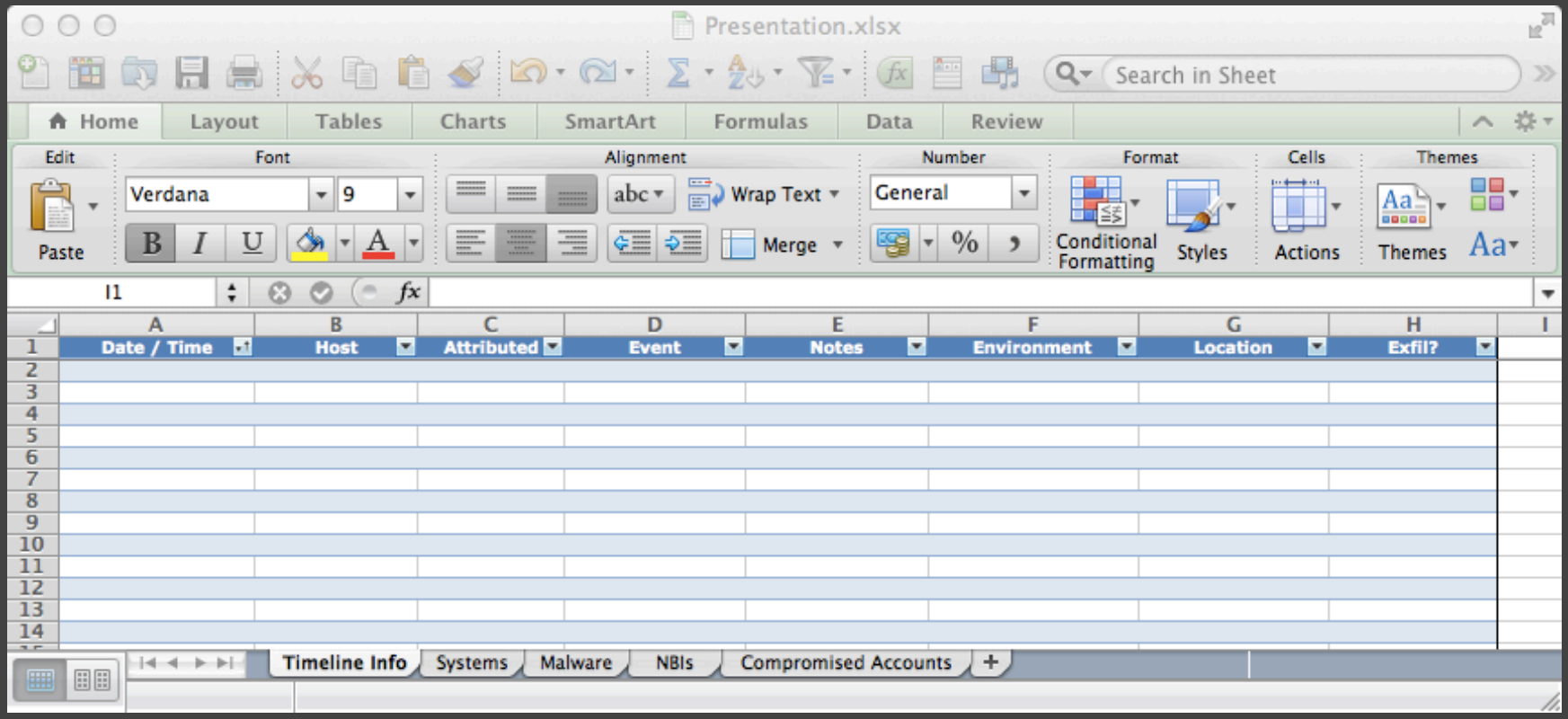
xkcd #350 – Network



Do adversaries do SIGINT?



Incident management – the way it is (Excel)



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

- 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

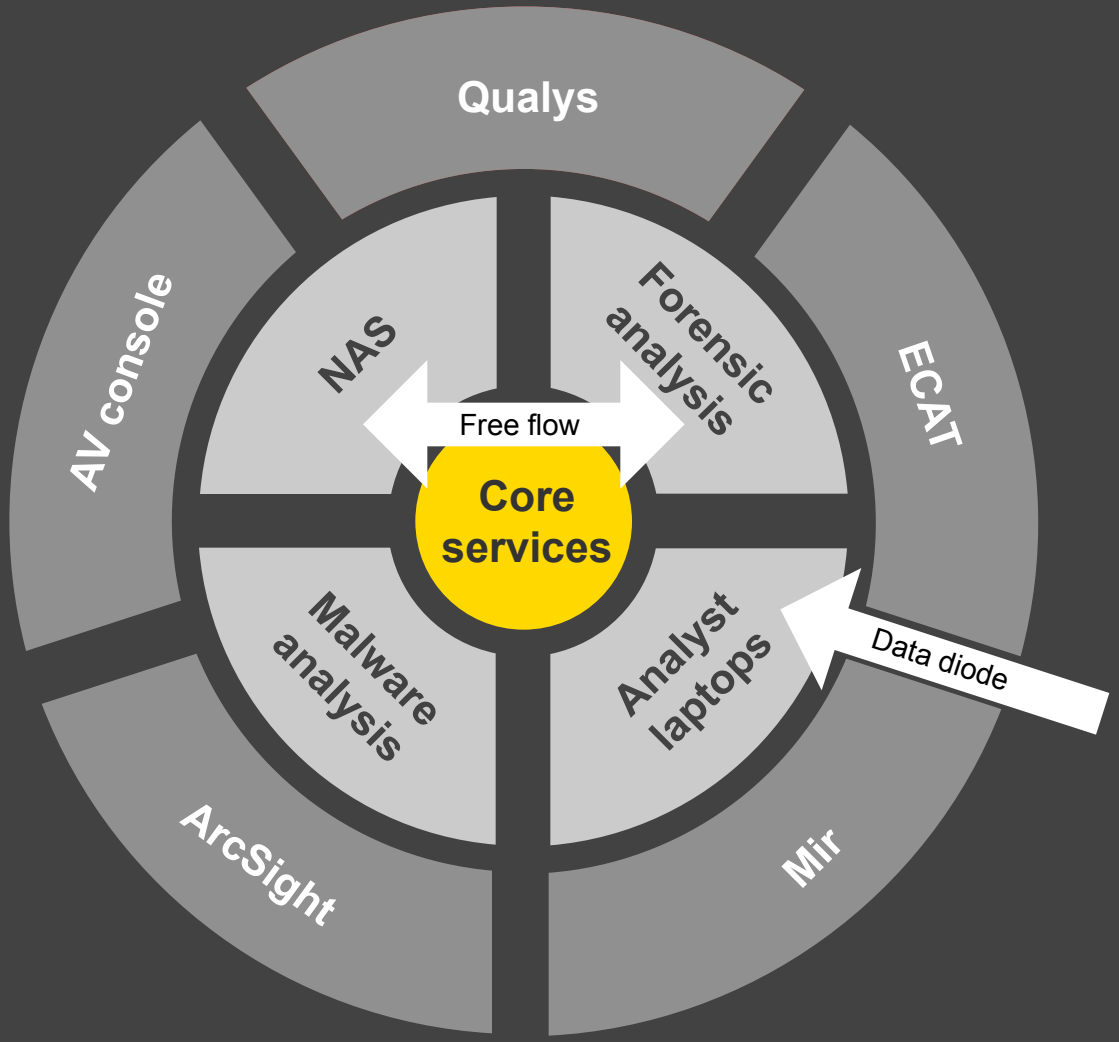
Documentation/collaboration

- 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



What do we need to succeed?

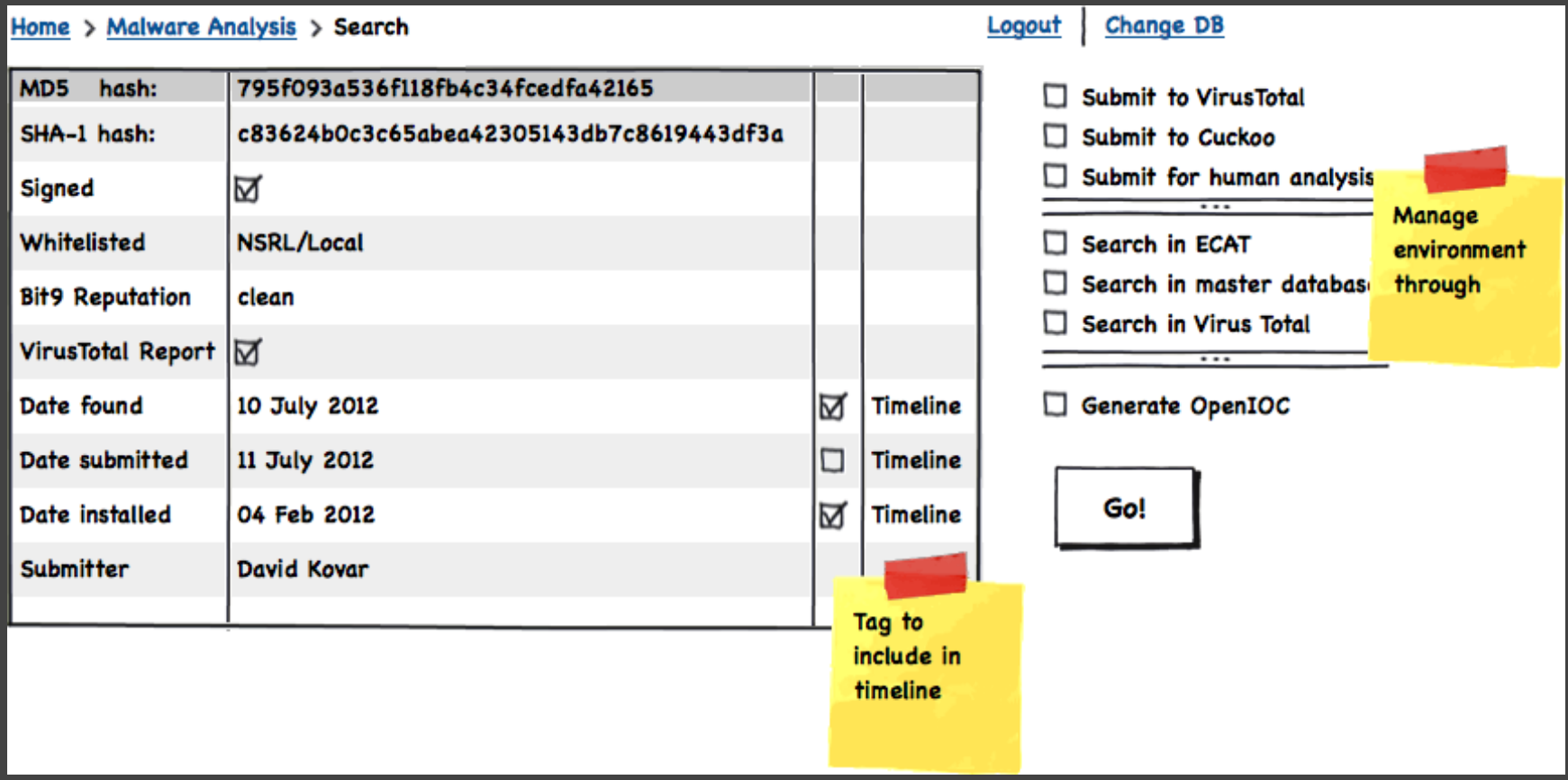
- Good people
- Good tools
- Good processes
- Good data
- Good management of all of the above

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.

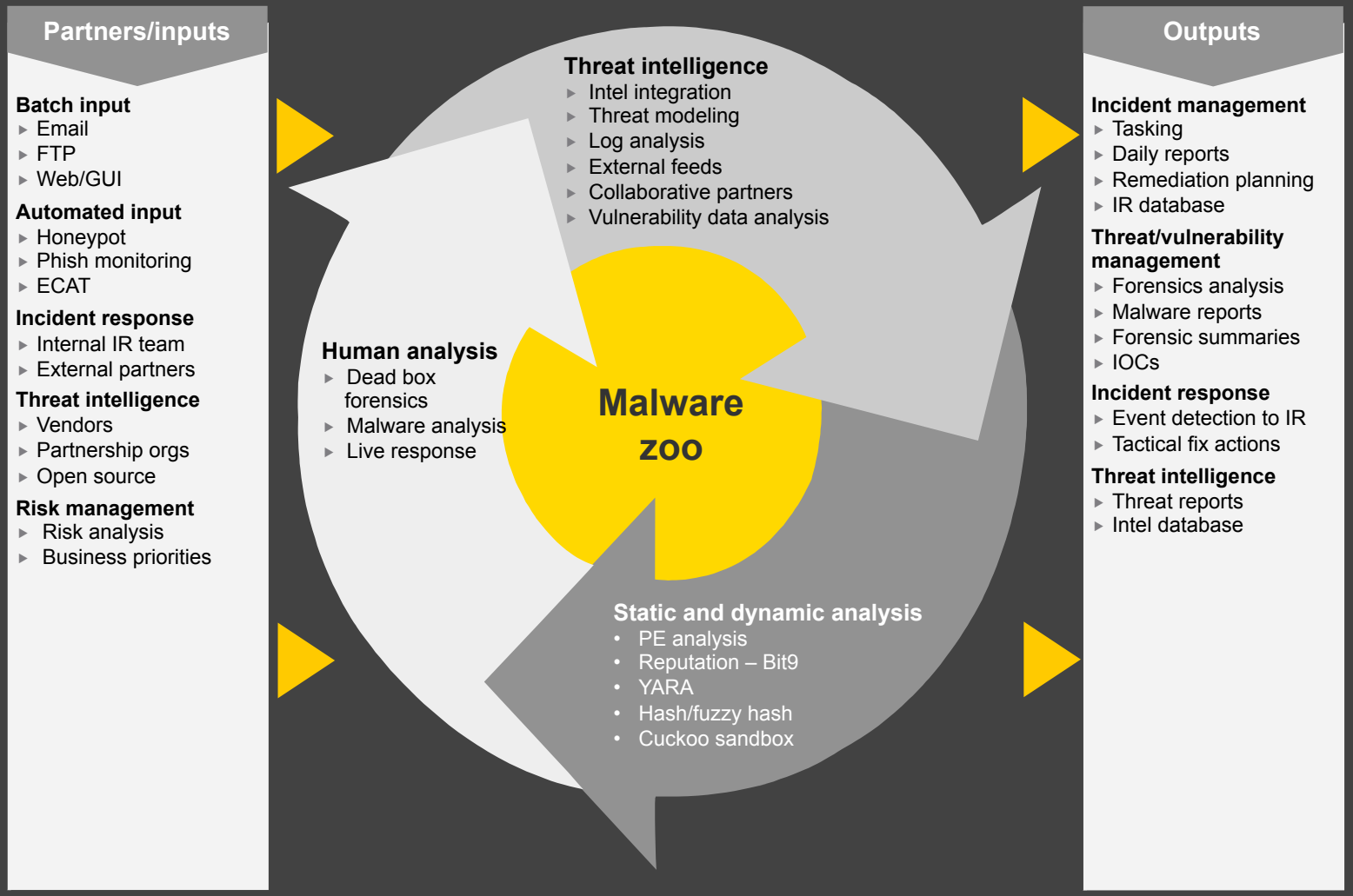
Malware management – the way it should be



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



Outputs – planning and reporting

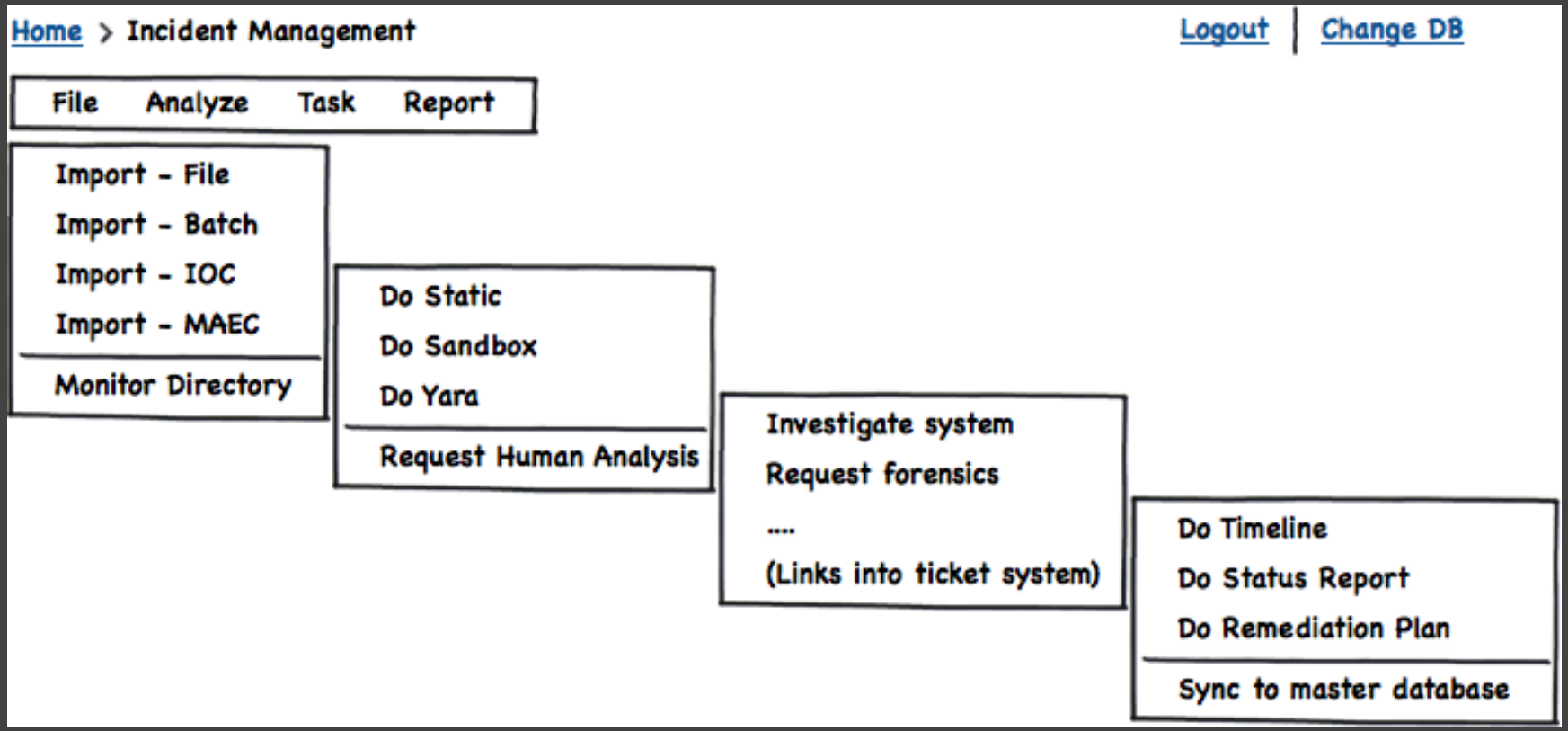
- Database entries generate tickets to manage tasks
- Template-driven recommended steps for certain issues
- Generate current status automatically
- Generate bulk of remediation plan automatically

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