



An overview of the CERT/CC and CSIRT Community

Jason A. Rafail

October 2007



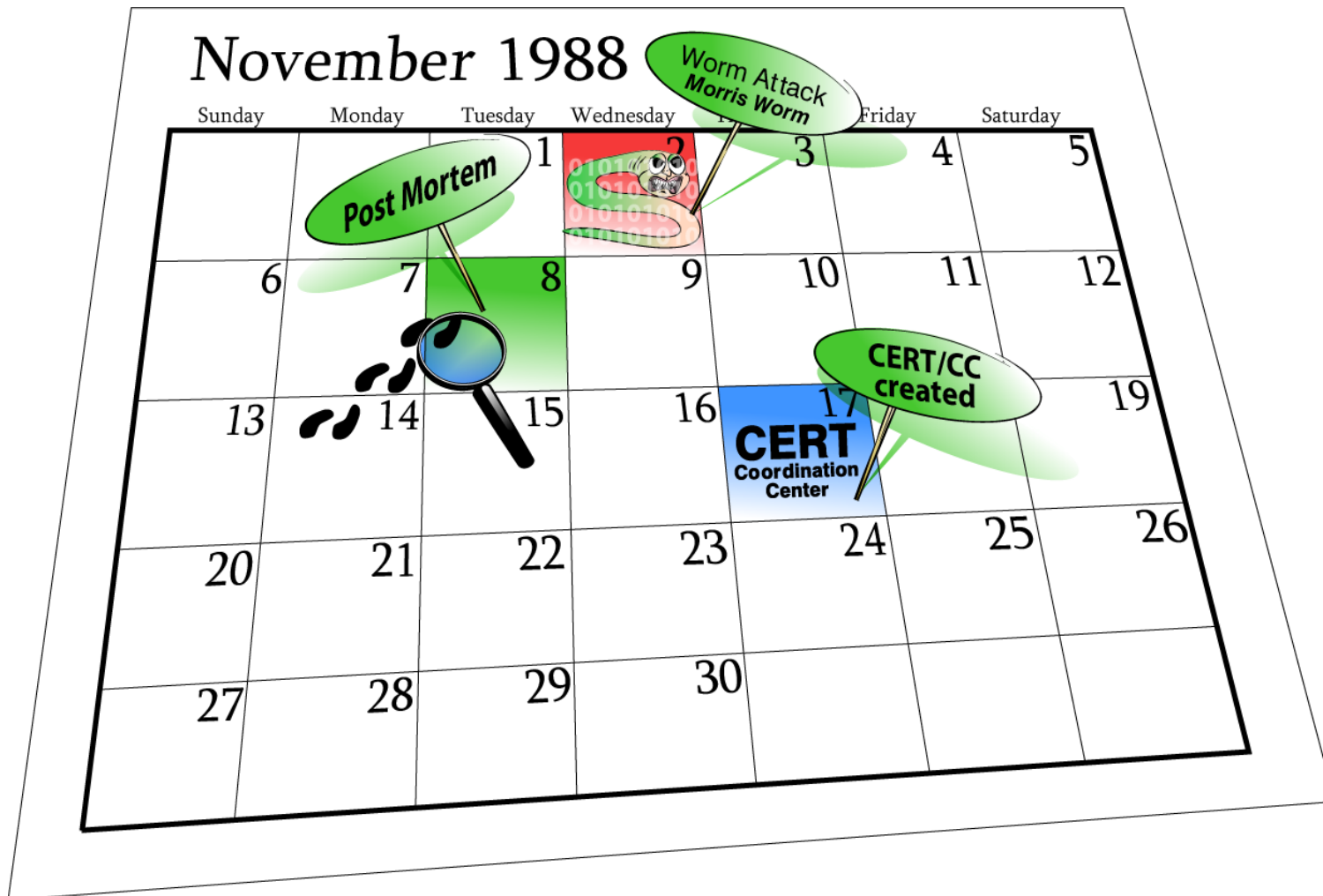
Overview

- CERT/CC
- CSIRTs with National Responsibility
- Partnerships and Trust
- Training
- Conclusion

Overview

- CERT/CC
- CSIRTs with National Responsibility
- Partnerships and Trust
- Training
- Conclusion

CERT/CC Beginning



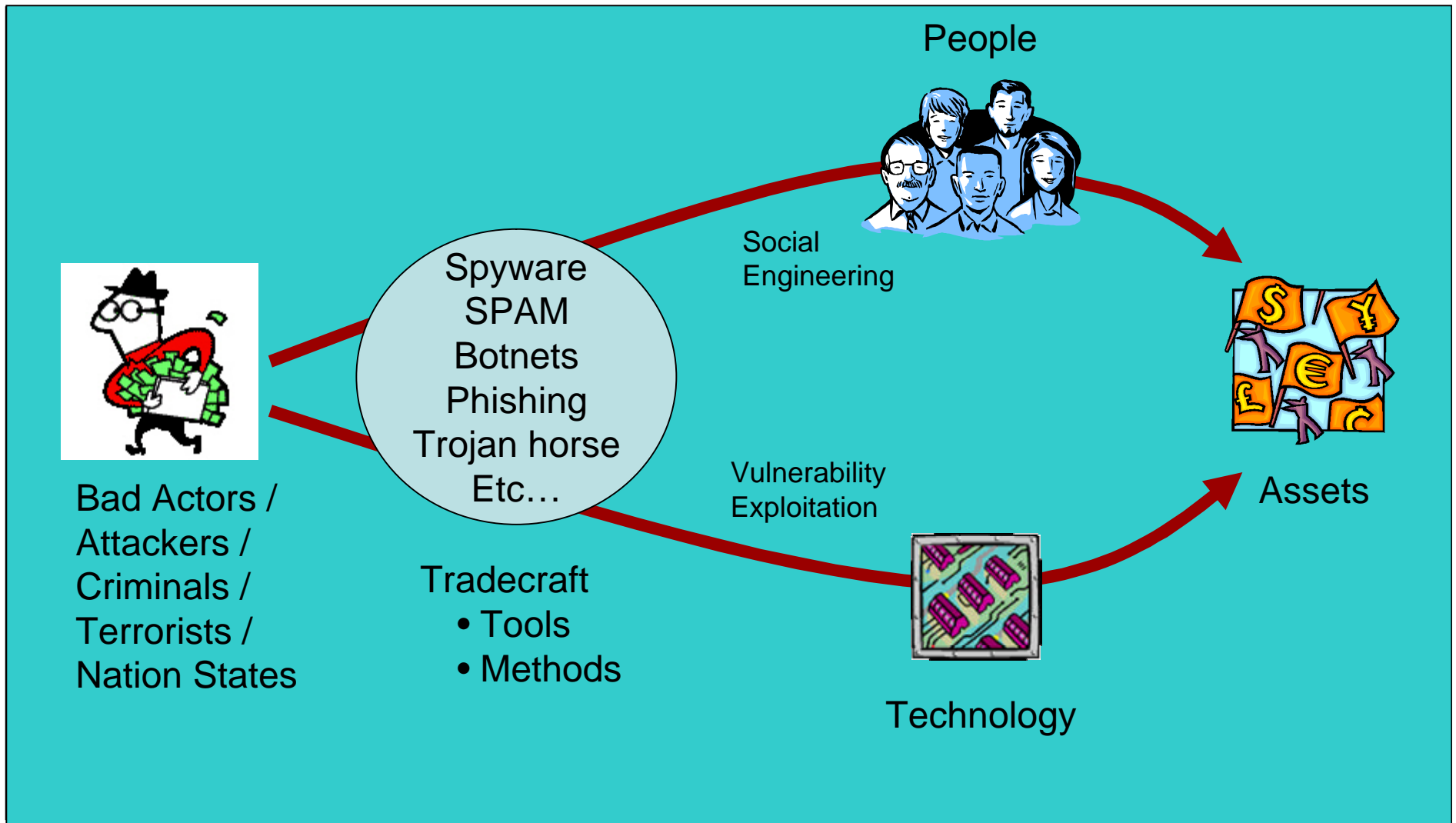
Purpose of CERT

CERT exists to ensure that appropriate technology, systems development, practices, and supporting infrastructures are used to resist, recognize and recover from attacks on networked systems, to limit damage, and to ensure continuity of critical services in the presence of attacks, accidents and failures.

Work with National CSIRTs to create capability and services that are of benefit to their constituency.

Provide training and develop methods for advanced technical analysis for Industry, Academia, Law Enforcement, etc...

Internet Security



Technology & People

Internet security is a social problem

- People compromise technology
 - Research & improve technology (e.g., people)
- People compromise people
 - Educate & improve people

The common thread is “people compromising...”

- Attribution, law enforcement
- International cooperation
- National CSIRT position / influence / coordination

Overview

- CERT/CC
- **CSIRTs with National Responsibility**
- Partnerships and Trust
- Training
- Conclusion

“CSIRTs with National Responsibility”

Generally speaking*, these are teams with

- government recognition; explicit or de facto
- broad responsibility for providing CSIRT services to constituencies that might include
 - critical infrastructure
 - government
 - system and network administrators
 - general public
 - other CSIRT teams in the country/economy with more specific constituencies

****there is no globally accepted definition of what a “national CSIRT” is or how it is recognized.***

National CSIRTs Around the World



<https://www.cert.org/csirts/national/contact.html>

National CSIRT Services

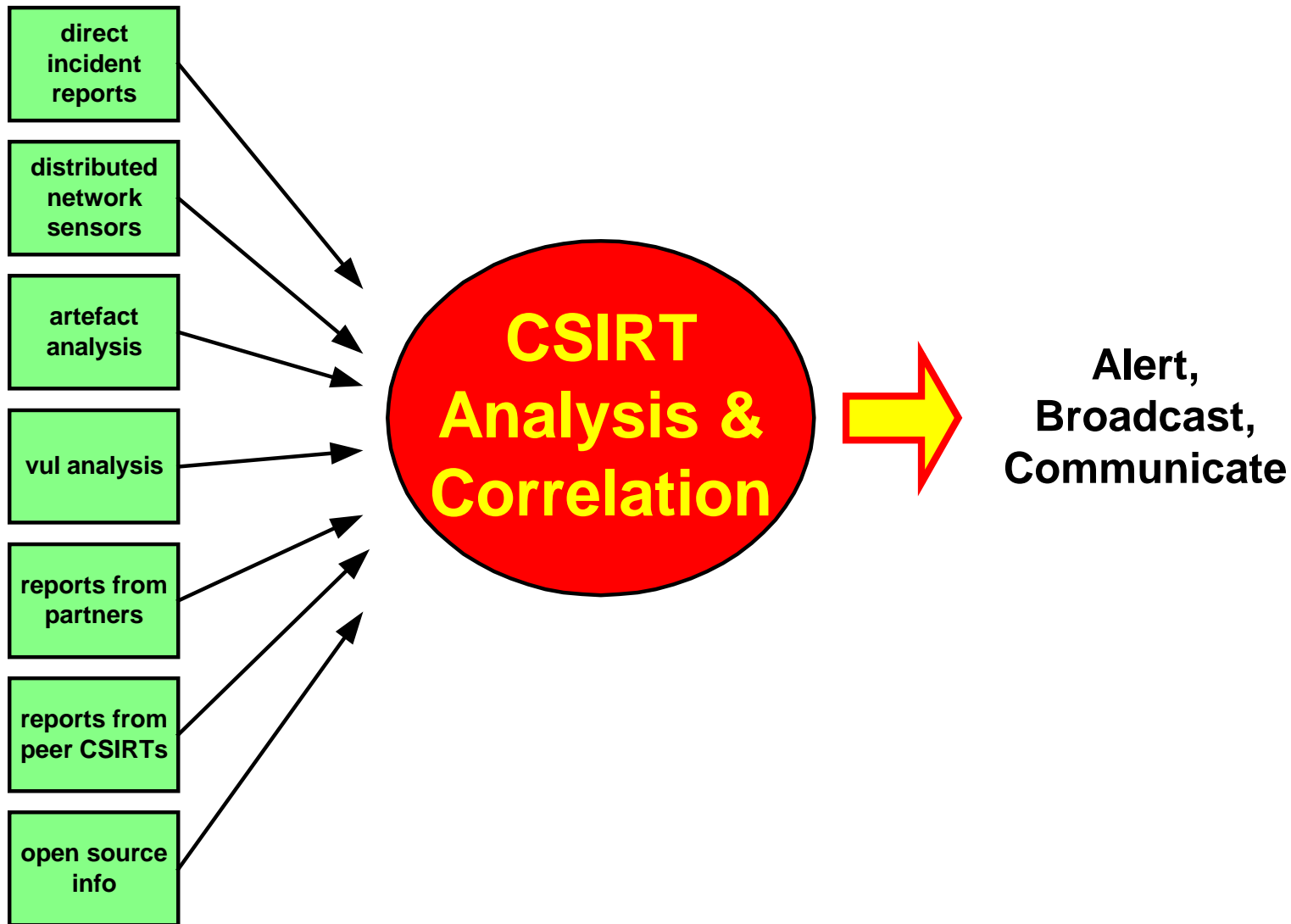
Technical

- Coordination
- Alerting Services
- Technical Publications
- Incident Analysis
- Vulnerability Analysis
- Artifact Analysis
- Forensic Analysis
- Training

Non-Technical

- Alerting Services
- User focused publications
- General Security and Computing Information

Communication via a Process



Principles of Information Release

- Strive for accuracy
- Validate/verify information
- Rate information for probability of accuracy
- Work to determine the limit for release of unverified information or speculation
- Identify the level of confidence in information
- Protect sources appropriately, but ensure information is appropriately attributed
- Coordinate with all affected to ensure information is released appropriately

Dissemination Capabilities

- Web site (public or private)
- Electronic mailing lists
- Recorded telephone message lines
- Conference calls with key partners/constituents
- News media
- Service providers/Vendors
- SMS and other mobile communications

Overview

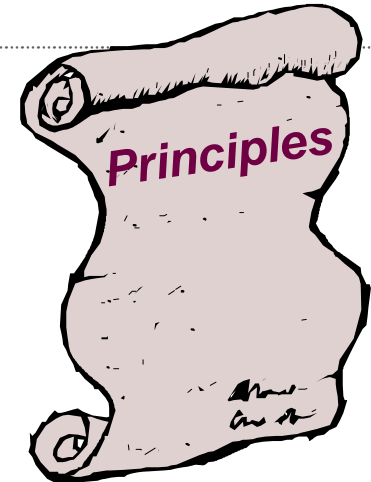
- CERT/CC
- CSIRTs with National Responsibility
- **Partnerships and Trust**
- Training
- Conclusion

Key Partners/Info Sources for National CSIRT Teams

- peer CSIRT teams
- other CSIRT teams within the country
- government
- law enforcement
- intelligence agencies
- major and minor ISPs
- software vendors
- hardware vendors
- anti-virus community
- Internet experts
- academia
- information distribution partners
- open sources
- critical infrastructure providers

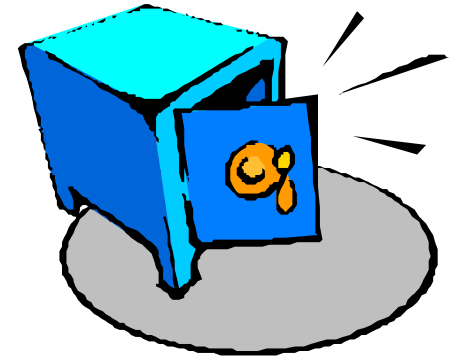
Building Trust: Principles

- provide valued services
 - proactive as well as reactive
- ensure confidentiality and impartiality
 - we do not identify victims but can pass information anonymously and describe activity without attribution
 - unbiased source of trusted information
- coordinate with other organisations and experts
 - academic, government, corporate
 - distributed model for incident response teams (coordination and cooperation, not control)



Contacts

- CERT/CC Contacts
 - hundreds of relationships
 - 700+ hardware and software contacts
 - security and technology experts
 - hundreds of government employees
 - ISPs/telecom providers
 - other organizational and National CSIRTs
 - contacts verified by out-of-band procedures
 - use cryptographically secure communications



Raising Awareness and Outreach

Regularly attend, present and participate in conferences, including

— FIRST

www.first.org

— IETF

www.ietf.org

— RSA

www.rsaconference.com

— NANOG

www.nanog.org

— USENIX

www.usenix.org

◦ LISA

◦ Security Symposium

◦ Technical Conference

Overview

- CERT/CC
- CSIRTs with National Responsibility
- Partnerships and Trust
- **Training**
- Conclusion

Virtual Training Environment (VTE)

A library of information assurance and computer forensics best practices.

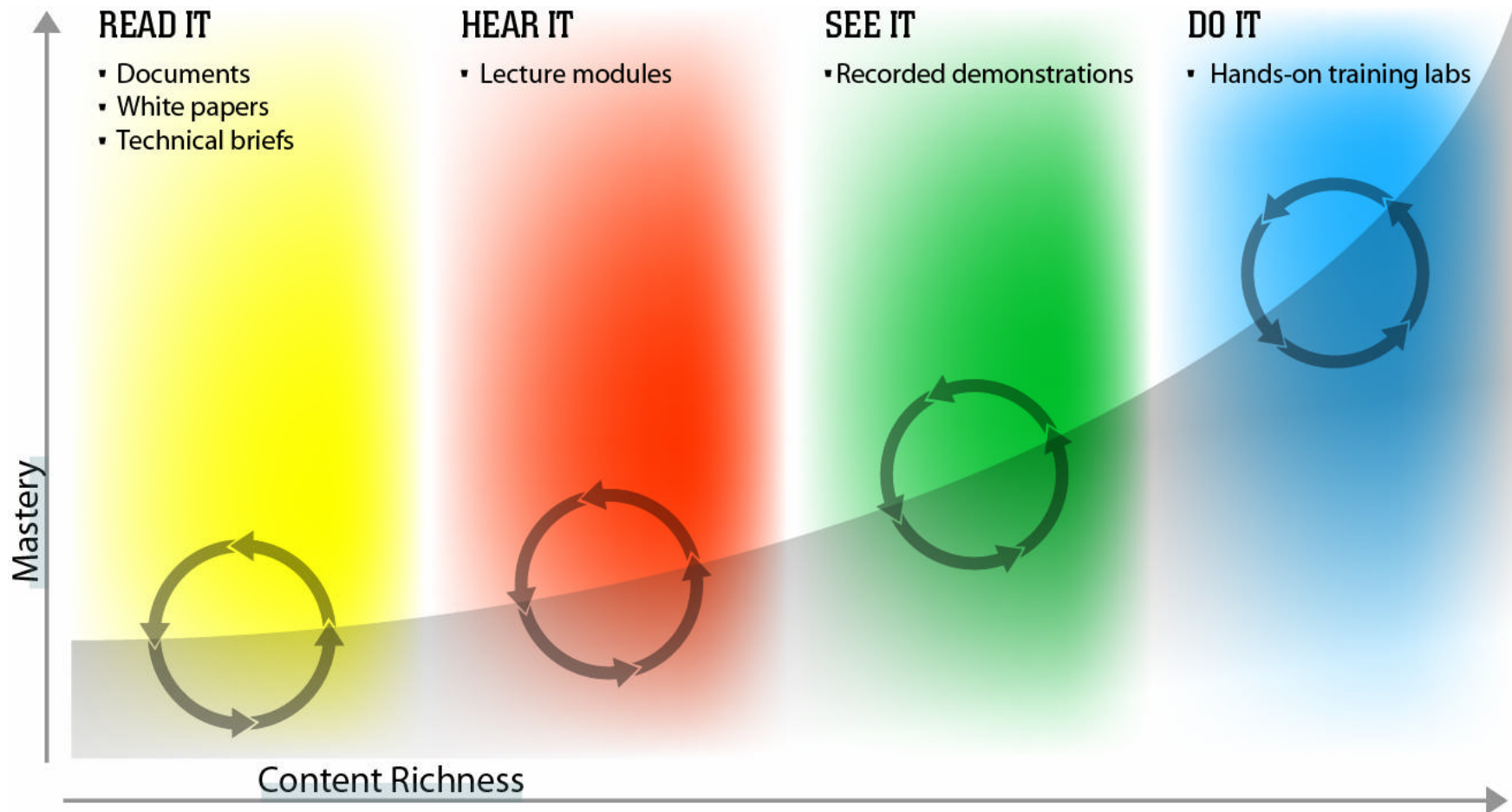
- contains more than 400 hours of multimedia-based instruction
- targeted at system administrators and computer incident first responders

Two access modes


- Library – publicly / premium* content
- Training – requires fee for use

*access to labs for registered users

The VTE 'Power Curve'



VTE - Visual Overview



Home | Library | Training | About VTE | Get Access | Help

The CERT **Virtual Training Environment (VTE)** - A revolutionary resource for information assurance, incident response and computer forensic training, with over 400 hours of material available. VTE blends the best of classroom instruction and self-paced online training, delivering training courses, anytime access to answers, and hands-on training labs all through a standard Web browser.
VTE is produced by the CERT® program of the Software Engineering Institute at Carnegie Mellon University.

Much of the VTE material is available for FREE in the [VTE Public Library](#). Access to the VTE Premium Library and training courses requires an account.

Members of the DoD may request free VTE accounts under a sponsorship agreement with DISA for [DoD D 8570.1](#) compliance training. [Learn more](#) about this program or [request an account](#) now.

Not covered by a sponsorship agreement? You can still use the free [VTE Public Library](#), learn more [about VTE](#), then sign up for a [trial account](#).

Interested in learning more? Follow the instructions below.

Current & Users	Organizations	Public
<p>First make sure your computer is set up for VTE, then log in to begin training:</p> <ul style="list-style-type: none">• Access your current courses• Log in to access VTE Library Premium Content• VTE readiness Browser Check	<p>Learn more about VTE and how it can help you support skill development and compliance training initiatives in information security, computer forensics, and incident response:</p> <ul style="list-style-type: none">• See the materials in the VTE Public Library and decide if they are useful to your organization• Request a trial account for VTE Premium Access to experience hands-on labs for yourself.• Review VTE public and private courses• Contact CERT to develop a training and skill development program for your organization	<p>Access FREE computer security and forensics training in the VTE Library.</p> <ul style="list-style-type: none">• 200+ hours of lectures and demos from CERT• No registration required! <p>Access the VTE Library</p>



VTE - Visual Overview

The image shows a presentation slide on the left and an EtherPeek NX network traffic capture window on the right. The slide is titled "Application Filtering and Network Access Controls" and shows a photo of a classroom. The EtherPeek NX window displays a capture of network traffic, including a TCP 3-way handshake and subsequent HTTP requests.

Slide Content:

Application Filtering and Network Access Controls

Slide Notes

Page 2
Okay, so not just talking about firewalling, not just talking about network packet filtering, there's still a lot of ways we can exert control

15 minutes 24 seconds Remaining

Done

EtherPeek NX Capture 1:

Packet	Source	Destination	Flags	Size	Absolute Time	Protocol	St
1	IP-192.168.30.1	IP Broadcast		90	11:35:58.217093	UDP RIP	
2	IP-192.168.40.1	IP Broadcast		70	11:35:58.561812	UDP RIP	
3	00:05:32:CE:BB:C3	Mcast 802.1d Brid...	*	64	11:35:59.339107	802.1	
4	IP-192.168.30.67	IP-192.168.30.250		66	11:36:00.698706	TCP HTTP	.
5	IP-192.168.30.250	IP-192.168.30.67		66	11:36:00.698949	TCP HTTP	..
6	IP-192.168.30.67	IP-192.168.30.250		64	11:36:00.698951	TCP HTTP	..
7	IP-192.168.30.67	IP-192.168.30.250		369	11:36:00.699628	TCP HTTP	/
8	IP-192.168.30.250	IP-192.168.30.67		248	11:36:00.705182	TCP HTTP	..
9	IP-192.168.30.67	IP-192.168.30.250		425	11:36:00.708646	TCP HTTP	/
10	IP-192.168.30.250	IP-192.168.30.67		197	11:36:00.710539	TCP HTTP	..
11	IP-192.168.30.67	IP-192.168.30.250		66	11:36:00.711829	TCP HTTP	..
12	IP-192.168.30.250	IP-192.168.30.67		66	11:36:00.711879	TCP HTTP	..
13	IP-192.168.30.67	IP-192.168.30.250		64	11:36:00.712005	TCP HTTP	..
14	IP-192.168.30.67	IP-192.168.30.250		425	11:36:00.712946	TCP HTTP	/
15	IP-192.168.30.67	IP-192.168.30.250		425	11:36:00.713640	TCP HTTP	/
16	IP-192.168.30.250	IP-192.168.30.67		197	11:36:00.715125	TCP HTTP	..
17	IP-192.168.30.67	IP-192.168.30.250		425	11:36:00.716231	TCP HTTP	/
18	IP-192.168.30.250	IP-192.168.30.67		197	11:36:00.716760	TCP HTTP	..
19	IP-192.168.30.67	IP-192.168.30.250		425	11:36:00.717946	TCP HTTP	/
20	IP-192.168.30.250	IP-192.168.30.67		197	11:36:00.718631	TCP HTTP	..
21	IP-192.168.30.250	IP-192.168.30.67		197	11:36:00.720235	TCP HTTP	..

Done

Secure Coding Training

Targeted at enhancing developer skills and capabilities.

Secure Coding in C and C++

- Addison-Wesley book

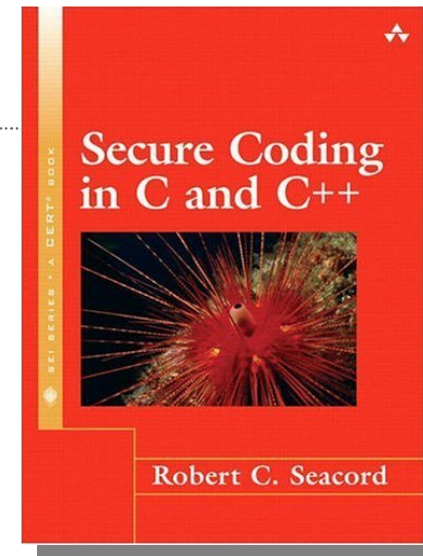
Training courses

- Direct offerings
- Partnered with industry
- University course offerings

Secure string and integer library development

Secure coding web pages

<http://www.cert.org/secure-coding/>



Overview

- CERT/CC
- CSIRTs with National Responsibility
- Partnerships and Trust
- Training
- **Conclusion**

Conclusions

- National CSIRTs provide a conduit for communications and coordination
- Partnerships are needed for successful response and prevention of incidents
- Help establish trusted relationships with vendors, government and academia
- Established principles to handle information in a trustworthy manner
- Provide technical expertise in various areas
- Industry and Private sector CSIRTs are necessary
- Value added analysis and services

Document Resources

Handbook for Computer Security Incident Response Teams (CSIRTs)

<http://www.cert.org/archive/pdf/csirt-handbook.pdf>

Steps for Creating National CSIRTs

<http://www.cert.org/archive/pdf/NationalCSIRTs.pdf>

Action List for Developing a Computer Security Incident Response Team (CSIRT)

http://www.cert.org/csirts/action_list.html

Creating a Computer Security Incident Response Team: A Process for Getting Started

<http://www.cert.org/csirts/Creating-A-CSIRT.html>

CSIRT Services

<http://www.cert.org/csirts/services.html>

More available at: <http://www.cert.org/csirts>

For more information...

National CSIRT contact list:

<http://www.cert.org/csirts/national/contact.html>

<http://www.cert.org/csirts/national/>

CSIRT and Technical Training:

<http://www.cert.org/csirts/>

<http://vte.cert.org>

<http://www.cert.org/secure-coding/>

CERT/CC:

<http://www.cert.org>