

# CEIC<sup>®</sup> 2014

## Responding to a Cyber Security Incident

A Real World Customer Example

[www.encase.com/ceic](http://www.encase.com/ceic)

### Responding to a Cyber Security Incident

**CEIC 2014**

#### Intro

#### Jasen Yens

- EnCE<sup>®</sup>-certified digital investigations specialist and a principal consultant at Guidance Software. He has over 15 years of experience in the security industry.

Page 2

## Responding to a Cyber Security Incident

**CEIC 2014**

### Intro

Recognized globally as the world leader in e-discovery and digital investigations, Guidance Software and our EnCase® software solutions provide the foundation for organizations to conduct thorough and effective computer investigations of any kind, including intellectual property theft, incident response, compliance auditing and responding to e-discovery requests—all while maintaining the forensic integrity of the data.

Guidance Software works with businesses around the world, in a wide variety of industries, including financial services, technology, defense, energy, pharmaceutical, manufacturing and retail.

Page 3

## Responding to a Cyber Security Incident

**CEIC 2014**

### Agenda

- Cybersecurity overview
- Drivers for EnCase Cybersecurity
- Response Phases
- EnCase IR checklist
- Encase Users
- Cybersecurity in Action
- Questions

Page 4

## Responding to a Cyber Security Incident

CEIC 2014

### EnCase Cybersecurity Implementation

- EnCase Infrastructure Deployment to Production for a Single Site
- Project Planning and Management
- Hardware
- System Architecture, Networking and Security Model Design
- Software Installation and Functional Testing
- Production Acceptance Testing
- Operational Run books / Use Cases
- Fault Tolerance Planning
- EnCase Administrator Instruction

Page 5

## Responding to a Cyber Security Incident

CEIC 2014

### EnCase Cybersecurity Features

Feature	Description
Kernel-level Scans	Locates deleted, in use and otherwise hard-to-see data locations
System Integrity Assessments	Expose unknowns and known bad via scheduled audits
Large-scale Volatile Data Analysis	Discover system anomalies and similarities, expose attack artifacts
Near-match Analysis	Expose iterations of morphed code and variations of detected threats
Deep Forensic Analysis	Completely and thoroughly investigate any anomaly or breach
Built-in Data Search Templates	Available for PII data and configurable for other formats (account numbers, IP, etc.)
Scheduling	Program scans to run once, weekly or monthly, at the day and time of your choice
Web-based Review	Review and tag searched files using web tool; designed for collaboration
Remediation	Immediate address risk by killing running process and wiping related disk artifacts
Integration with SIEM and Alerting Systems	Visibility into potentially affected hosts the moment an alert is generated

Page 6

## Responding to a Cyber Security Incident

CEIC 2014

### EnCase Cybersecurity Overview

#### REAL-TIME AND ON-DEMAND INCIDENT RESPONSE

- Validate & triage threats
- Locate other instances of the threat
- Remove malware files and kill malicious processes

#### SENSITIVE DATA DISCOVERY

- Locate where sensitive data resides across the enterprise for security and compliance purposes
- Wipe off sensitive data stored in unauthorized locations



Page 7

## Responding to a Cyber Security Incident

CEIC 2014

### Drivers for EnCase Cybersecurity

#### Proactive

- Regulatory scans driven by business (Banking, Retail, Healthcare, Government, etc.)
- Unapproved applications

#### Reactive

- Cyber-forensics triage, analysis, volatile data, and remediation
- Data leakage
- Stolen Intellectual property

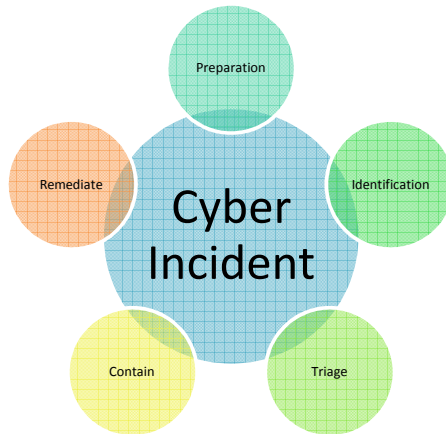


Page 8

## Responding to a Cyber Security Incident

CEIC 2014

### Incident Response Phases



Page 9

## Master Title

CEIC 2014

### Response Style – Fast & Nimble

#### Pro's

- Fast Response
- No approval process
- Any tools or combination of tools can be used.

#### Con's

- Often steps taken are not clearly documented
- Tools used are not often validated
- Can cause conflict with change controls and other internal processes



Page 10

## Responding to a Cyber Security Incident

CEIC 2014

### Response Style - Slow and Calculated

#### Pro's

- All response steps are clearly documented
- Tools used are validated before use
- Clear communication
- Repeatable

#### Con's

- Quick changes cannot be made
- All changes require formal approval (Can't skip the line)



Page 11

## Responding to a Cyber Security Incident

CEIC 2014

### Response Style - Hybrid

#### Pro's

- Uses the best of 'Fast and nimble 'and 'Slow and calculated'



Page 12

## Responding to a Cyber Security Incident

CEIC 2014

### EnCase IR checklist

- Number of Examiner machines
- Examiner Profile Configuration
- Target Machines that have servlet
- Servlet deployment strategy
- Any updates that need to be applied
- Storage (Room for Growth)



Page 13

## Responding to a Cyber Security Incident

CEIC 2014

### Capture

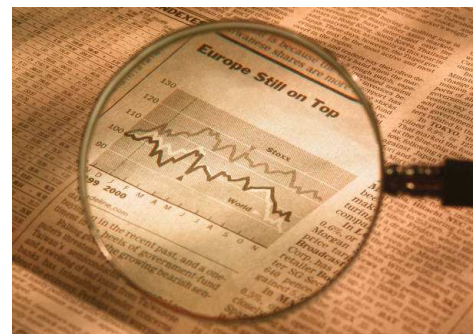
Sample can be captured from a number of different sources.

Preserve evidence in a Logical Evidence File or Encase Evidence file

You don't lose malware files on your network

Full forensic images for deeper dives in depth analysis

Logical evidence files for loose file collection of artifacts



Page 14



## Responding to a Cyber Security Incident

CEIC 2014

### Analysis

- Hash Analysis
- Date and Time
- File Signature
- Memory Analysis
- Cybersecurity Modules



Page 15

## Responding to a Cyber Security Incident

CEIC 2014

### Encase Clients / Users separation of duties

- Internal Investigations
- System Administrators
- CISO
- Legal
- Security Operation Center
- Auditors
- Others



Page 16



## Responding to a Cyber Security Incident

CEIC 2014

### Indicators

- PSEXEC.exe, A.bat, 1.exe, and AMC.exe found in the following location C:\\$Recycle.BIN
- AMC.exe running as a service
- Email containing the attached PDF AEROSPACE.pdf
- Search registry keys
- MD5 Hash '0999db84e16adf64c15a7b8039484b33'
- URL History search
- Prefetch



Page 17

## Responding to a Cyber Security Incident

CEIC 2014

### Cybersecurity in Action

1. Metadata scan for listed indicators
2. Cybersecurity Modules
3. Analysis
4. Process remediation
5. File remediation
6. 2<sup>nd</sup> Pass
7. Conclusion

Page 18

**Master Title**

**CEIC 2014**

## Questions

JASEN YENS

[JASEN.YENS@GUIDANCESOFTWARE.COM](mailto:JASEN.YENS@GUIDANCESOFTWARE.COM)



Page 19