OWASP AppSensor Project
Patterns for Logging, Architecture & Signalling

- Colin Watson
  colin.watson(at)owasp.org

- Application-specific attack detection
- Logging
- Architectures
- Signalling
- Example web applications
- Dashboard demonstrations
One issue

- Advanced attackers
Two questions

1) Is the application being attacked now?

2) Have any unknown vulnerabilities been exploited today?

☐ Yes   ☐ No   ☐ Don't know
Three test cases

1) Stepping through a process in the incorrect order
   Step five, /step5/
   then step two /step2/

2) Requesting an unauthorised resource identifier
   Show my account, /updateProfile?id=1005
   then show me someone else's /updateProfile?id=1006

3) Payment transfer exceeding limit
   Send 27 pounds, /transfer?amount=27.00
   then send rather more /transfer?amount=270000
Four conventional defenses

1) Transport layer security (TLS, formerly SSL)

2) Firewall

3) Deep packet inspection

4) Web application firewall
Transport layer security (SSL)

3) Payment transfer exceeding limit

Send 27 pounds, then send rather more

/transfer?amount=27.00
/transfer?amount=270000

☐ Protected  ✗ Unprotected
3) Payment transfer exceeding limit

Send 27 pounds,
then send rather more

```
/transfer?amount=27.00
/transfer?amount=270000
```

- Protected
- Unprotected
Deep packet inspection

1) Stepping through a process in the incorrect order
   Step five, then step two

☐ Protected  ☒ Unprotected
2) Requesting an unauthorised resource identifier

Show my account,
then show me someone else's

/updateProfile?id=1005
/updateProfile?id=1006

☐ Protected  ☒ Unprotected
Proper attack detection

• Integrated
  • Understands the application
  • Understands normal vs. suspicious use
  • Updated when the business process changes

• Effective
  • Minimal false positives
  • Immediate response

• Scalable
  • Automatic detection
  • Real time
Inside the application

• Applications have:
  • Full knowledge of the business logic
  • An understanding of the roles & permissions of users
  • Knowledge of malicious vs. normal use
  • Access to user and system history and trends
  • Information to instantly detect attackers
  • The ability to respond automatically in real-time such as taking a more defensive posture
Some things your application may already do

- Blocking certain HTTP verbs
- Terminating a request when blacklisted inputs are received
- Fraud detection
- Adding time delays to each successive failed authentication attempt
- Locking a user account after a number of failed authentication attempts
- Application honey pot functionality
- Logging a user out when they use the browser's “back” button
- Terminating a session if a user's geo-location changes
- Blocking access by certain IP addresses when malicious behaviour is detected
- Disable non-core function
- Recording unexpected actions
- Application logging
Attack-Aware with Active Defences

1) Event detection
2) Analysis
3) Attack determination
4) Response selection
5) Response execution
Application attack detection points

- Request
- Authentication
- Session
- Access control
- Input
- Encoding
- Command injection
- File input/output
- Honey trap

- User trend
- System trend
- Reputation

- Custom
Detecting Malicious Users

- “Users” are not perfect

Unacceptable | Acceptable
Malicious Attacks | Normal Application Use

- Application-specific actions

Unacceptable | Acceptable
Reject | Accept
Ask for Re-entry | Accept but Sanitize
Importance of Context

- Server-side validation only

- Server-side with duplicate client-side validation
Unknown attacks

• [This list is intentionally left blank]
Conventional attack responses

- No change (e.g. just continue logging)
- Process terminated (e.g. reset connection)
Full spectrum responses

- **No change**
- Logging increased
- Administrator notification
- Other notification (e.g. other system)
- Proxy
- User status change
- User notification
- Timing change
- **Process terminated**
- Function amended
- Function disabled
- Account log out
- Account lock out
- Application disabled
- Collect data from user
Further Explanations and Detailed Documentation

- Video presentations by Michael Coates, AppSensor Project Leader:
  - Automated Application Defenses to Thwart Advanced Attackers, June 2010
    http://michael-coates.blogspot.com/2010/06/online-presentation-thursday-automated.html
  - Attack Aware Applications, April 2011
    https://www.owasp.org/index.php/Minneapolis_St_Paul#tab=Video.2FAudio.2FSlides.2FHandouts

- Videos of AppSensor attack detection demonstrations:
  - AppSensor Project media
    https://www.owasp.org/index.php/Minneapolis_St_Paul#tab=Video.2FAudio.2FSlides.2FHandouts

- Written guidance:
    https://www.owasp.org/images/2/2f/OWASP_AppSensor_Beta_1.1.pdf
  - Implementation Planning Methodology, Colin Watson, 2010
  - Developer Guide (for use with ESAPI)
Implementation

- New project requirements
- Retrofitting existing applications
- Preliminary requirements
  - Application logging
  - Application risk assessment
  - Secure coding
- Monitoring and tuning
Architectures
Architectures (continued)
Architectures (continued)
Application Logging Inspiration

• See:

  • How to Do Application Logging Right, Anton Chuvakin and Gunnar Peterson, IEEE Security & Privacy Journal
    http://arctecgroup.net/pdf/howtoapplogging.pdf

  • OWASP ESAPI Logger (Java), OWASP

• See also:

  • SP 800-92 Guide to Computer Security Log Management, NIST

  • OWASP Logging Project, OWASP
    https://www.owasp.org/index.php/Category:OWASP_Logging_Project#tab=Main

• Some commentary:

  • Application Security Logging, (own blog)

  • AppSensor Project Mailing List, OWASP
## Application Event Logging Aspiration

<table>
<thead>
<tr>
<th>When</th>
<th>Request</th>
<th>Who/what</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event date/time</td>
<td>Purpose</td>
<td>Source</td>
</tr>
<tr>
<td>Log date/time</td>
<td>Target</td>
<td>User identity</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Security Event</th>
<th>AppSensor Detection</th>
<th>Extra?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Sensor ID</td>
<td>Request headers</td>
</tr>
<tr>
<td>Severity</td>
<td>Sensor location</td>
<td>Request body</td>
</tr>
<tr>
<td>Confidence</td>
<td>AppSensor ID(s)</td>
<td>Response headers</td>
</tr>
<tr>
<td>Custom classifications</td>
<td>Description</td>
<td>Response body</td>
</tr>
<tr>
<td>Owner</td>
<td></td>
<td>Error stack trace</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Location</th>
<th>Result</th>
<th>Record integrity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>Status</td>
<td>Identity</td>
</tr>
<tr>
<td>Service/application name</td>
<td>Reason for status</td>
<td>Hash</td>
</tr>
<tr>
<td>Port</td>
<td>HTTP status code</td>
<td></td>
</tr>
<tr>
<td>Protocol</td>
<td>AppSensor Result ID(s)</td>
<td></td>
</tr>
<tr>
<td>HTTP method</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>Entry point</td>
<td>Message</td>
<td></td>
</tr>
<tr>
<td>Request number</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
AppSensor Signalling

- Standards
  - Common Event Format (CEF)
  - Common Event Expression (CEE)
- Custom
  - Devices elsewhere on the network
    - Firewalls
    - Web application firewalls
    - Traffic management
  - Other business systems
    - Management reporting
    - CRM
    - Correlation engines (e.g. fraud management)
- Broadcasting
- Third parties
Common Event Format

• Prefix
  • Timestamp Host Message
    • June 10 16:48:53 appserver02 Message

• Message
  • CEF:Version|Device Vendor|Device Product|Device Version|Signature ID|Name|Severity|Extension
    • CEF:0|widgetco|shoponline|3.7.03|R03|XSS attempt blocked|7|Extension

• Extension
  • Collection key-value pairs
    - Predefined keys
    - Device custom strings and numbers (x6)
    - Custom dictionary extensions
Common Event Format (continued)

- src=10.25.102.65
- suser=W0005
- proto=TCP
- dpt=80
- dproc=httpd
- request=/catalogue/showProduct/
- requestMethod=GET
- deviceExternalID=AppSensor06
- msg=Cross site scripting attempt in parameter prodid
- cat=detection
- act=block
- cs1Label=requestClientApplication cs1=Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10.6; en-GB; rv:1.9.2.17) Gecko/20110420
- cs2Label=AppSensorSensorID cs2=R03
- cs3Label=AppSensorDetectionType cs3=IE1
- cs4Label=StatusCode cs4=403
- cn1Label=RequestID cn1=000070825566
- cn2Label=AppSensorLogID cn2=1650833
- cn3Label=Confidence cn3=100
Common Event Format (continued)

1. Auth Failed Event
   <165>Jun 08 20:47:29 someapp.mozilla.com CEF:0|mozilla|someapp|1.3|AuthFail|User Authentication Failed|5|
   cs1Label=requestClientApplication cs1=Mozilla/5.0 (Windows; U; Windows NT 5.1; id; rv:1.9.2.17) Gecko/20110420
   FireDownload/2.0.1 Firefox/3.6.17 96690903 Service 2.02155 requestMethod=GET
   request=https://someapp.mozilla.com/1.0/someuser/info/collections src=1.2.3.4 dst=2.3.4.5 suser=joeuser

2. Invalid Channel Event (custom event)
   <166>Jun 08 20:48:42 someapp.mozilla.com CEF:0|mozilla|someapp|1.3|Invalid X-KeyExchange-Channel|Invalid X-
   KeyExchange-Channel|5|cs1Label=requestClientApplication cs1=Mozilla/5.0 (Windows NT 6.1; rv:2.0b9)
   Gecko/20100101 Firefox/4.0b9 requestMethod=GET request=/4xjq src=1.2.3.4 dest=someapp.mozilla.com
   suser=joeuser

3. Username does not match URL (custom event)
   <165>Jun 08 20:50:16 someapp.mozilla.com CEF:0|mozilla|someapp |1.3|AuthFail|Username Does Not Match URL|7|
   cs1Label=requestClientApplication cs1=Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.2.17) Gecko/20110420
   Firefox/3.6.17 (.NET CLR 3.5.30729; .NET4.0C) requestMethod=GET
   request=https://someapp.mozilla.com/1.0/bobuser/info/collections src=1.2.3.4 dst=2.3.4.5 cs2Label=url_user
   cs2=joeuser suser=joeuser

4. Password Changed (System trend)
   <166>Jun 08 20:52:08 someapp.mozilla.com CEF:0|mozilla|someapp|1.3|PasswordReset|Password Changed|5|
   cs1Label=requestClientApplication cs1=Mozilla/5.0 (Macintosh; Intel Mac OS X 10.6; rv:2.0.1) Gecko/20100101
   Firefox/4.0.1 requestMethod=POST request=/forgot src=1.2.3.4 dest=someapp.mozilla.com suser=joeuser
## Application Event Logging Aspiration

<table>
<thead>
<tr>
<th>When</th>
<th>Request</th>
<th>Who/what</th>
<th>Security Event</th>
<th>Extra?</th>
<th>Record integrity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event date/time</td>
<td>Purpose</td>
<td>Source</td>
<td>Type</td>
<td>Request headers</td>
<td>Identity</td>
</tr>
<tr>
<td>Log date/time</td>
<td>Purpose</td>
<td>User identity</td>
<td>Severity</td>
<td>Request body</td>
<td>Hash</td>
</tr>
<tr>
<td></td>
<td>Purpose</td>
<td>HTTP User Agent</td>
<td>Confidence</td>
<td>Response headers</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Purpose</td>
<td></td>
<td>Custom classifications</td>
<td>Response body</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Target</td>
<td></td>
<td>Owner</td>
<td>Error stack trace</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Error message</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Location</th>
<th>AppSensor Detection</th>
<th>Extra?</th>
<th></th>
<th>Record integrity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>Sensor ID</td>
<td>Request headers</td>
<td></td>
<td>Identity</td>
</tr>
<tr>
<td>Service/application name</td>
<td>Sensor location</td>
<td>Request body</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Port</td>
<td>AppSensor ID(s)</td>
<td>Response headers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Protocol</td>
<td>Description</td>
<td>Response body</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HTTP method</td>
<td></td>
<td>Error stack trace</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Entry point</td>
<td></td>
<td>Error message</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Request number</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Result</th>
<th>Extra?</th>
<th>Record integrity</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Request headers</td>
<td>Identity</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reason for status</td>
<td>Request body</td>
<td>Hash</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HTTP status code</td>
<td>Response headers</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AppSensor Result ID(s)</td>
<td>Description</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Message</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Extra?</th>
<th>Record integrity</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Request headers</td>
<td>Request headers</td>
<td>Identity</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Request body</td>
<td>Request headers</td>
<td>Hash</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Response headers</td>
<td>Response headers</td>
<td>Identity</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Response body</td>
<td>Response headers</td>
<td>Hash</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Error stack trace</td>
<td>Response headers</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Error message</td>
<td>Response headers</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identity</td>
<td>Request headers</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hash</td>
<td>Request headers</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
No 1 - Ecommerce Website Base Configuration

• Key risks
  • Product pricing errors, discounts and fiddles
  • Order process manipulation
  • Payment card mis-use
  • Personal data loss
• AppSensor detection points
  • General request filtering
  • Catalogue, basket and payment functions
  • Database
## No 1 - Detection Points

<table>
<thead>
<tr>
<th>Area</th>
<th>Identifier</th>
<th>#</th>
<th>AppSensor ID(s)</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Request</td>
<td>R01</td>
<td>R</td>
<td>RE1, RE2, RE3, RE4</td>
<td>Invalid and incorrect HTTP verb</td>
</tr>
<tr>
<td></td>
<td>R02</td>
<td>R</td>
<td>CIE1</td>
<td>SQL injection attempt</td>
</tr>
<tr>
<td></td>
<td>R03</td>
<td>R</td>
<td>IE1</td>
<td>Cross site scripting (XSS) attempt</td>
</tr>
<tr>
<td>Catalogue</td>
<td>C01</td>
<td>IE4</td>
<td></td>
<td>Product value mismatch</td>
</tr>
<tr>
<td>Basket</td>
<td>B01</td>
<td>IE4</td>
<td></td>
<td>Basket value mismatch</td>
</tr>
<tr>
<td>Payment</td>
<td>P01</td>
<td>-</td>
<td></td>
<td>Card authorisation failure</td>
</tr>
<tr>
<td></td>
<td>P02</td>
<td>IE4</td>
<td></td>
<td>Price mismatch between order and payment</td>
</tr>
<tr>
<td>Database</td>
<td>D01</td>
<td>+</td>
<td>CIE2</td>
<td>Returned record set size incorrect</td>
</tr>
<tr>
<td></td>
<td>D02</td>
<td>+</td>
<td>IE5</td>
<td>Database table integrity fault</td>
</tr>
</tbody>
</table>

AppSensor detection point type identities and descriptions

## No 1 – Response Actions

<table>
<thead>
<tr>
<th>Area/Sensors</th>
<th>Description</th>
<th>Threshold</th>
<th>AppSensor ID(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Request</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>R01, R02, R03</td>
<td>Block request</td>
<td>1</td>
<td>G</td>
</tr>
<tr>
<td></td>
<td>Log out authenticated user</td>
<td>3</td>
<td>J</td>
</tr>
<tr>
<td></td>
<td>Block IP address (and customer account if known) for whole site (manual reset)</td>
<td>6</td>
<td>L (and K)</td>
</tr>
<tr>
<td>Catalogue/Basket</td>
<td>Alert operations staff</td>
<td>1</td>
<td>B</td>
</tr>
<tr>
<td>C01, C02</td>
<td>Block IP address for dynamic areas (1 day, auto reset)</td>
<td>2</td>
<td>I</td>
</tr>
<tr>
<td>Payment</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>P01</td>
<td>Alert operations staff / Redirect back to from checkout pages to the shopping basket summary</td>
<td>3</td>
<td>B / G</td>
</tr>
<tr>
<td>Payment</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>P02</td>
<td>Alert operations staff / Put order on hold / Block future order check-out for the customer (manual reset)</td>
<td>1</td>
<td>B / D / I</td>
</tr>
<tr>
<td>Database</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>D01</td>
<td>Alert operations staff / Abort process / Display error page / Block customer account (manual reset)</td>
<td>1</td>
<td>B / G / E / K</td>
</tr>
<tr>
<td>Database</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>D02</td>
<td>Alert DBA and operations staff</td>
<td>1</td>
<td>B</td>
</tr>
<tr>
<td>[All]</td>
<td>Increase application logging granularity / Indicate on monitoring dashboard</td>
<td>1</td>
<td>A / C</td>
</tr>
</tbody>
</table>

AppSensor response action type identities and descriptions

https://www.owasp.org/index.php/AppSensor_ResponseActions
No 2 - Ecommerce Website Advanced Configuration

- Additional requirements
  - Greater granularity of input validation issues
  - Shopping basket and order processing session checks
  - User and system trends
  - Integration with reputation monitoring
- Additional AppSensor detection points
  - Valid parameter names and application entry points
  - Integrity checks on user submitted data
  - User trend for orders completed
  - System trends for site utilisation, and catalogue/basket/payment usage
  - Third party malware monitoring feed
  - Intrusion Protection System feed
## No 2 - Detection Points

<table>
<thead>
<tr>
<th>Area</th>
<th>Identifier</th>
<th>#</th>
<th>AppSensor ID(s)</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Request</td>
<td>R04</td>
<td>R</td>
<td>RE5, RE6</td>
<td>Extra/duplicated/missing input parameter</td>
</tr>
<tr>
<td></td>
<td>R05</td>
<td>R</td>
<td>ACE3</td>
<td>Invalid dynamic entry point (force browsing)</td>
</tr>
<tr>
<td>Catalogue</td>
<td>C02</td>
<td>+</td>
<td>IE2</td>
<td>Input validation white list exception</td>
</tr>
<tr>
<td></td>
<td>C03</td>
<td>+</td>
<td>ACE1, ACE2</td>
<td>Parameter manipulation for direct object access</td>
</tr>
<tr>
<td></td>
<td>C04</td>
<td></td>
<td>HT2</td>
<td>“Magic” product accessed</td>
</tr>
<tr>
<td>Basket</td>
<td>B02</td>
<td>+</td>
<td>IE2</td>
<td>Input validation white list exception</td>
</tr>
<tr>
<td></td>
<td>B03</td>
<td>S</td>
<td>SE1</td>
<td>Shopping basket cookie altered</td>
</tr>
<tr>
<td></td>
<td>B04</td>
<td>S</td>
<td>SE4</td>
<td>Shopping basket cookie substitution</td>
</tr>
<tr>
<td>Payment</td>
<td>P03</td>
<td>+</td>
<td>IE2</td>
<td>Input validation white list exception</td>
</tr>
<tr>
<td></td>
<td>P04</td>
<td></td>
<td>IE4</td>
<td>Input data integrity exception</td>
</tr>
<tr>
<td></td>
<td>P05</td>
<td>S</td>
<td>SE4</td>
<td>Payment cookie substitution</td>
</tr>
<tr>
<td>External</td>
<td>E01</td>
<td></td>
<td>RP4</td>
<td>Malware identified in site content by remote system</td>
</tr>
<tr>
<td></td>
<td>E02</td>
<td></td>
<td>RP2</td>
<td>Network Intrusion Protection System (IPS) alert</td>
</tr>
<tr>
<td>User Trend</td>
<td>U01</td>
<td></td>
<td>UT4</td>
<td>High rate of order placement</td>
</tr>
<tr>
<td>System Trend</td>
<td>S01</td>
<td></td>
<td>STE3</td>
<td>High or Low rate of general page impressions</td>
</tr>
<tr>
<td></td>
<td>S02</td>
<td></td>
<td>STE3</td>
<td>High or Low rate of catalogue page impressions</td>
</tr>
<tr>
<td></td>
<td>S03</td>
<td></td>
<td>STE3</td>
<td>High or Low rate of shopping baskets creation</td>
</tr>
<tr>
<td></td>
<td>S04</td>
<td></td>
<td>STE3</td>
<td>High rate of shopping basket deletion</td>
</tr>
<tr>
<td></td>
<td>S05</td>
<td></td>
<td>STE3</td>
<td>High rate of missing file (404 not found) errors</td>
</tr>
</tbody>
</table>
No 2 – Response Actions

- Overall detection point threshold set with a disruptive action
- Business layer input validation exceptions:
  - High thresholds when user data entry allowed
  - Low thresholds and disruptive response actions for clearly malicious behaviour
- Strict limits on access control exceptions
- Reputational information used to help identify site malware infection for early response
- Correlation with IPS information to block users also undertaking malicious behaviour on the network
- User trend information used to change credit rating
- System trend information used for:
  - Detection of phishing attacks and application work activity
  - Advance warning of problems such as resource exhaustion, warehouse and stock utilisation
- Never block privileged accounts, but alert and log vigorously
Dashboard demonstration

- Live (during presentation) demos for Ecommerce website
  - Base configuration
  - Advanced configuration
- Video (no sound/narration) of these demos available at:
  - Base configuration
    http://www.youtube.com/watch?v=zCaYREAyiRg
  - Advanced configuration
    http://www.youtube.com/watch?v=YZ5zGQ-XLkk
Two question revisited

1) Is the application being attacked now?

2) Have any unknown vulnerabilities been exploited today?

☐ Yes ☐ No ☐ Don't know
Make contact

Colin Watson

- colin.watson(at)owasp.org

AppSensor Project


Full-day training at AppSec USA

- Application Attack Detection & Response - A Hands-on Planning Workshop
  http://www.appsecusa.org/training.html#watson