Introduction

1. Automation needed to handle EINSTEIN (E³A) notices:
   • How can we handle large volumes of notices?
   • Can we prioritize the data?
   • Can we derive information from the data?
   • Does the aggregate of this information mean something?

2. Benefits realized:
   • Cost savings
   • Improved efficiency

3. Continuous Monitoring Strategy:
   • Security Manager
   • Risk Analyst
   • Security Analyst

4. Securely developed application

technology was developed by XLA to meet the needs of an existing EINSTEIN3 customer and continues to be used today.
xTRACT Automated Process

Data
- Notices received from EINSTEIN

E³A Notice
- Timestamp
- Reference #
- Destination
- Source (firewall)

Information
- Single or multiple notices grouped together

xTRACT Event
- Time span
- Reference #
- Network Activity
- User
- Source IP Address
- URL
- more

Knowledge
- Identified security event which requires action

Incident
- Investigation
- Trouble Ticket
- Incident Response

We MIGHT have a problem…?

We HAVE a problem!

Our problem is RIGHT HERE!!

xtract uses Notices to create Events with sufficient information for a Security Analyst to determine if an Incident has occurred.
An Incident can trigger cascading work for users across divisions, so false positive identification of Incidents reduces costs.
Multiple notices can comprise an event. Use Xtract to search across all events and notices to identify higher level Risks to the Enterprise.
Continuous Monitoring Strategy

NIST 800-137 provides different views to align with NIST 800-137.
Summary

Short term
- Ability to assess all potential threats (instead of sampling), without hiring more resources
- Reduces labor necessary to assess actual threat
- Improves relationships in organizations by targeted remediation instead of endless destruction of hard drives
- Enables customized, metrics-driven strategic risk management, tailored to each institution’s needs

Long term
- Significantly improves threat analysis and assessment rather than simple repetitive incident response
- Enables institutional behavior/policy change based on analytics

So, what can it do for my Organization…
Securely Developed Application

**OWASP Top Ten**
- A1. Cross Site Scripting (XSS)
- A2. Injection Flaws
- A3. Malicious File Execution
- A4. Insecure Direct Object Reference
- A5. Cross Site Request Forgery (CSRF)
- A6. Leakage and Improper Error Handling
- A7. Broken Authentication and Sessions
- A8. Insecure Cryptographic Storage
- A9. Insecure Communications
- A10. Failure to Restrict URL Access

**OWASP ESAPI**
- Validator, Encoder
- Encoder
- HTTPUtilities (Safe Upload)
- AccessReferenceMap, AccessController
- User (CSRF Token)
- EnterpriseSecurityException, HTTPUtils
- Authenticator, User, HTTPUtils
- Encryptor
- HTTPUtilities (Secure Cookie, Channel)
- AccessController

*implements OWASP ESAPI library.*
xtract
xla Threat Reduction, Analysis & Correlation Tool.

DEMONSTRATION
DATE/TIME (UTC) = 12/1/2014 11:07:10
PROTO = TCP
SAFE HIT SRCIP = 100.100.101.23
SRCPORT = 7555
DESTIP = 1.2.3.4
DESTPORT = 80
CUSTOMER DNS LOOKUP SRCIP = 10.8.8.12
REF# = abcd1234
Event Analysis

Use Excel’s built-in sorting and filtering features to identify risks: downloaded .exe files, large uploads, connections to strange domains or other suspicious patterns of behavior.

<table>
<thead>
<tr>
<th>Timestamp</th>
<th>User</th>
<th>Src</th>
<th>Dst</th>
<th>URL</th>
<th>Status</th>
<th>Sent</th>
<th>Rcvd</th>
</tr>
</thead>
<tbody>
<tr>
<td>7/1/14 9:12:01</td>
<td>mplanck</td>
<td>192.168.0.10</td>
<td>1.2.3.4</td>
<td></td>
<td>allowed</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>7/1/14 9:12:00</td>
<td>mplanck</td>
<td>192.168.0.10</td>
<td>80.0.1.12</td>
<td>google.com</td>
<td>allowed</td>
<td>1022</td>
<td>4320</td>
</tr>
<tr>
<td>7/1/14 9:11:59</td>
<td>mplank</td>
<td>192.168.0.10</td>
<td>12.2.6.8</td>
<td>hacker.com</td>
<td>blocked</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>7/1/14 9:11:59</td>
<td>mplank</td>
<td>192.168.0.10</td>
<td>52.1.1.12</td>
<td>malware.com</td>
<td>allowed</td>
<td>120</td>
<td>1409928</td>
</tr>
</tbody>
</table>

A Security Analyst can view network traffic before & after the notice to investigate the cause and effect and determine if an Incident has occurred.
## Event Review

### Incidents

<table>
<thead>
<tr>
<th>Incident</th>
<th>#</th>
<th>Severity</th>
<th>Notes</th>
<th>First Date</th>
<th>Last Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>info</td>
<td>testing</td>
<td>08/20/2014 12:06:04</td>
<td>08/20/2014 12:06:04</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>alert</td>
<td></td>
<td>08/08/2014 17:07:56</td>
<td>08/08/2014 17:07:56</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>info</td>
<td>N/A</td>
<td>08/07/2014 15:47:58</td>
<td>08/07/2014 15:48:06</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>warning</td>
<td></td>
<td>08/07/2014 10:37:42</td>
<td>08/07/2014 10:37:42</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>info</td>
<td>N/A</td>
<td>08/04/2014 15:58:59</td>
<td>08/04/2014 15:58:59</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>info</td>
<td>N/A</td>
<td>08/04/2014 10:48:53</td>
<td>08/04/2014 10:48:53</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>info</td>
<td>N/A</td>
<td>07/24/2014 11:51:48</td>
<td>07/24/2014 11:56:41</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>info</td>
<td>N/A</td>
<td>07/16/2014 17:15:37</td>
<td>07/16/2014 17:17:05</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>info</td>
<td>incident referred to HR</td>
<td>07/16/2014 14:59:06</td>
<td>07/16/2014 14:59:06</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>info</td>
<td>trouble ticket #01124</td>
<td>07/14/2014 20:48:19</td>
<td>07/14/2014 20:49:25</td>
</tr>
<tr>
<td>Sev</td>
<td>Total</td>
<td>Ref #</td>
<td>First Date</td>
<td>Last Date</td>
<td>Notes</td>
</tr>
<tr>
<td>-----</td>
<td>-------</td>
<td>---------</td>
<td>---------------</td>
<td>---------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>🔄</td>
<td>18</td>
<td>SAFE Hit Only</td>
<td>04/21/2014 14:23:48</td>
<td>08/20/2014 12:06:04</td>
<td>testing with really really long note...</td>
</tr>
<tr>
<td>🔄</td>
<td>5</td>
<td>abc123</td>
<td>06/26/2014 12:53:51</td>
<td>08/08/2014 17:07:56</td>
<td>n/a</td>
</tr>
<tr>
<td>🔄</td>
<td>4</td>
<td>122x34v</td>
<td>07/14/2014 20:48:19</td>
<td>08/07/2014 15:47:58</td>
<td>n/a</td>
</tr>
<tr>
<td>🔄</td>
<td>3</td>
<td>1234567</td>
<td>04/21/2014 14:23:42</td>
<td>04/21/2014 14:23:49</td>
<td>n/a</td>
</tr>
<tr>
<td>🔄</td>
<td>2</td>
<td>op987</td>
<td>07/24/2014 11:51:48</td>
<td>07/24/2014 11:56:41</td>
<td>n/a</td>
</tr>
<tr>
<td>🔄</td>
<td>1</td>
<td>zyxwv</td>
<td>07/16/2014 17:15:37</td>
<td>07/16/2014 17:15:37</td>
<td>n/a</td>
</tr>
</tbody>
</table>

**Date/Time**

07/16/2014 17:15:37

**Hit Type**

DNS with SAFE Hit

**Source**

192.168.3.216

**Destination**

1.2.3.10:80

**Users**

CPTOLEMY

**Download**

[ show ]

<table>
<thead>
<tr>
<th>Ref #</th>
<th>First Date</th>
<th>Last Date</th>
<th>Notes</th>
<th>Notices</th>
</tr>
</thead>
<tbody>
<tr>
<td>abcdxy</td>
<td>05/30/2014 15:38:07</td>
<td>05/30/2014 15:38:07</td>
<td>testing low</td>
<td>[ show ]</td>
</tr>
</tbody>
</table>
Reporting Features

Event / Notice Comparison

Event Severity by Month

Events by Status

Events by Severity

Confidential and Proprietary Excellence Always.
FOR MORE INFORMATION PLEASE CONTACT:

xtract@xla.com