OWASP London - 15th May 2014

# AppSensor Guide v2.0

Colin Watson
AppSensor Guide v2.0 Lead Author
OWASP AppSensor Project Co-Leader

© Watson Hall Ltd

# Running order

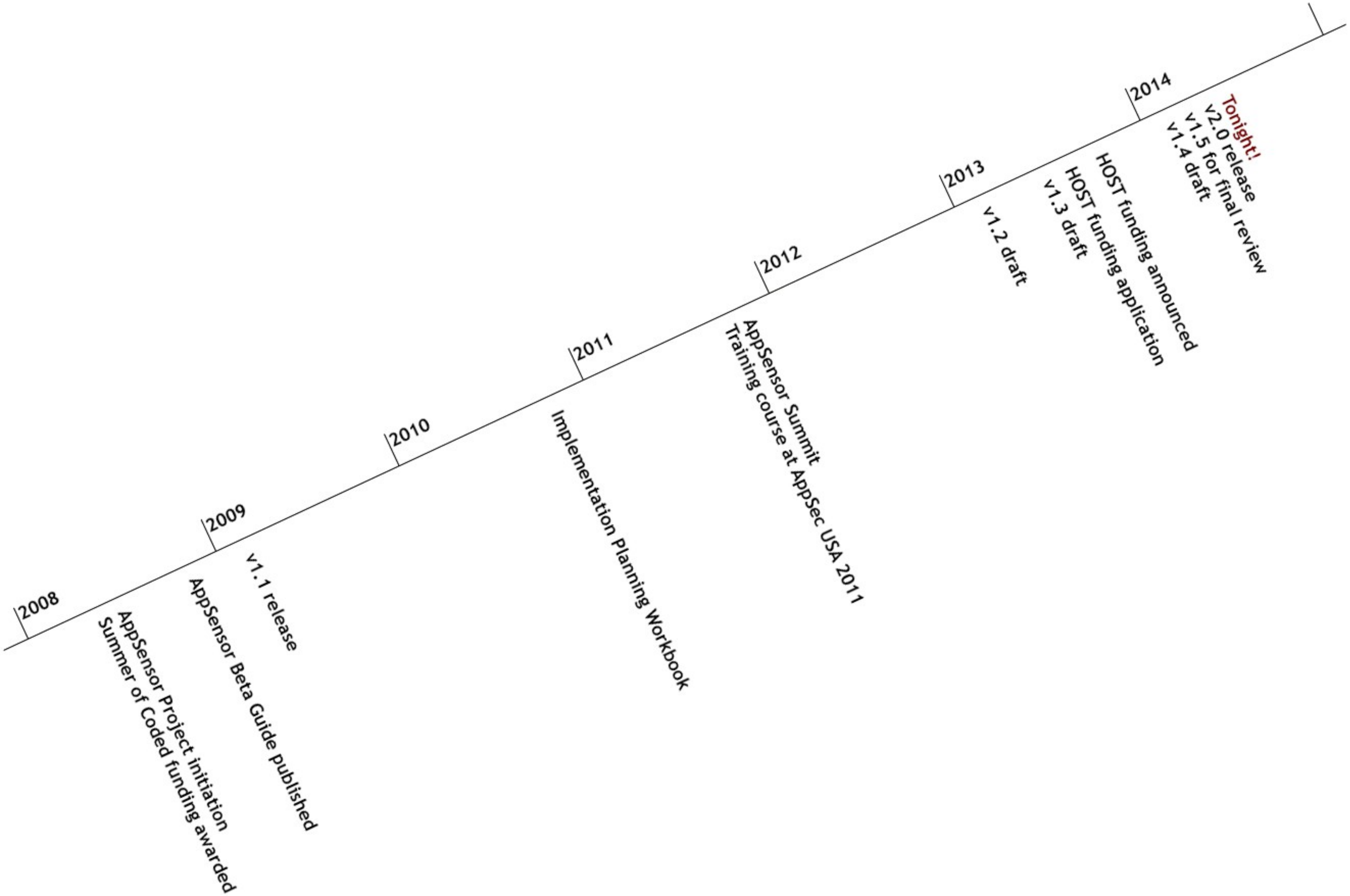
Guide v2.0

- Preamble
- Overview
- Illustrative case studies
- Making it happen
- Demonstration implementations
- Model dashboards
- Reference materials

This presentation

- Timeline
- Terminology
- Architectures
- Detection points
- Live demo
- Responses
- Case studies
- Media
- Q&A

# AppSensor Guide v2.0 timeline



2008

AppSensor Project initiation
Summer of Coded funding awarded

AppSensor Beta Guide published

2009

v1.1 release

2010

2011

Implementation Planning Workbook

2012

AppSensor Summit
Training course at AppSec USA 2011

2013

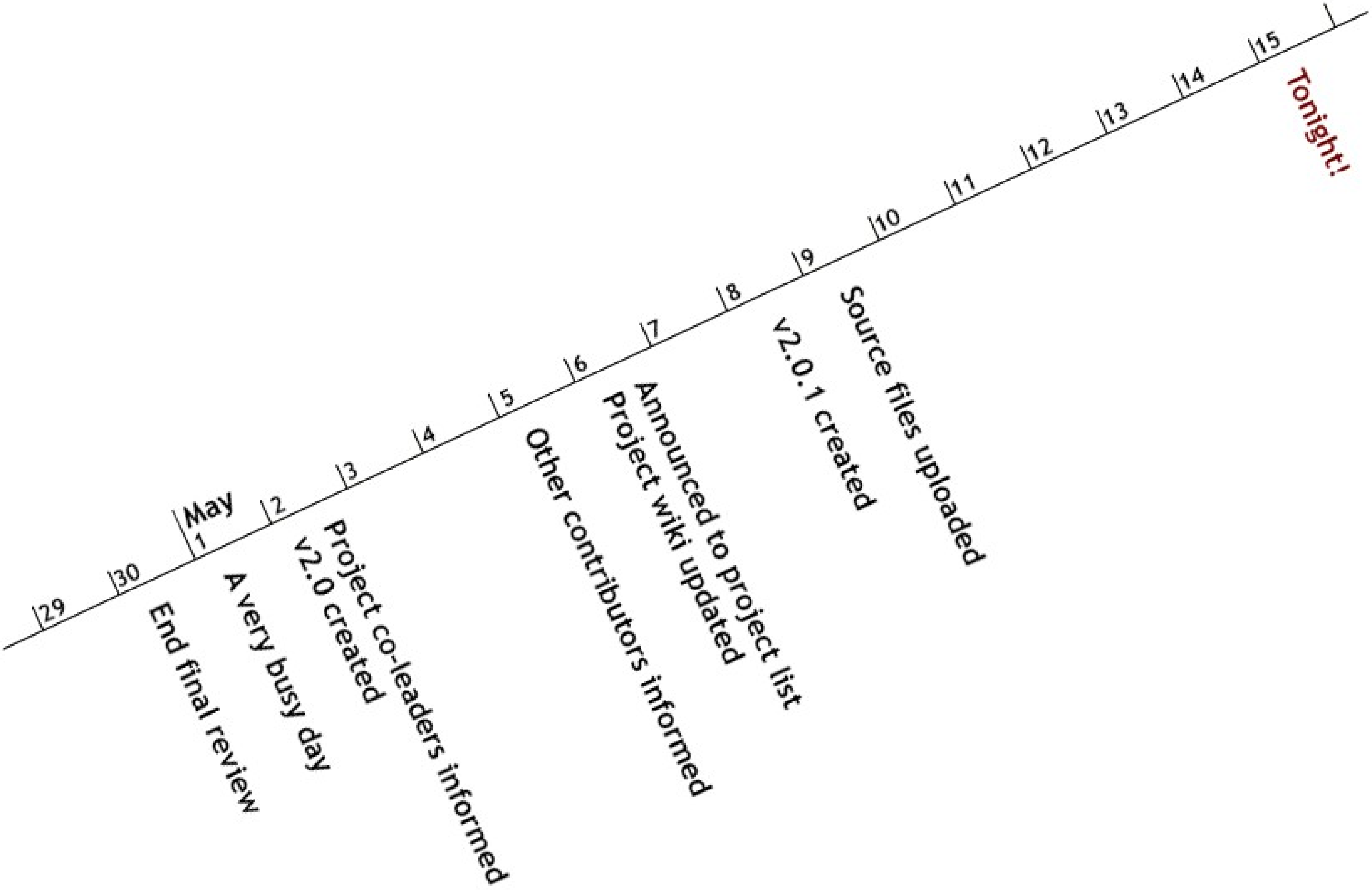
v1.2 draft

HOST funding announced
HOST funding application
v1.3 draft

2014

Tonight!
v2.0 release
v1.5 for final review
v1.4 draft

# AppSensor Guide v2.0 release timeline



End final review

A very busy day

Project co-leaders informed
v2.0 created

Other contributors informed

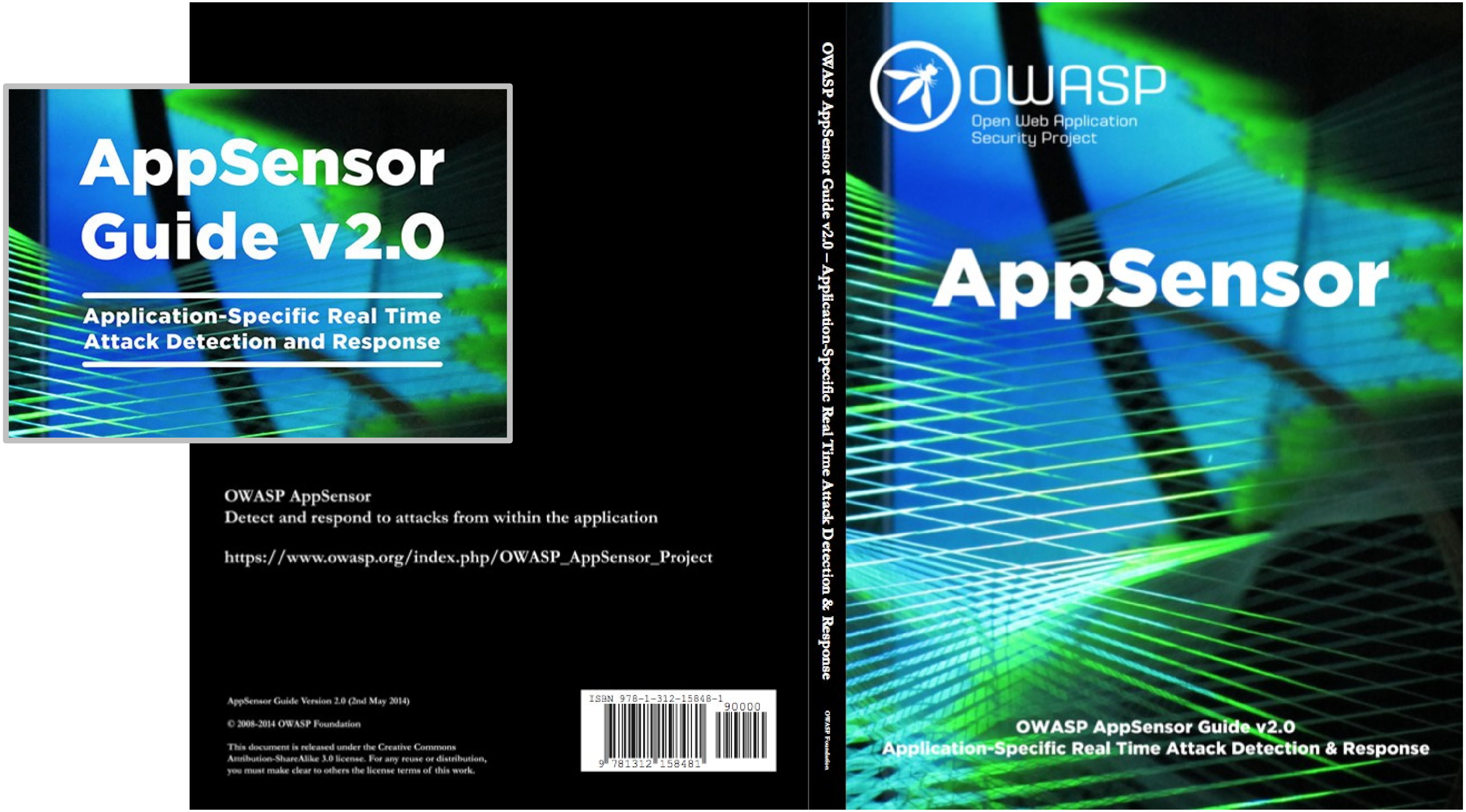
Announced to project list
Project wiki updated

v2.0.1 created

Source files uploaded

Tonight!

# Branding



AppSensor Guide v2.0

Application-Specific Real Time Attack Detection and Response

OWASP AppSensor
Detect and respond to attacks from within the application

https://www.owasp.org/index.php/OWASP_AppSensor_Project

AppSensor Guide Version 2.0 (2nd May 2014)

© 2008-2014 OWASP Foundation

This document is released under the Creative Commons Attribution-ShareAlike 3.0 license. For any reuse or distribution, you must make clear to others the license terms of this work.

ISBN 978-1-312-15848-1

OWASP AppSensor Guide v2.0 – Application-Specific Real Time Attack Detection & Response

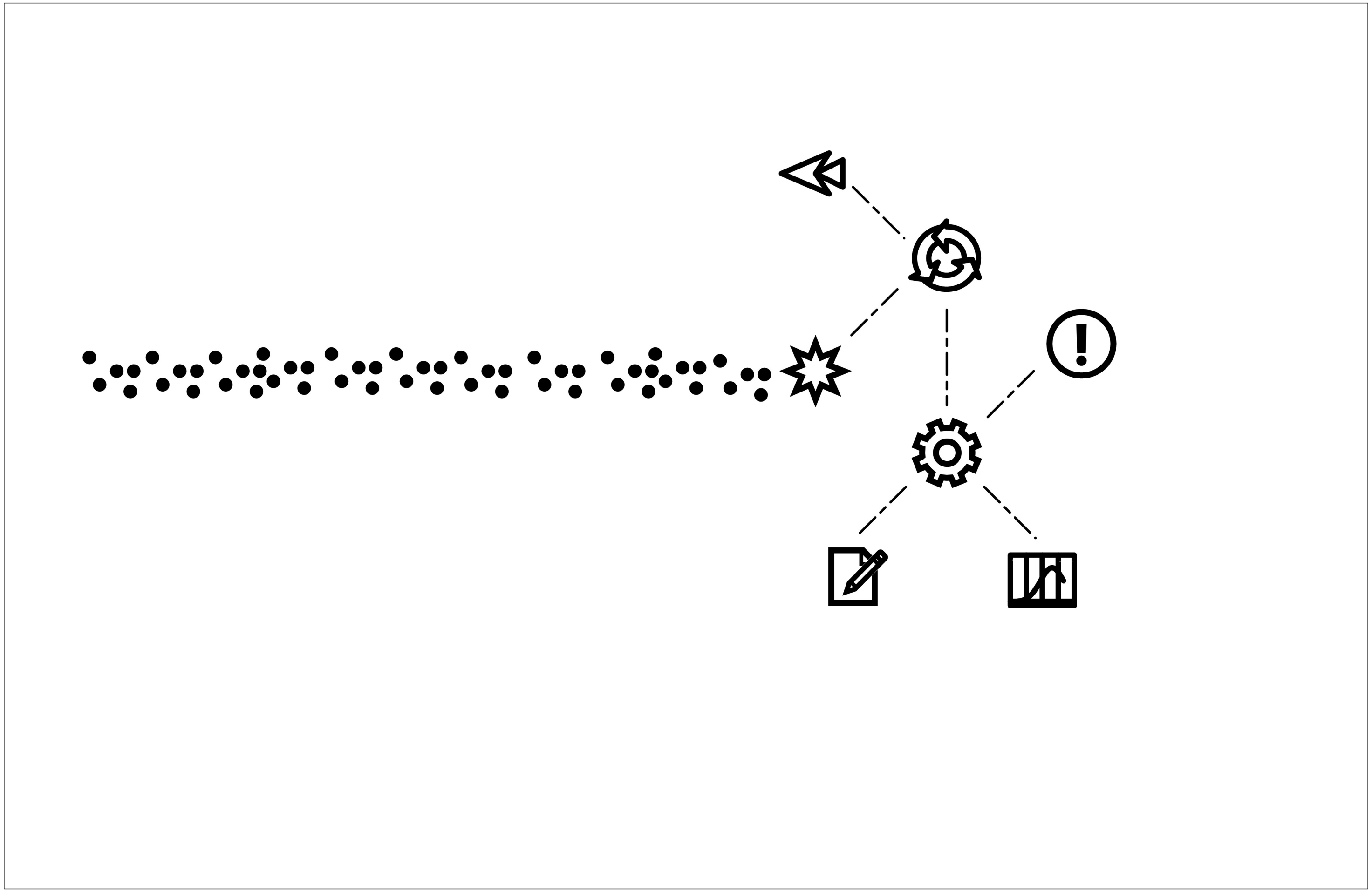
OWASP Foundation

OWASP
Open Web Application
Security Project

AppSensor

OWASP AppSensor Guide v2.0
Application-Specific Real Time Attack Detection & Response

# Terminology



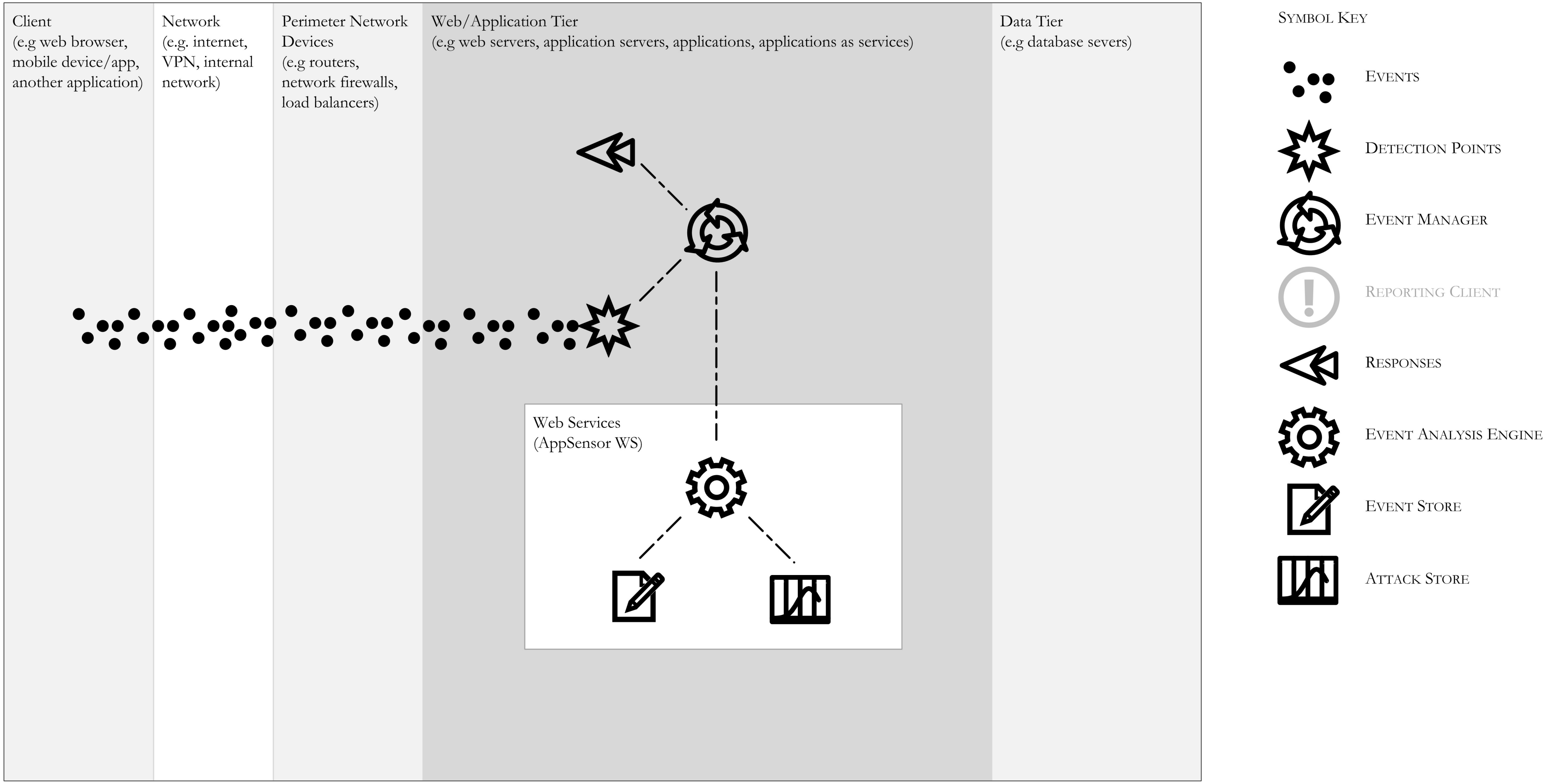
Symbol Key

- Events
- Detection Points
- Event Manager
- Reporting Client
- Responses
- Event Analysis Engine
- Event Store
- Attack Store

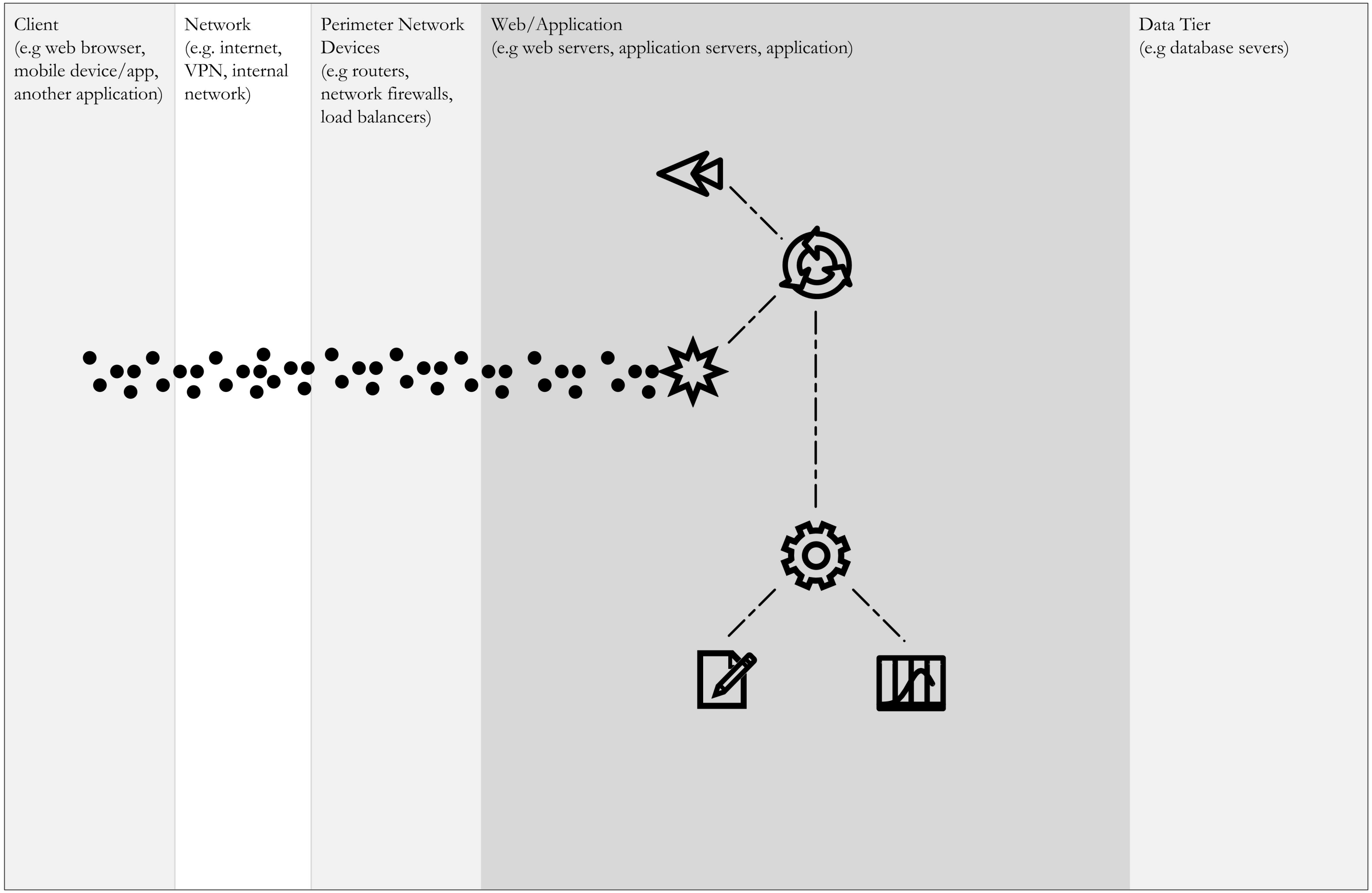
# Part IV : Demonstration Implementations

- Seven examples

# Chapter 20 : Web Services (AppSensor WS)


Client
(e.g web browser, mobile device/app, another application)
Network
(e.g. internet, VPN, internal network)
Perimeter Network Devices
(e.g routers, network firewalls, load balancers)
Web/Application Tier
(e.g web servers, application servers, applications, applications as services)
Data Tier
(e.g database severs)
Web Services
(AppSensor WS)
Symbol Key
Events
Detection Points
Event Manager
Reporting Client
Responses
Event Analysis Engine
Event Store
Attack Store

# Chapter 21 : Fully Integrated (AppSensor Core)



Client (e.g web browser, mobile device/app, another application)

Network (e.g. internet, VPN, internal network)

Perimeter Network Devices (e.g routers, network firewalls, load balancers)

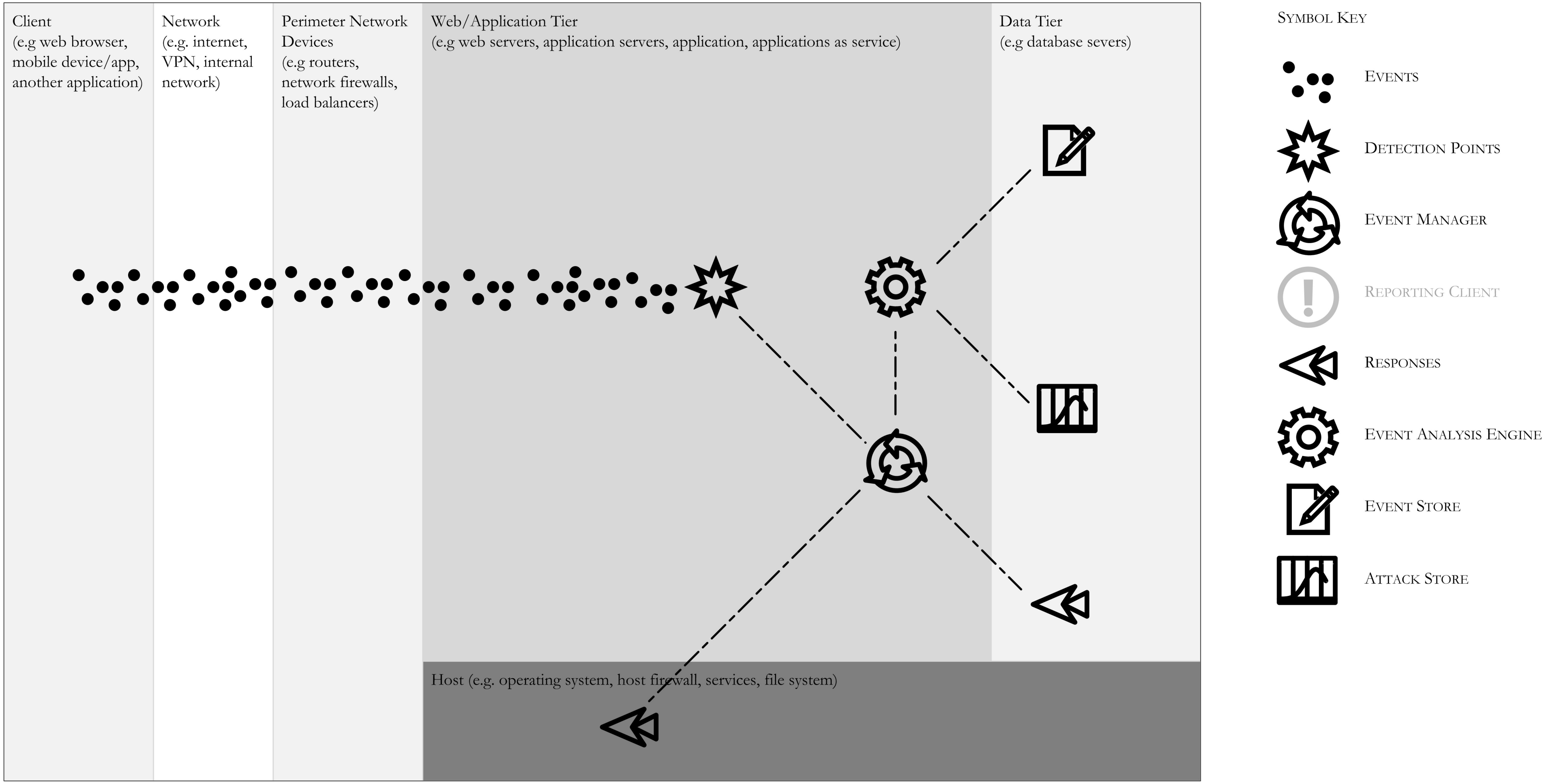
Web/Application (e.g web servers, application servers, application)

Data Tier (e.g database severs)

Symbol Key

- Events
- Detection Points
- Event Manager
- Reporting Client
- Responses
- Event Analysis Engine
- Event Store
- Attack Store

# Chapter 22 :
# Light Touch Retrofit



Client
(e.g web browser, mobile device/app, another application)

Network
(e.g. internet, VPN, internal network)

Perimeter Network Devices
(e.g routers, network firewalls, load balancers)

Web/Application Tier
(e.g web servers, application servers, application, applications as service)

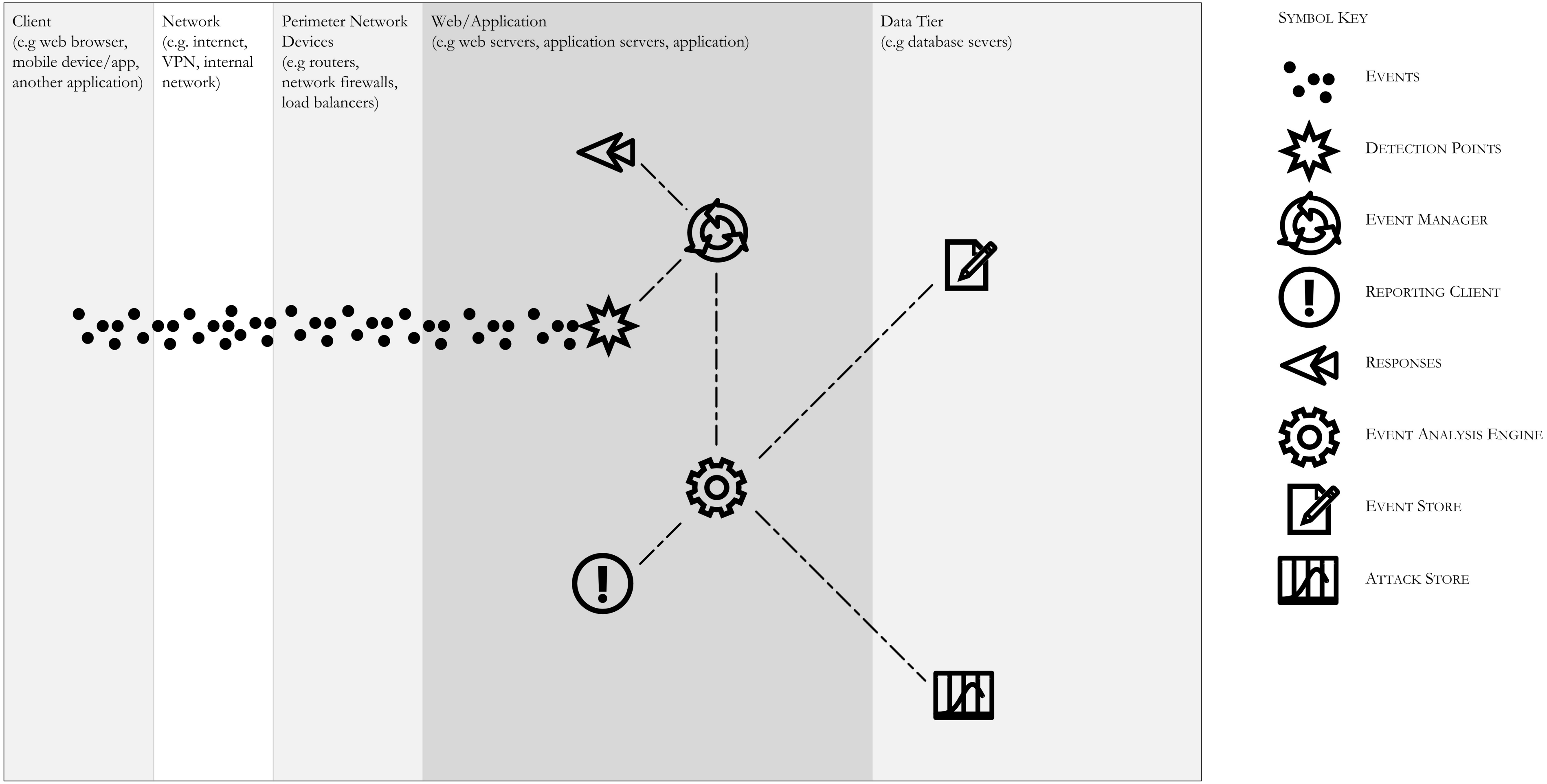
Data Tier
(e.g database severs)

Host (e.g. operating system, host firewall, services, file system)

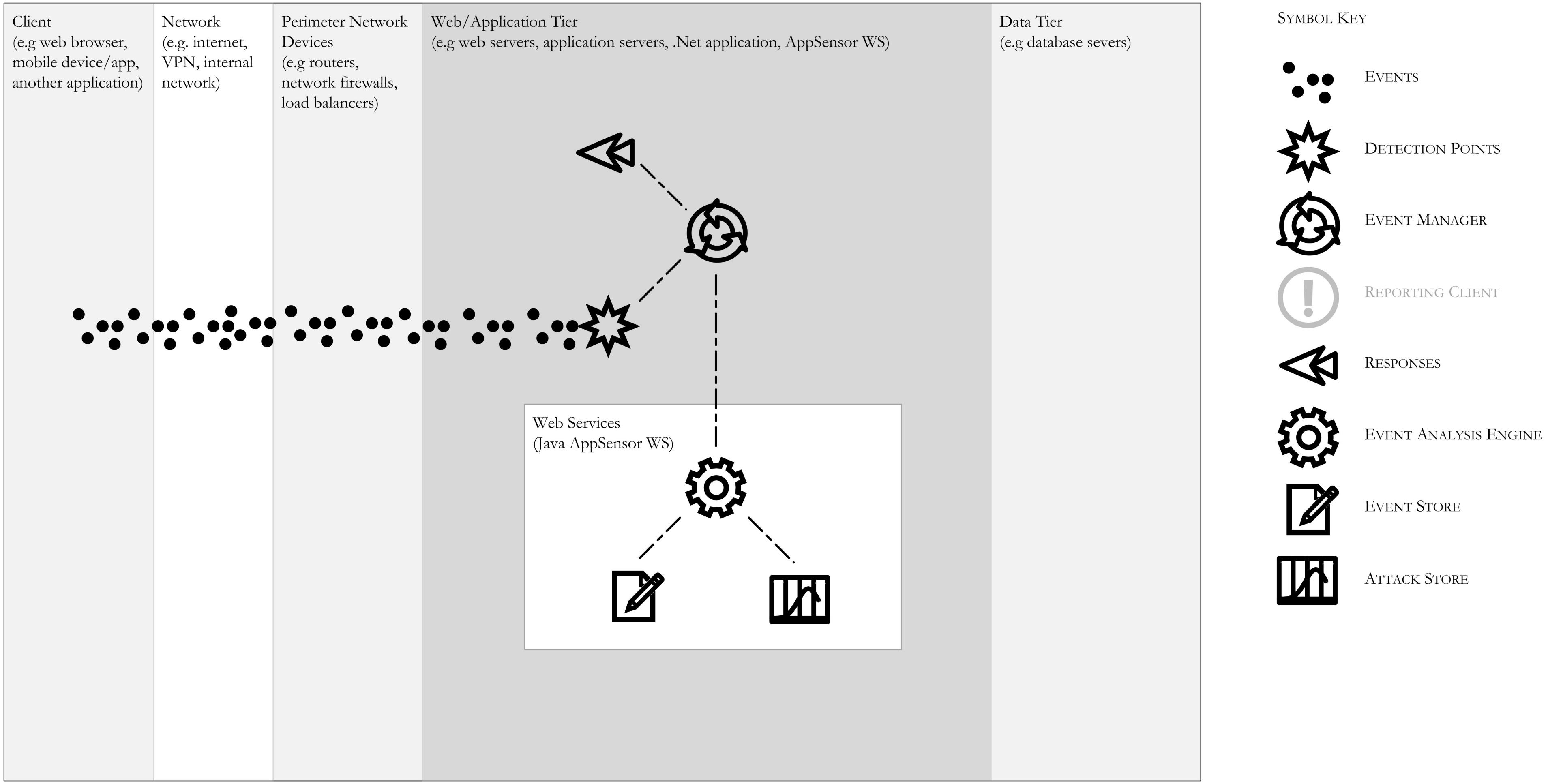
Symbol Key

- Events
- Detection Points
- Event Manager
- Reporting Client
- Responses
- Event Analysis Engine
- Event Store
- Attack Store

# Chapter 23 : Ensnare for Ruby


Client
(e.g web browser, mobile device/app, another application)
Network
(e.g. internet, VPN, internal network)
Perimeter Network Devices
(e.g routers, network firewalls, load balancers)
Web/Application
(e.g web servers, application servers, application)
Data Tier
(e.g database severs)
Symbol Key
Events
Detection Points
Event Manager
Reporting Client
Responses
Event Analysis Engine
Event Store
Attack Store

# Chapter 24 : Invocation of AppSensor Code Using Jni4Net



Client (e.g web browser, mobile device/app, another application)

Network (e.g. internet, VPN, internal network)

Perimeter Network Devices (e.g routers, network firewalls, load balancers)

Web/Application Tier (e.g web servers, application servers, .Net application, AppSensor WS)

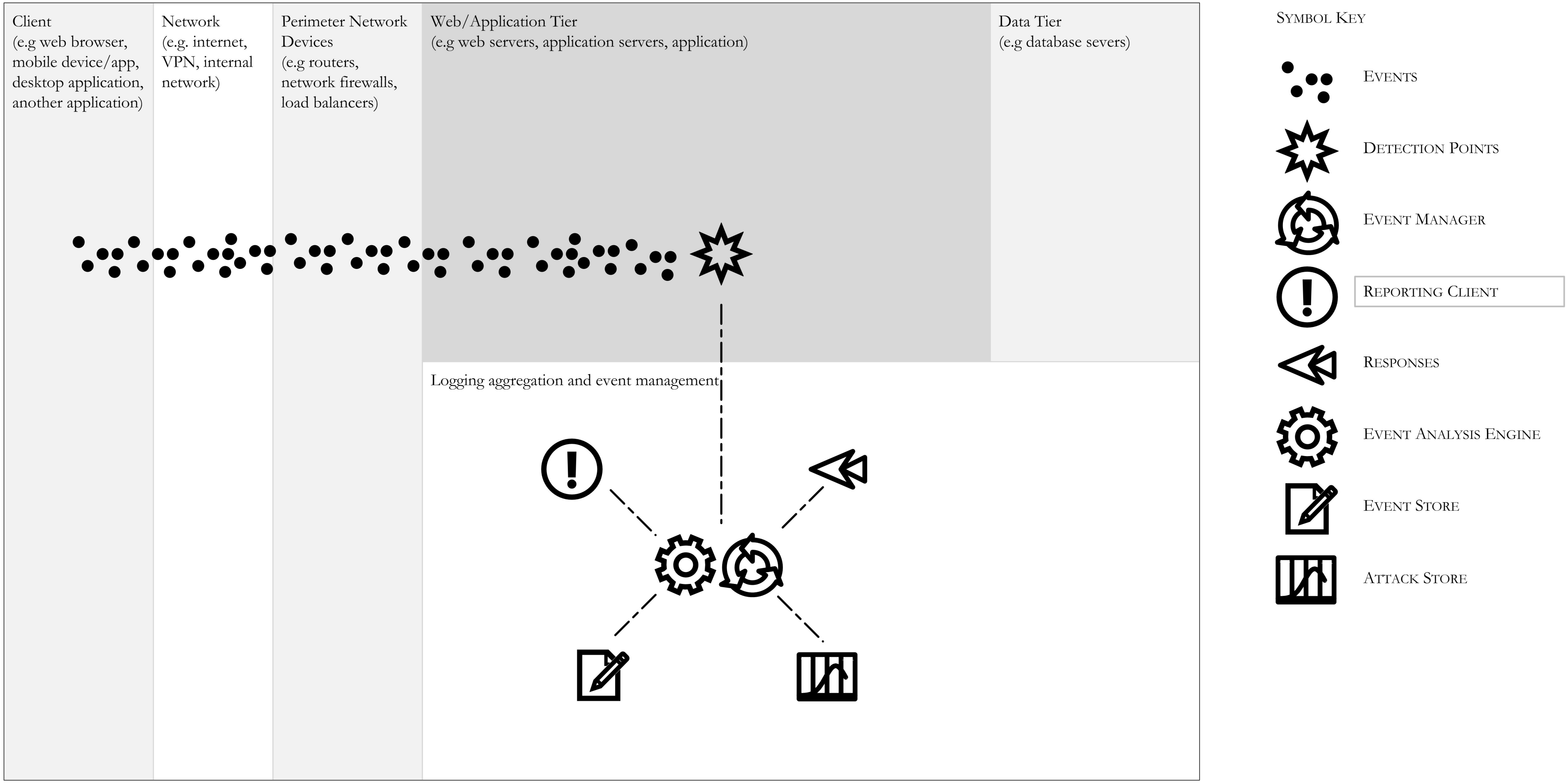
Data Tier (e.g database severs)

Web Services (Java AppSensor WS)

Symbol Key

- Events
- Detection Points
- Event Manager
- Reporting Client
- Responses
- Event Analysis Engine
- Event Store
- Attack Store

# Chapter 25 :
# Using an External Log Management System



Client
(e.g web browser, mobile device/app, desktop application, another application)

Network
(e.g. internet, VPN, internal network)

Perimeter Network Devices
(e.g routers, network firewalls, load balancers)

Web/Application Tier
(e.g web servers, application servers, application)

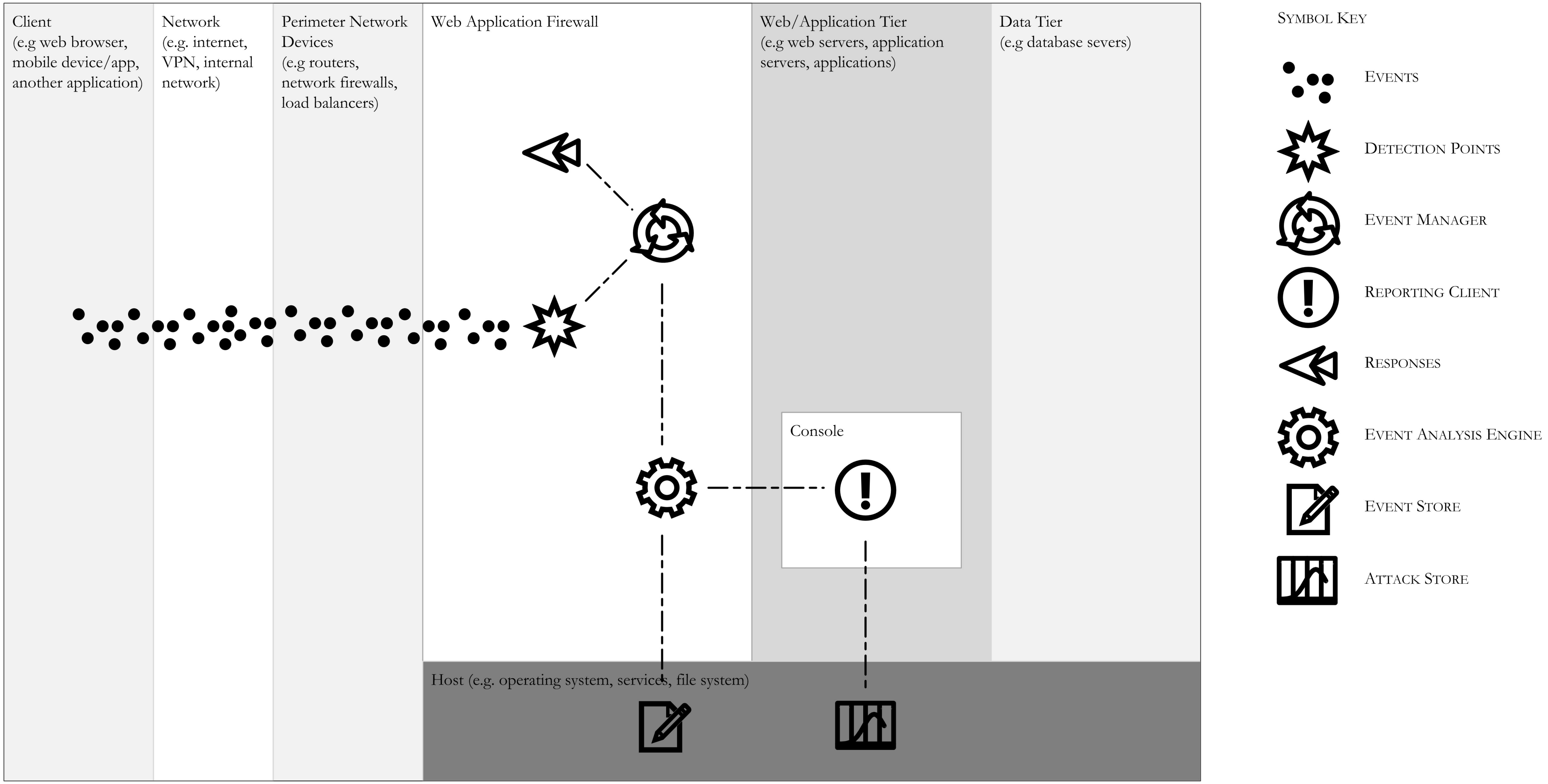
Data Tier
(e.g database severs)

Logging aggregation and event management

Symbol Key

- Events
- Detection Points
- Event Manager
- Reporting Client
- Responses
- Event Analysis Engine
- Event Store
- Attack Store

# Chapter 26 :
# Leveraging a Web Application Firewall



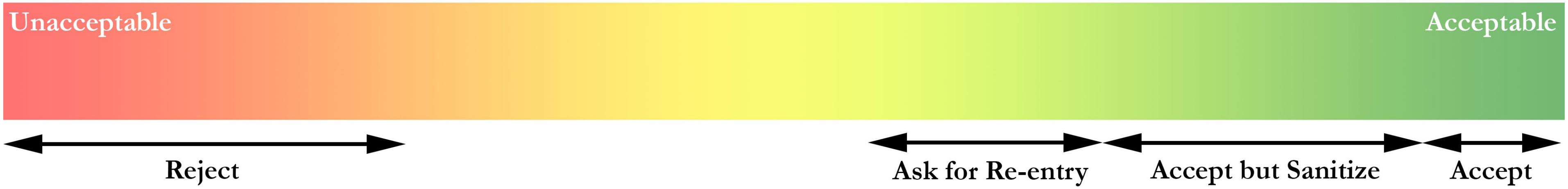
Client
(e.g web browser, mobile device/app, another application)
Network
(e.g. internet, VPN, internal network)
Perimeter Network Devices
(e.g routers, network firewalls, load balancers)
Web Application Firewall
Web/Application Tier
(e.g web servers, application servers, applications)
Data Tier
(e.g database severs)
Console
Host (e.g. operating system, services, file system)
Symbol Key
Events
Detection Points
Event Manager
Reporting Client
Responses
Event Analysis Engine
Event Store
Attack Store

# Detecting malicious use

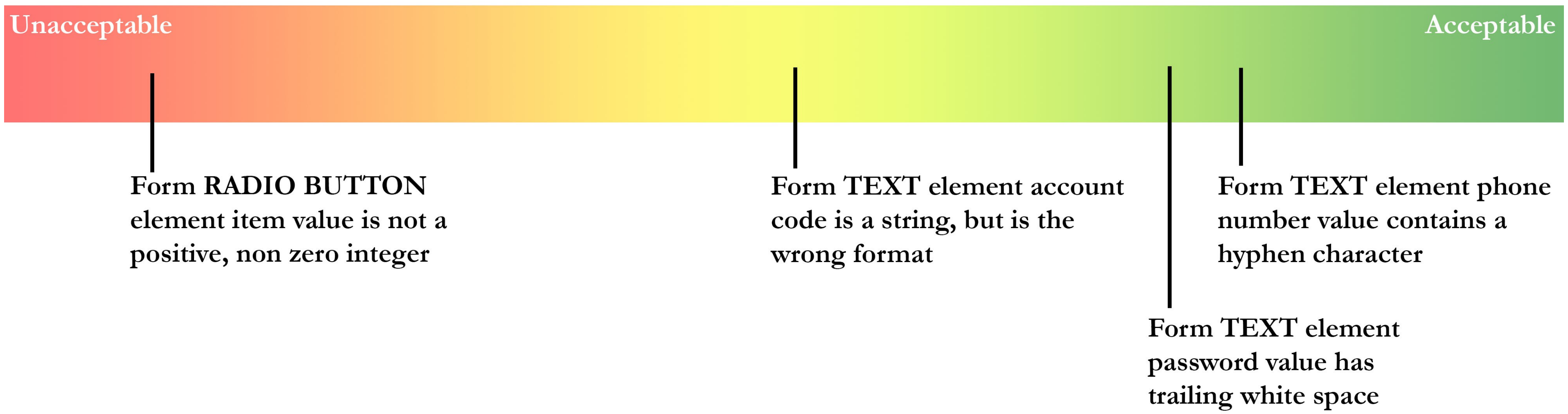
Unacceptable

Acceptable

# Human error


Unacceptable
Acceptable
Reject
Ask for Re-entry
Accept but Sanitize
Accept

# Inhuman behaviour



Unacceptable

Acceptable

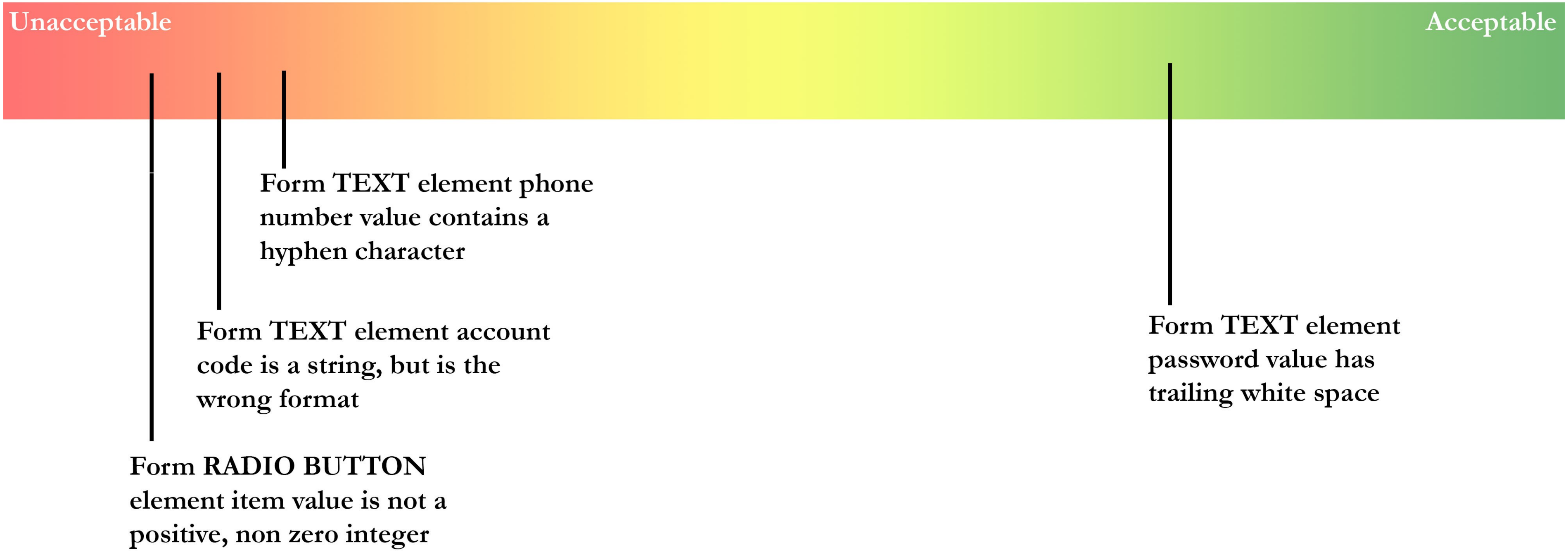
Form RADIO BUTTON element item value is not a positive, non zero integer

Form TEXT element account code is a string, but is the wrong format

Form TEXT element password value has trailing white space

Form TEXT element phone number value contains a hyphen character

# Inhuman behaviour in a different context



Unacceptable

Acceptable

Form TEXT element phone number value contains a hyphen character

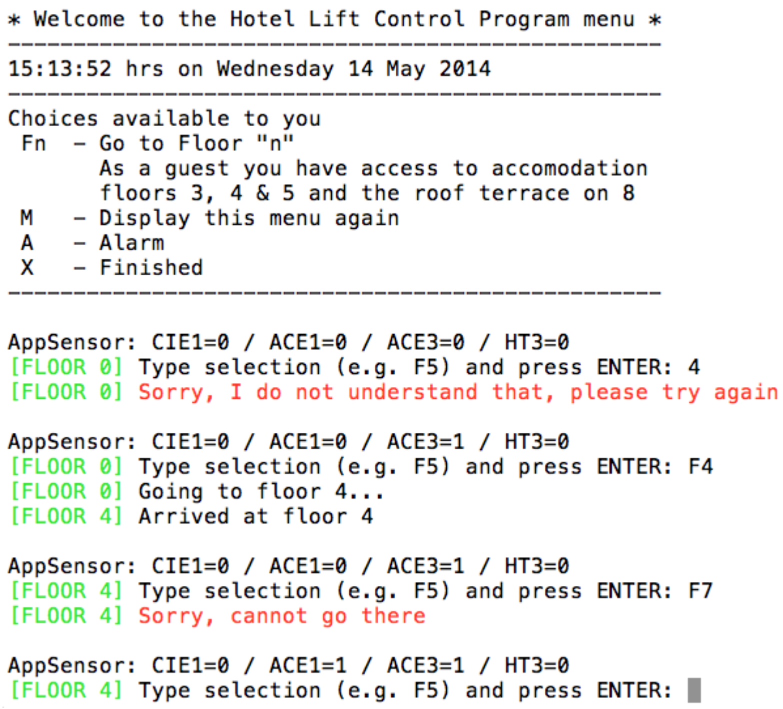
Form TEXT element account code is a string, but is the wrong format

Form RADIO BUTTON element item value is not a positive, non zero integer

Form TEXT element password value has trailing white space

# Live demo

- A hotel lift



```
* Welcome to the Hotel Lift Control Program menu *
--------------------------------------------------
15:13:52 hrs on Wednesday 14 May 2014
--------------------------------------------------
Choices available to you
 Fn   - Go to Floor "n"
        As a guest you have access to accomodation
        floors 3, 4 & 5 and the roof terrace on 8
 M    - Display this menu again
 A    - Alarm
 X    - Finished
--------------------------------------------------

AppSensor: CIE1=0 / ACE1=0 / ACE3=0 / HT3=0
[FLOOR 0] Type selection (e.g. F5) and press ENTER: 4
[FLOOR 0] Sorry, I do not understand that, please try again

AppSensor: CIE1=0 / ACE1=0 / ACE3=1 / HT3=0
[FLOOR 0] Type selection (e.g. F5) and press ENTER: F4
[FLOOR 0] Going to floor 4...
[FLOOR 4] Arrived at floor 4

AppSensor: CIE1=0 / ACE1=0 / ACE3=1 / HT3=0
[FLOOR 4] Type selection (e.g. F5) and press ENTER: F7
[FLOOR 4] Sorry, cannot go there

AppSensor: CIE1=0 / ACE1=1 / ACE3=1 / HT3=0
[FLOOR 4] Type selection (e.g. F5) and press ENTER: 
```

# The six “best” detection point types

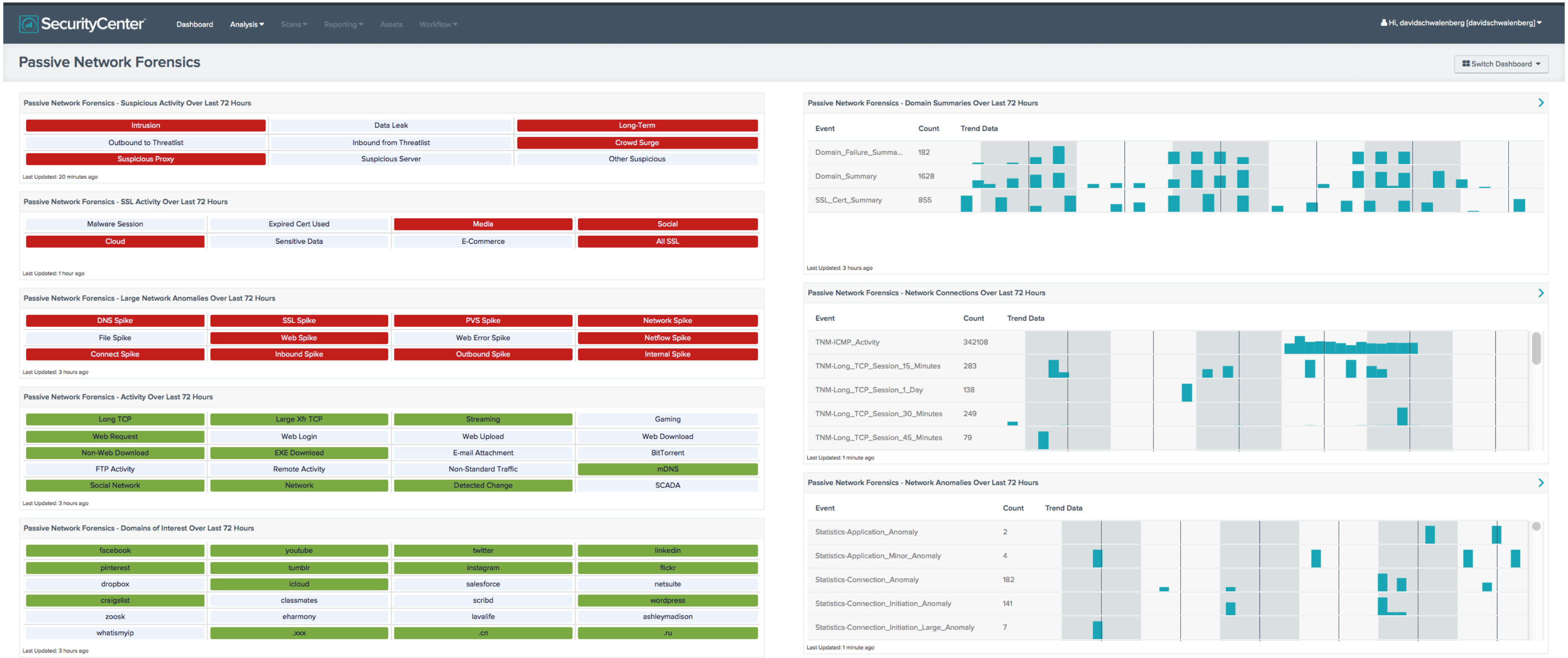
- Authorization failures
  (e.g. resource or action requested with insufficient privileges)
- Client-side input validation bypass
  (e.g. data format mismatch or missing mandatory values)
- Whitelist input validation failures
  (e.g. invalid data type or data length/range)
- Authentication failures
  (e.g. password change failures, re-authentication failure)
- Blatant code injection attack
  (e.g. common SQL injection strings)
- High rate of function use
  (e.g. requests/pages/views/windows per 5 minutes)

# Response types

| Category | | Response | |
|---|---|---|---|
| Type | Description | ID | Description |
| Silent | User unaware of application's response | ASR-A | Logging Change |
| | | ASR-B | Administrator Notification |
| | | ASR-C | Other Notification |
| | | ASR-N | Proxy |
| Passive | Changes to user experience but nothing denied | ASR-D | User Status Change |
| | | ASR-E | User Notification |
| | | ASR-F | Timing Change |
| Active | Application functionality reduced for user(s) | ASR-G | Process Terminated |
| | | ASR-H | Function Amended |
| | | ASR-I | Function Disabled |
| | | ASR-J | Account Logout |
| | | ASR-K | Account Lockout |
| | | ASR-L | Application Disabled |
| Intrusive | User's environment altered | ASR-M | Collect Data from User |

# What does your attacker dashboard look like?

Not AppSensor:



## Passive Network Forensics

Passive Network Forensics - Suspicious Activity Over Last 72 Hours

| | | |
|---|---|---|
| Intrusion | Data Leak | Long-Term |
| Outbound to Threatlist | Inbound from Threatlist | Crowd Surge |
| Suspicious Proxy | Suspicious Server | Other Suspicious |

Last Updated: 20 minutes ago

Passive Network Forensics - SSL Activity Over Last 72 Hours

| | | | |
|---|---|---|---|
| Malware Session | Expired Cert Used | Media | Social |
| Cloud | Sensitive Data | E-Commerce | All SSL |

Last Updated: 1 hour ago

Passive Network Forensics - Large Network Anomalies Over Last 72 Hours

| | | | |
|---|---|---|---|
| DNS Spike | SSL Spike | PVS Spike | Network Spike |
| File Spike | Web Spike | Web Error Spike | Netflow Spike |
| Connect Spike | Inbound Spike | Outbound Spike | Internal Spike |

Last Updated: 3 hours ago

Passive Network Forensics - Activity Over Last 72 Hours

| | | | |
|---|---|---|---|
| Long TCP | Large Xfr TCP | Streaming | Gaming |
| Web Request | Web Login | Web Upload | Web Download |
| Non-Web Download | EXE Download | E-mail Attachment | BitTorrent |
| FTP Activity | Remote Activity | Non-Standard Traffic | mDNS |
| Social Network | Network | Detected Change | SCADA |

Last Updated: 3 hours ago

Passive Network Forensics - Domains of Interest Over Last 72 Hours

| | | | |
|---|---|---|---|
| facebook | youtube | twitter | linkedin |
| pinterest | tumblr | instagram | flickr |
| dropbox | icloud | salesforce | netsuite |
| craigslist | classmates | scribd | wordpress |
| zoosk | eharmony | lavalife | ashleymadison |
| whatismyip | .xxx | .cn | .ru |

Last Updated: 3 hours ago

Passive Network Forensics - Domain Summaries Over Last 72 Hours

| Event | Count | Trend Data |
|---|---|---|
| Domain_Failure_Summa... | 182 | |
| Domain_Summary | 1628 | |
| SSL_Cert_Summary | 855 | |

Last Updated: 3 hours ago

Passive Network Forensics - Network Connections Over Last 72 Hours

| Event | Count | Trend Data |
|---|---|---|
| TNM-ICMP_Activity | 342108 | |
| TNM-Long_TCP_Session_15_Minutes | 283 | |
| TNM-Long_TCP_Session_1_Day | 138 | |
| TNM-Long_TCP_Session_30_Minutes | 249 | |
| TNM-Long_TCP_Session_45_Minutes | 79 | |

Last Updated: 1 minute ago

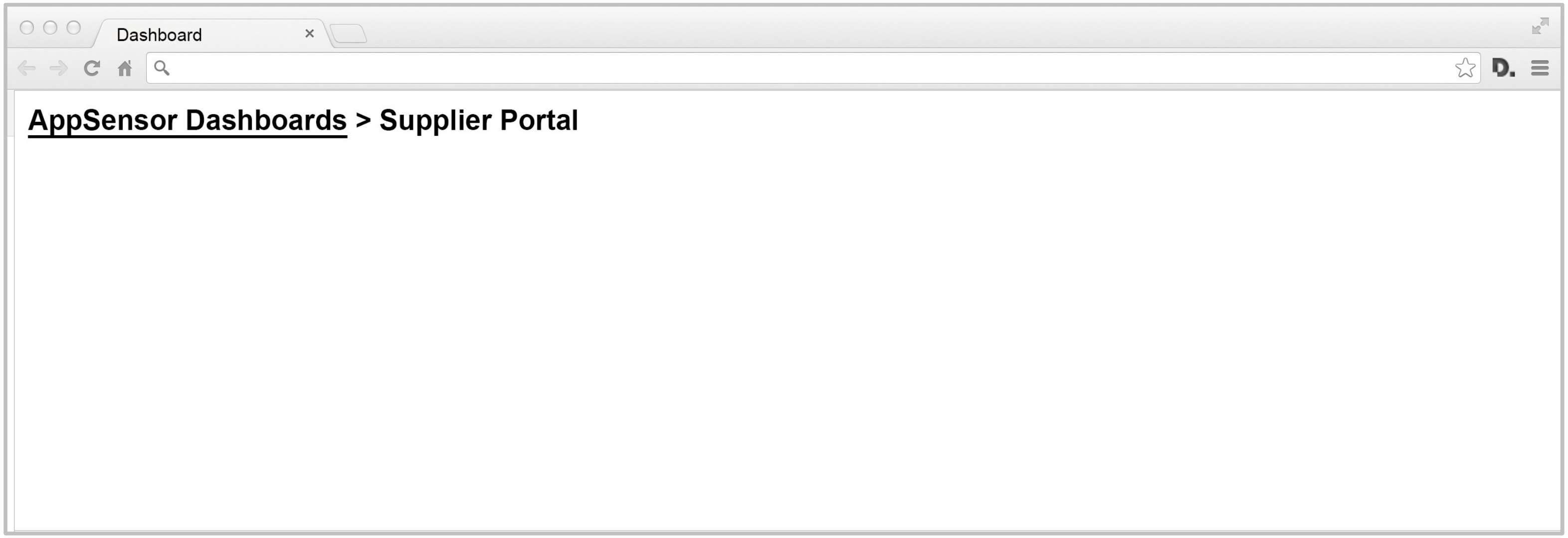
Passive Network Forensics - Network Anomalies Over Last 72 Hours

| Event | Count | Trend Data |
|---|---|---|
| Statistics-Application_Anomaly | 2 | |
| Statistics-Application_Minor_Anomaly | 4 | |
| Statistics-Connection_Anomaly | 182 | |
| Statistics-Connection_Initiation_Anomaly | 141 | |
| Statistics-Connection_Initiation_Large_Anomaly | 7 | |

Last Updated: 1 minute ago

# Detection, analysis and response all completed

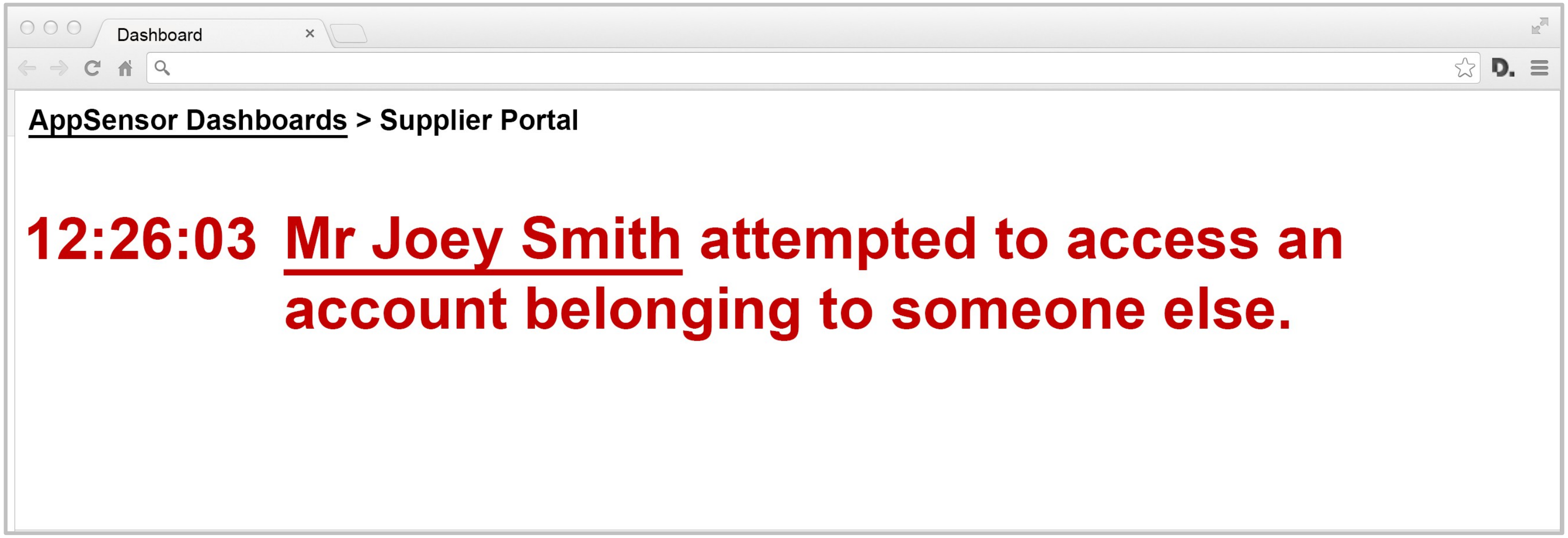
With AppSensor:



AppSensor Dashboards > Supplier Portal

# Detection, analysis and response all completed

With AppSensor:

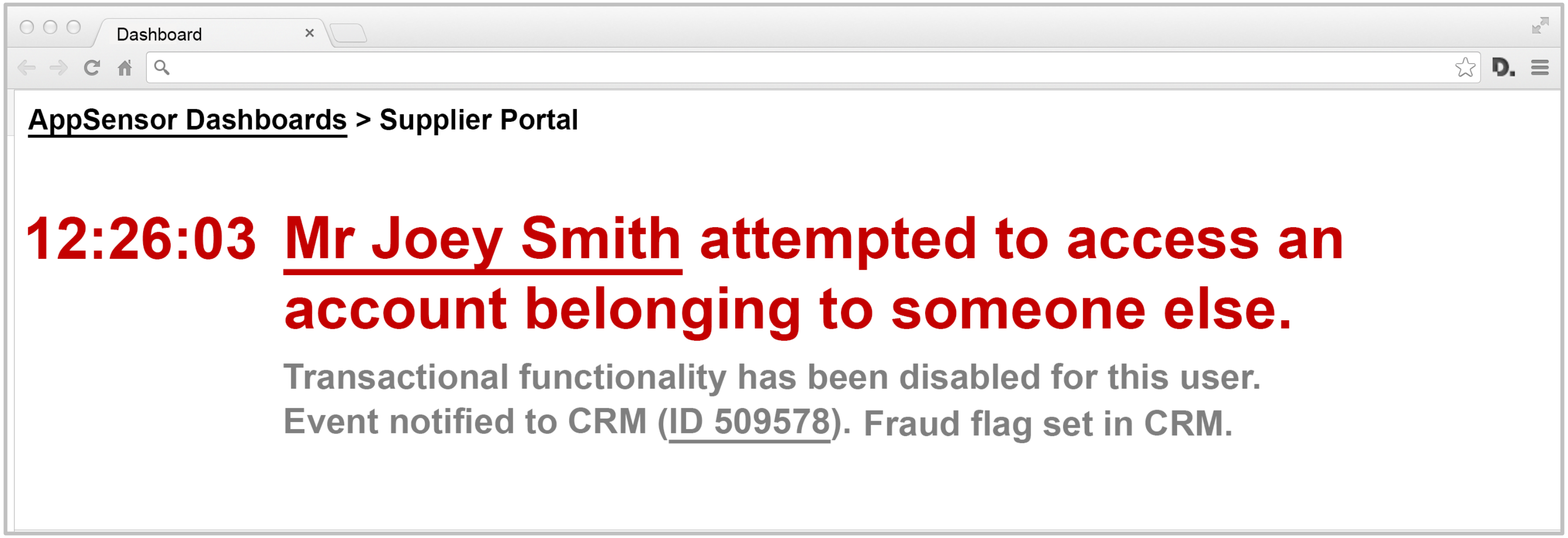


AppSensor Dashboards > Supplier Portal

12:26:03 Mr Joey Smith attempted to access an account belonging to someone else.

# Detection, analysis and response all completed

With AppSensor:



AppSensor Dashboards > Supplier Portal

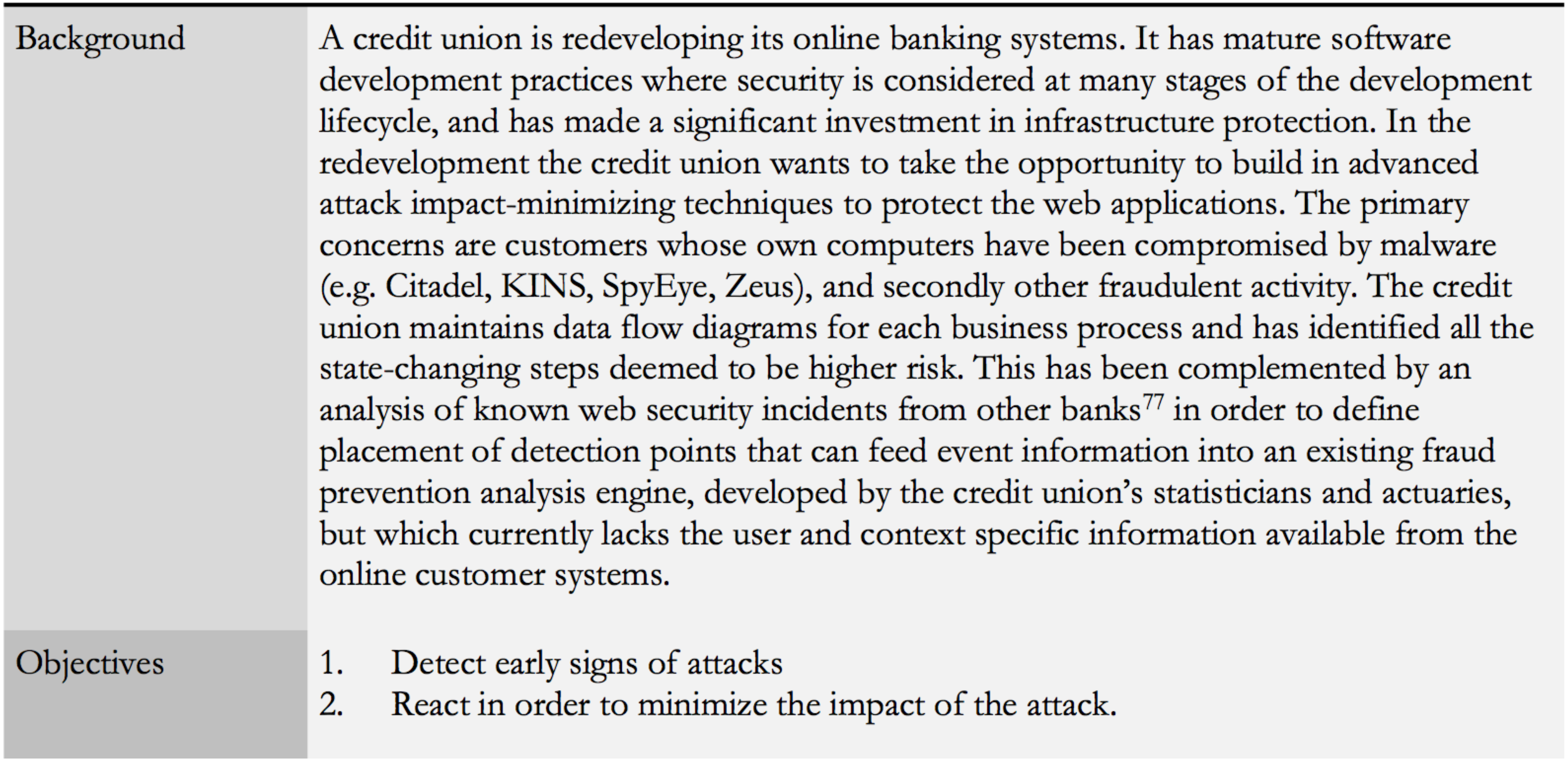
12:26:03 Mr Joey Smith attempted to access an account belonging to someone else.

Transactional functionality has been disabled for this user.
Event notified to CRM (ID 509578). Fraud flag set in CRM.

# Part II :
# Illustrative Case Studies

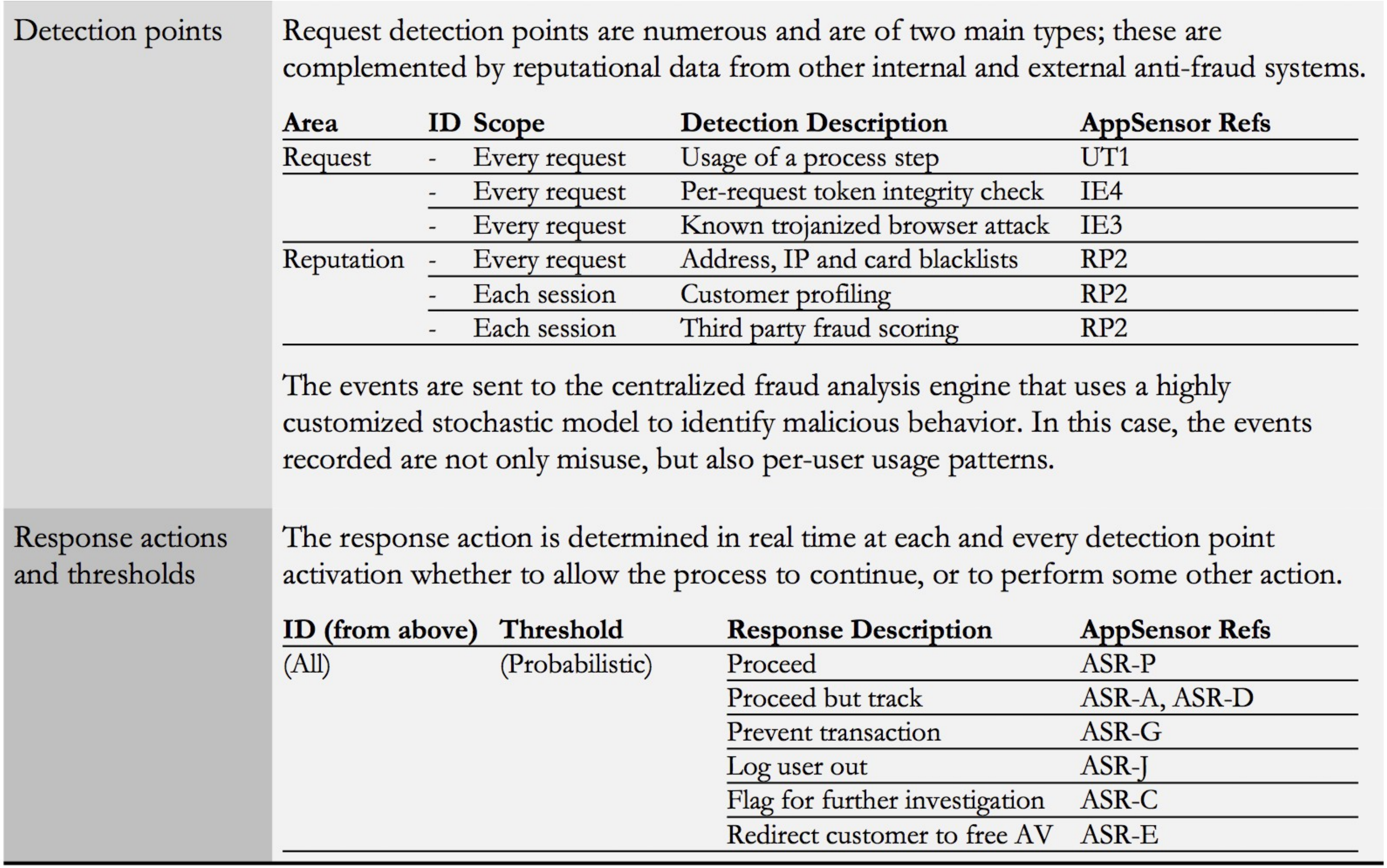
- Chapter 5 : Case Study of a Rapidly Deployed Web Application
- Chapter 6 : Case Study of a Magazine's Mobile App
- Chapter 7 : Case Study of a Smart Grid Consumer Meter
- Chapter 8 : Case Study of a Financial Market Trading System
- Chapter 9 : Case Study of a B2C Ecommerce Website
- Chapter 10 : Case Study of B2B Web Services
- Chapter 11 : Case Study of a Document Management System
- Chapter 12 : Case Study of a Credit Union's Online Banking

# Case Study : Credit Union’s Online Banking 1/2



| | |
|---|---|
| Background | A credit union is redeveloping its online banking systems. It has mature software development practices where security is considered at many stages of the development lifecycle, and has made a significant investment in infrastructure protection. In the redevelopment the credit union wants to take the opportunity to build in advanced attack impact-minimizing techniques to protect the web applications. The primary concerns are customers whose own computers have been compromised by malware (e.g. Citadel, KINS, SpyEye, Zeus), and secondly other fraudulent activity. The credit union maintains data flow diagrams for each business process and has identified all the state-changing steps deemed to be higher risk. This has been complemented by an analysis of known web security incidents from other banks[77] in order to define placement of detection points that can feed event information into an existing fraud prevention analysis engine, developed by the credit union’s statisticians and actuaries, but which currently lacks the user and context specific information available from the online customer systems. |
| Objectives | 1. Detect early signs of attacks<br>2. React in order to minimize the impact of the attack. |

# Case Study : Credit Union’s Online Banking 1/2



Detection points

Request detection points are numerous and are of two main types; these are complemented by reputational data from other internal and external anti-fraud systems.

| Area | ID | Scope | Detection Description | AppSensor Refs |
|---|---|---|---|---|
| Request | - | Every request | Usage of a process step | UT1 |
| | - | Every request | Per-request token integrity check | IE4 |
| | - | Every request | Known trojanized browser attack | IE3 |
| Reputation | - | Every request | Address, IP and card blacklists | RP2 |
| | - | Each session | Customer profiling | RP2 |
| | - | Each session | Third party fraud scoring | RP2 |

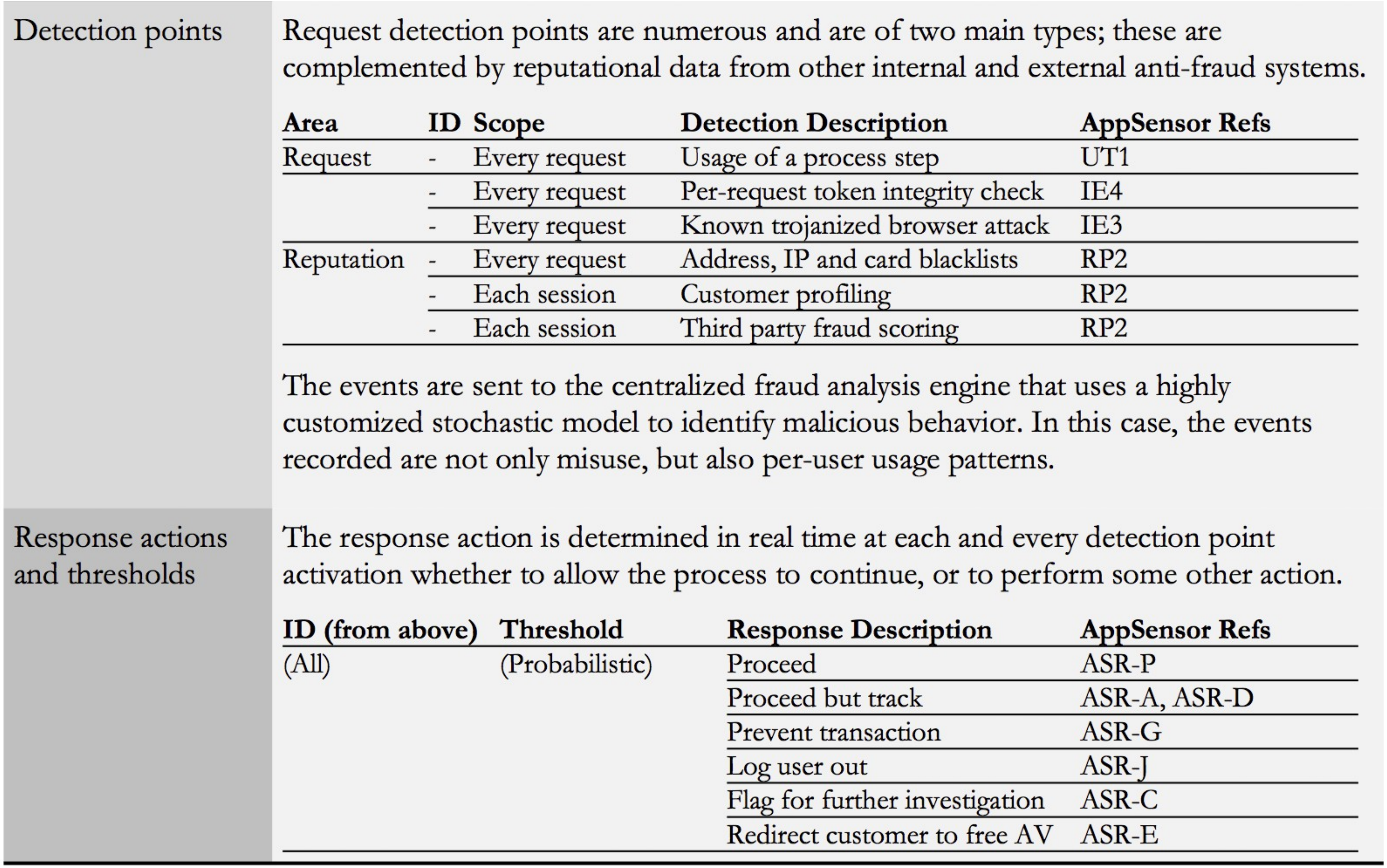
The events are sent to the centralized fraud analysis engine that uses a highly customized stochastic model to identify malicious behavior. In this case, the events recorded are not only misuse, but also per-user usage patterns.

Response actions and thresholds

The response action is determined in real time at each and every detection point activation whether to allow the process to continue, or to perform some other action.

| ID (from above) | Threshold | Response Description | AppSensor Refs |
|---|---|---|---|
| (All) | (Probabilistic) | Proceed | ASR-P |
| | | Proceed but track | ASR-A, ASR-D |
| | | Prevent transaction | ASR-G |
| | | Log user out | ASR-J |
| | | Flag for further investigation | ASR-C |
| | | Redirect customer to free AV | ASR-E |

# Case Study : Credit Union's Online Banking 1/2



Detection points

Request detection points are numerous and are of two main types; these are complemented by reputational data from other internal and external anti-fraud systems.

| **Area** | **ID** | **Scope** | **Detection Description** | **AppSensor Refs** |
|---|---|---|---|---|
| Request | - | Every request | Usage of a process step | UT1 |
| | - | Every request | Per-request token integrity check | IE4 |
| | - | Every request | Known trojanized browser attack | IE3 |
| Reputation | - | Every request | Address, IP and card blacklists | RP2 |
| | - | Each session | Customer profiling | RP2 |
| | - | Each session | Third party fraud scoring | RP2 |

The events are sent to the centralized fraud analysis engine that uses a highly customized stochastic model to identify malicious behavior. In this case, the events recorded are not only misuse, but also per-user usage patterns.

Response actions and thresholds

The response action is determined in real time at each and every detection point activation whether to allow the process to continue, or to perform some other action.

| **ID (from above)** | **Threshold** | **Response Description** | **AppSensor Refs** |
|---|---|---|---|
| (All) | (Probabilistic) | Proceed | ASR-P |
| | | Proceed but track | ASR-A, ASR-D |
| | | Prevent transaction | ASR-G |
| | | Log user out | ASR-J |
| | | Flag for further investigation | ASR-C |
| | | Redirect customer to free AV | ASR-E |

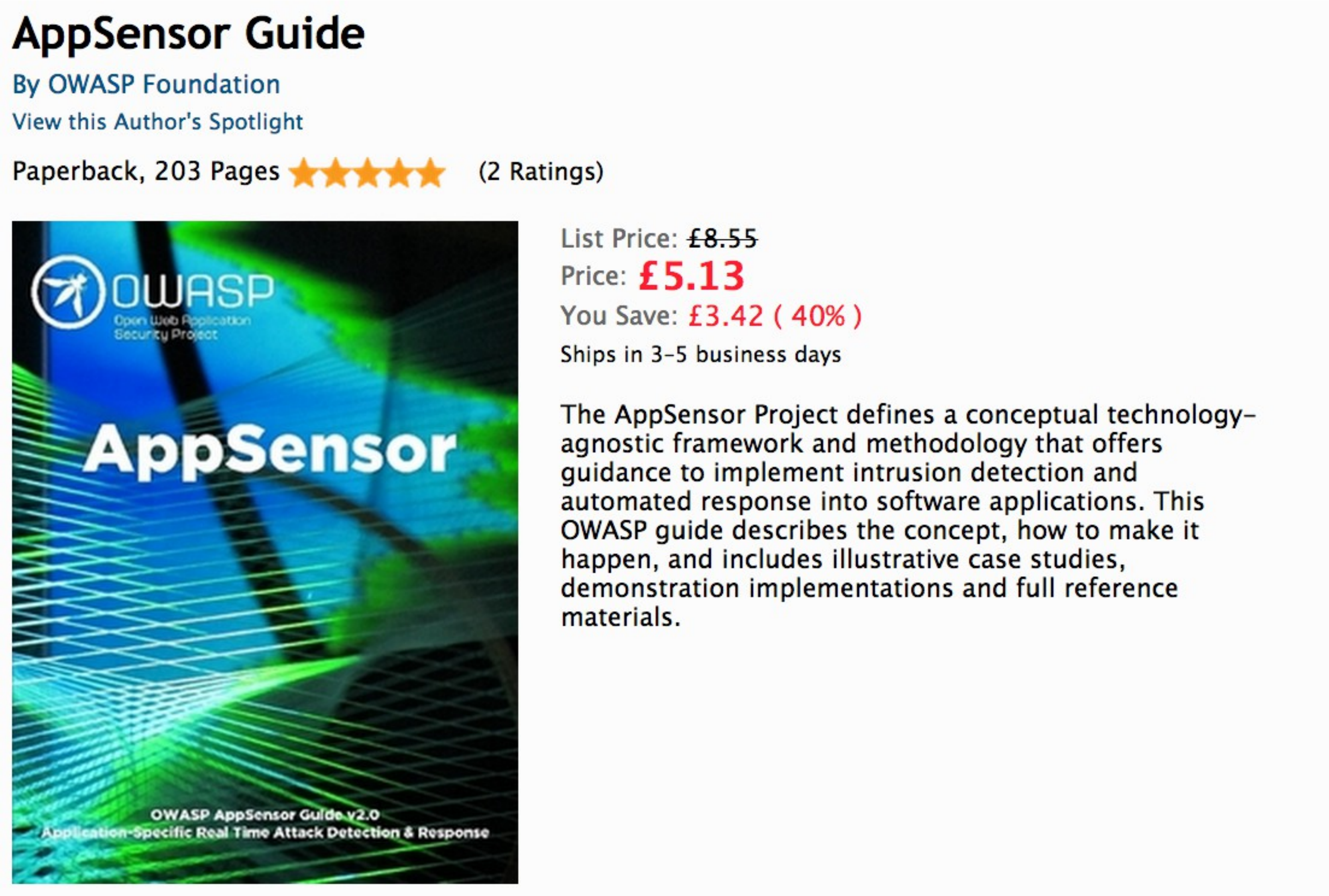
# Where to obtain the new guide

# In your machine

- AppSensor Guide v2.0, May 2014
  - PDF
    https://www.owasp.org/index.php/File:Owasp-appsensor-guide-v2.pdf
  - DOC
    https://www.owasp.org/index.php/File:Owasp-appensor-guide-v2.doc
  - Source materials
    https://4ed64fe7f7e3f627b8d0-bc104063a9fe564c2d8a75b1e218477a.ssl.cf2.rackcdn.com/appsensor-guide-2v0-owasp.zip
- Article in CrossTalk Magazine, September 2011
  http://www.crosstalkonline.org/storage/issue-archives/2011/201109/201109-Watson.pdf

# In print

- http://www.lulu.com/shop/owasp-foundation/appsensor-guide/paperback/product-21617378.html



AppSensor Guide

By OWASP Foundation

View this Author's Spotlight

Paperback, 203 Pages ★★★★★ (2 Ratings)

List Price: ~~£8.55~~

Price: £5.13

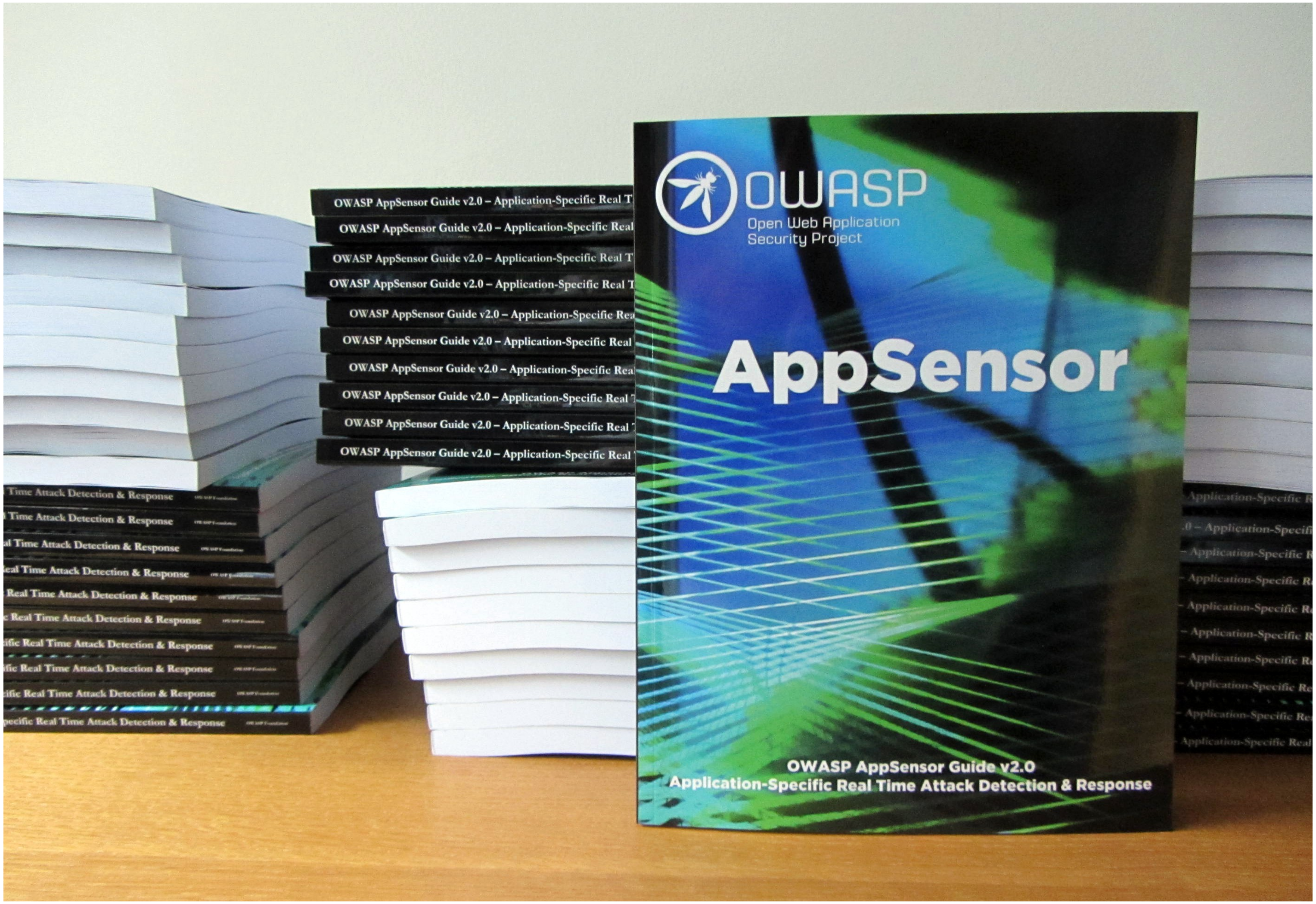
You Save: £3.42 ( 40% )

Ships in 3-5 business days

The AppSensor Project defines a conceptual technology-agnostic framework and methodology that offers guidance to implement intrusion detection and automated response into software applications. This OWASP guide describes the concept, how to make it happen, and includes illustrative case studies, demonstration implementations and full reference materials.

OWASP
Open Web Application Security Project
AppSensor
OWASP AppSensor Guide v2.0
Application-Specific Real Time Attack Detection & Response

# In your hand


OWASP
Open Web Application Security Project
AppSensor
OWASP AppSensor Guide v2.0
Application-Specific Real Time Attack Detection & Response

# “In your hand” thank you

- OWASP Project Reboot Initiative 2012 (Eoin Keary)
  https://www.owasp.org/index.php/Projects_Reboot_2012
- AppSensor reboot application
  https://www.owasp.org/index.php/Projects_Reboot_2012_-_OWASP_AppSensor
  - $5,000
    - Pay for any design costs in creating a front cover for the book (10%)
    - Fund the printing (and delivery) of 250 copies of the book, which can be used by project participants as prizes or give-aways during AppSensor presentations at OWASP chapter meetings, OWASP conferences and related events (60%)
    - Pay for the layout and printing of flyers to promote the project and book in conference bags (30%)

# Thank you to the guide's creators

**Version 2.0**

Lead Author

Colin Watson

Co-Authors

Dennis Groves John Melton

Other Contributors, Editors and Reviewers

Josh Amishav-Zlatin Ryan Barnett Michael Coates Craig Munson Jay Reynolds

**Version 1**

Author

Michael Coates

# Thank you to the project's contributors

Josh Amishav-Zlatin

Ryan Barnett

Simon Bennetts

Joe Bernik

Rex Booth

Luke Briner

Rauf Butt

Fabio Cerullo

Marc Chisinevski

Robert Chojnacki

Michael Coates

Dinis Cruz

August Detlefsen

Ryan Dewhurst

Erlend Oftedal

Sean Fay

Dennis Groves

Randy Janida

Chetan Karande

Eoin Keary

Alex Lauerman

Junior Lazuardi

Jason Li

Manuel López Arredondo

Bob Maier

Jim Manico

Sherif Mansour Farag

John Melton

Craig Munson

Giri Nambari

Jay Reynolds

Chris Schmidt

Sahil Shah

Eric Sheridan

John Steven

Alex Thissen

Don Thomas

Christopher Tidball

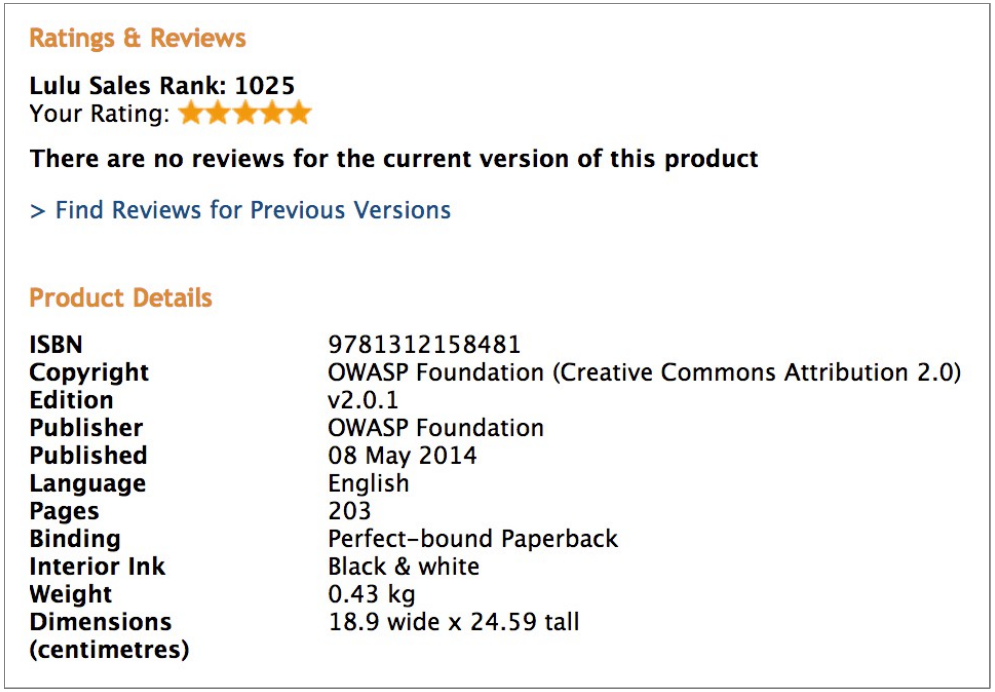
Kevin W Wall

Colin Watson

Mehmet Yilmaz

# Thank you, the audience

- Use the concept
- Tweet and blog about the AppSensor Project and the new guide
- Create a Lulu.com account
  - Rate the guide
  - Review it



**Ratings & Reviews**

**Lulu Sales Rank: 1025**
Your Rating: ★★★★★

**There are no reviews for the current version of this product**

> Find Reviews for Previous Versions

**Product Details**

| | |
|---|---|
| **ISBN** | 9781312158481 |
| **Copyright** | OWASP Foundation (Creative Commons Attribution 2.0) |
| **Edition** | v2.0.1 |
| **Publisher** | OWASP Foundation |
| **Published** | 08 May 2014 |
| **Language** | English |
| **Pages** | 203 |
| **Binding** | Perfect-bound Paperback |
| **Interior Ink** | Black & white |
| **Weight** | 0.43 kg |
| **Dimensions (centimetres)** | 18.9 wide x 24.59 tall |

@AppSensor

https://www.owasp.org/index.php/AppSensor

# Q & A

# Take aways

- Don't ever offer to write a book
- Every AppSensor instance is different
- AppSensor can be as simple or complex as you choose

# Your speaker

Colin Watson

WATSON HALL

Watson Hall Ltd

https://www.watsonhall.com

colin@watsonhall.com

020 7183 3710