



# Herman Stevens

Born: June 7<sup>th</sup>, 1961

**Astyran BVBA**  
**Noordheuvel 70**  
**B - 2990 Wuustwezel**  
**Belgium**

Email: herman.stevens@astyran.sg

Mobile: +32 (478) 681314  
+65-9725 2561

**Astyran Pte. Ltd.**  
**16 Raffles Quay**  
**#33-03 Hong Leong Building**  
**Singapore 048581**

## Professional Profile

Mr. Stevens has over ten years of experience as an IT professional covering diverse platforms and security issues. He has performed in multiple roles using a wide range of skills and experiences.

Mr. Stevens currently focuses on **application security** where the alignment of business expectations of security with technical possibilities and constraints in a mostly outsourced environment is very challenging.

The bulk of his security experience is comprised of **Information Security Governance** related work (risk assessments, ISO 17799/27001 policies, best practices using ITIL, COBIT ...), **technical vulnerability assessments** such as penetration tests and code reviews on the application level, delivering **security** related **training** and Payment Card Industry (PCI) **audits**.

Mr. Stevens likes to experience other cultures and insights and is eager to assess and explore different information security related issues and pragmatic solutions across the world. He successfully delivered and lead projects in Belgium and abroad (in most parts of Europe, the Middle East, South East Asia and the United States).

## Qualifications

- Certified Information Systems Security Professional (**CISSP**), certificate #67.059, International Information Systems Security Certification Consortium (ISC2) since November 2004
- Certified Information Systems Auditor (**CISA**), certificate #0438385, Information Systems Audit and Control Association (ISACA) since November 2003
- Payment Card Industry Qualified Security Assessor Professional (**PCI QSAP** or **QSA**, <https://www.pcisecuritystandards.org>) from April 2005 till June 2007
- Payment Application Security Professional (**PCI PASP**) from April 2006 till June 2007

## Education

- Bachelor in Management and Computer Science from ACE Groep T, Leuven, Belgium (June 2000). This course included the programming languages C, C++ and COBOL and practices and theory on computer systems, operating systems, databases as well as project management and the SDLC.
- 2001 – Course Unix Fundamentals by SUN
- 2000 – MultiSecure Extended Technical Training by Ubizen
- 1999 – Course Fast Track to PowerBuilder by Powersoft
- 1999 – Course Adabas C Fundamentals by Software AG

## Professional Memberships

- Member of the Association for Computing Machinery (ACM, <http://www.acm.org>) since 2009
- Member of the IEEE Computer Society (IEEE, <http://www.computer.org>) since 2009
- Member of the Open Web Application Security Project (OWASP,

<http://www.owasp.org>) since 2009

- Member of the Brussels-European Chapter of the International System Security Association (ISSA, [www.issa-be.org](http://www.issa-be.org)) since 2008
- Member of the International Information Systems Security Certification Consortium (ISC2, <http://www.isc2.org>) since 2004
- Member of the Information Systems Audit and Control Association (ISACA, <http://www.isaca.org>) since 2003

## Professional Experience

**2010–present day** Executive director of Astyran Pte. Ltd., Singapore

**2008–present day** Manager and owner of Astyran BVBA, Belgium

Mr. Stevens is currently manager and owner of Astyran and works for national and international companies and governments to deliver pragmatic security consultancy, application security assessments, secure code reviews, audits and information security awareness training.

**2007–2007** NET2S (now part of BT Global Services), Brussels, Belgium  
**Senior Security Consultant**

Mr. Stevens was responsible for business development, pre-sales related activities and the delivery of information security consultancy and security awareness training for developers.

**2000–2007** Ubizen (now part of Cybertrust/Verizon Business), Leuven, Belgium  
**Principal Security Consultant**

Mr. Stevens started as product trainer and then moved on to become security consultant as part of the Risk Assessment and Management group within the Ubizen Professional Services department. Main focus was application security.

**1998–2000** Smals-MvM, Brussels, Belgium  
**Developer**

Analysis, development and maintenance of applications (mainly written in C, Cobol, Java, Natural, PowerBuilder and some assembler) for Belgian Social Security Agencies. Mr. Stevens also reviewed and corrected large code bases for Y2K problems on a Fujitsu Siemens BS 2000 mainframe. Back-end databases where Oracle and Software AG Adabas.

**1984–1998** SBB Sociaal Verzekeringsfonds (now Acerta), Leuven, Belgium  
**Administration**

General administration regarding the Belgian Social Security system. Automation using Visual Basic.

## Speaking Opportunities

- On March 6<sup>th</sup> 2008, Mr. Stevens presented his insights in source code reviews at the eBanking Fraud and Cyber Security Seminar of the Monetary Authority of Singapore.
- In November 2007 Mr. Stevens, together with Mr. Frantzen, delivered a much appreciated and discussed presentation on *Application security awareness training for developers* at the joint meeting of the Belgian ISSA and OWASP chapters.

## Conferences Attended

- Singapore Security Meetup (Singapore, 11 May 2011): Presentation 'Latest Browser Security Features' by Tobias Gondrom
- OWASP Benelux Day 2009 (Leuven – Belgium, 2 December 2009), see <http://www.owasp.org>
- HITB 2009 Conference (Kuala Lumpur – Malaysia, 7 and 8 October 2009), see <http://www.hackinthebox.org>.
- Brucon 2009 Conference (Brussels – Belgium, 18 and 19 September 2009), see <http://www.brucon.org>.
- LSEC Application Security Seminar (Leuven – Belgium, 9 September 2008), see <http://www.lsec.be>

## Experience and Accomplishments

### *Important 2011 Projects*

- Mr. Stevens performed a web application assessment for one of the applications of **Trusted Area**. Trusted Area is a secure social communication and networking platform for companies or organizations.
- For the **Monetary Authority of Singapore**, Mr. Stevens performed a **source code security review** of the changes since 2009 in the Notes Operation Registration Management Plus (NORMS+) application at Currency House. NORMS+ is an automated material flow and warehousing system which comprises a chain of inter-connected robot sub-systems that manages the storage, inventory and retrieval of currency notes, as well as the issuance and receiving of cash with banks
- For **BCA Indonesia** (former Bank Central Asia) Mr. Stevens performs - as part of an ongoing project – several web application vulnerability assessments of internet facing applications and critical web based intranet applications.
- For the **Hong Kong Hospital Authority** Mr. Stevens developed and delivered a web application security training for developers, created security guidelines for developers and wrote a report regarding SDLC Security Framework, Standards and Best Practices.

### *Important 2010 Projects*

- For **BCA Indonesia** (former Bank Central Asia) Mr. Stevens performs - as part of an ongoing project – several web application vulnerability assessments of internet facing applications and critical web based intranet applications.
- Mr. Stevens created and delivered a security awareness course and workshop for developers based on the OWASP Top Ten at the **Brussels Airport Company**. The Brussels Airport Company is the company to which the Belgian State has granted the licence to operate Brussels Airport.
- Mr. Stevens performed a web vulnerability assessment of two critical applications managing and monitoring installations at customers' sites around the world for **Agfa-Gevaert**. Agfa-Gevaert is a European multinational corporation that develops, manufactures and distributes analogue and digital products and systems for the making, processing and reproduction of images.
- For the **Monetary Authority of Singapore**, Mr. Stevens performed a **source code security review** (main technologies Java, XML) of the code changes since 2009 in the MEPS+ application. MEPS+ is a Singaporean high-value interbank payment and book-entry securities settlement system riding on the SWIFT messaging network. Goal was to assess the application for developer planted malware and generic security issues.
- For **Banco De Oro** (BDO) in the **Philippines**, Mr. Stevens created and delivered a three day security training for their development team: the first day an in depth training regarding typical web application security issues, the second day about secure coding and a third day about web application penetration testing and vulnerability assessments.
- For **Belgacom** (the largest Belgian telecom provider), Mr. Stevens was part of a team that reviewed all in-house developed or outsourced applications or bought solutions for security issues. This encompassed typical internal and external web applications, VOIP solutions, TR-69 client boxes and ACS servers, customer management applications and mobile payment applications. Reviews were mostly white box vulnerability assessments and code reviews. Mr. Stevens also performed a penetration test on their GPRS/3G network and systems.

- Mr. Stevens created and delivered a security awareness course for developers at the **European Anti-Fraud Office (OLAF)**. The mission of OLAF is to protect the financial interests of the European Union, to fight fraud, corruption and any other irregular activity, including misconduct within the European Institutions.
- Mr. Stevens created JAVA secure development guidelines and created and delivered a security awareness course for developers at the **Landsbond Van Christelijke Mutualiteiten (LCM)**, one of the organizations responsible for the payment of health insurance related allowances according to the Belgian social security laws

### *Major 2009 Projects*

- At **AXA Bank and Insurance Group** Belgium, Mr. Stevens delivered the security awareness training for all members of the development teams (project leaders, architects, analysts and developers). The training consisted of a generic, high-level training on the first day, followed by a more in-depth technical training on the second day geared towards web developers.
- For a development company (specialized in clearing, settlement and commercial banking systems) in Singapore, Mr. Stevens was involved as subject matter expert in a project regarding an advanced payment application. This encompassed a security requirements review, the creation of a formal threat model and ensuring that the architecture and design included security in line with the high risk business context.
- For the **Bank Mandiri**, the largest Indonesian bank, Mr. Stevens performed an **application vulnerability assessment** of an Internet facing application and an application vulnerability assessment of a business critical internal remittance application.
- For **Banco De Oro (BDO)** in the **Philippines**, Mr. Stevens performed a **source code review** (main technologies J2EE, Servlets, Struts framework) of their corporate and consumer banking web sites (both internal and external functionality).
- For the **Monetary Authority of Singapore**, Mr. Stevens performed a **source code security review** (main technologies Java, XML) of the code changes since 2008 in the MEPS+ application. MEPS+ is a Singaporean high-value interbank payment and book-entry securities settlement system riding on the SWIFT messaging network.
- For the **Monetary Authority of Singapore**, Mr. Stevens performed a **source code security review** (main technologies Visual Basic, Java, Pro C) of the changes since 2008 in the Notes Operation Registration Management Plus (NORMS+) application at Currency House. NORMS+ is an automated material flow and warehousing system which comprises a chain of inter-connected robot sub-systems that manages the storage, inventory and retrieval of currency notes, as well as the issuance and receiving of cash with banks.

### *Major 2008 Projects*

- Mr. Stevens performed a secure design and source code review of a mission critical application at **Eurocontrol CFMU** following changes at the front-end of the application (use of portlets, Adobe Flex and the Google Web Toolkit (GWT)), the J2EE back-end and the new self-registration process.
- For a **development company** (specialized in clearing, settlement and commercial banking systems) in **Singapore**, Mr. Stevens was involved as subject matter expert in a project regarding an advanced payment application. This encompassed a security requirements review, the creation of a formal threat model and ensuring that the architecture and design included security in line with the high risk business context.
- For **Mobistar** Belgium (a member of the Orange group and operating in the fields of mobile and fixed telephony, ADSL and other markets), Mr. Stevens performed a penetration test and vulnerability

assessment of multiple applications at their Residential and Business Portal.

- For **Emailvision** (the European market and technology leader in “on-demand” software for email marketing automation) Mr. Stevens performed a vulnerability assessment of their flagship product Campaign Commander.
- For **Cobelguard**, specialised in physical security services, Mr. Stevens performed a **web application vulnerability assessment** of their business critical online planning, reporting and incident escalation solution.
- For the **Monetary Authority of Singapore**, Mr. Stevens performed a **source code security review** of the Notes Operation Registration Management Plus (NORMS+) application at Currency House. NORMS+ is essentially an automated material flow and warehousing system which comprises a chain of inter-connected robot sub-systems that manages the storage, inventory and retrieval of currency notes, as well as the issuance and receiving of cash with banks. The objective was to review the source code for security flaws and malicious code and to review the security design architecture and functions.
- For the **Monetary Authority of Singapore**, Mr. Stevens performed a **source code security review** of the recent code changes in the MEPS+ application. The objective was to review the source code for security flaws and malicious code, review the security design architecture and functions and ascertain that the updated code did not allow unauthorized access to the system. MEPS+ is a Singaporean high-value interbank payment and book-entry securities settlement system riding on the SWIFT messaging network.

## Older Projects

### *Training*

At **AXA Belgium**, Mr. Stevens delivered the security awareness training for all members of the development teams (project leaders, architects, analysts and developers). The training consisted of a generic, high-level training on the first day, followed by a more in-depth technical training on the second day geared towards web developers.

**MasterCard UK** appealed to Mr. Stevens for the design and delivery of security training for MasterCard management and developers, giving an overview of general security issues, security architecture, secure development, application level attacks and browser related security issues.

At the **Saudi Arabian Monetary Agency** (Tadawul department, the stock-market) Mr. Stevens delivered the Security Awareness training for all management and staff.

In the framework of the Information Systems Security Improvement Project at **Saudi Telecom Corporation** and the creation of a Secure Operations Centre, Mr. Stevens trained the Saudi Telecom Security Analysts in generic security related issues, incident response and TCP/IP networking.

Mr. Stevens delivered training about Risk Assessment, Asset Classification and Business Continuity at **Smals-MVM**, and held workshops about Security planning to organizations connected to the Belgian Crossroad Bank for Social Security.

For the **Telindus High-Tech Institute** (now part of Belgacom), Mr. Stevens updated the E-Commerce Applications training and delivered this training to several partners of Telindus.

As Mr. Stevens started his career at **Ubizen** as the Product Trainer he also created and delivered technical training on several Ubizen security products, such as MultiSecure ETS (strong authentication and signatures for web applications), Payment Router (secure payment product) and Ubizen DMZ/Shield (application level firewall). This included providing content, designing exercises, writing exam questions, configuring the hardware and software used in training and conducting training sessions. Mr. Stevens delivered this training at customers' sites (e.g. MedContrax Washington, Umicore Belgium) and at dedicated training centers (Ubizen College Belgium, Ubizen Holland, Atel Italy) for several partners and customers of Ubizen.

### *Application Security*

For the **Abu Dhabi Securities Market** (ADSM) Mr. Stevens did an initial security assessment of their critical applications, both on management and technical level with the goal to identify security vulnerabilities, weaknesses or non-compliances with best practices. Mr. Stevens used interviews, documentation and configuration reviews. The applications were highly advanced (SMS gateways, surveillance servers, web portal)

or very specific to the stock market (Horizon Trade Engine and Equator clearance, settlement, depository and registry system, Host-on-Demand servers, COMM servers, FIX/MDF links, trader workstations).

**eSheel** is a Specific Targeted Research Project (STREP) of the **European Union** on electronic logbooks for fisheries. The fisheries logbook is one of the most vital parts of the fisheries management all over the world and encompasses all reports that the skipper has to fill in. Mr. Stevens wrote the security specification of the application, based on the Common Criteria (ISO/IEC 15408).

At **Euroclear** Mr. Stevens performed a blackbox penetration test of the Fundsettle and UAM web applications. Objective was to assess the security of the applications, including screening for typical application-level security issues such as cross-site scripting (XSS), SQL injection flaws, etc. and to recommend improvements.

For **Eurocontrol CFMU Belgium** Mr. Stevens was responsible for the review of the JSP-based web-interface, the J2EE based access component and the ADA back-end application of a critical CFMU web-facing application as well as the delivery of the final report and executive summary.

For **Fortis Belgium** ISRM (bank and insurance group), MR. Stevens wrote the global awareness document *Security Requirements for Web Development*. This highly readable and pragmatic document explained the most important security issues in web applications, together with implementation guidelines and practical examples, geared towards the Fortis environment.

As a lead consultant Mr. Stevens was responsible for a **General Motors Europe** project with the goal to assess the security status of five critical web applications (supply chain, sales and marketing related). The applications were scored against the implementation of web application development best practices with the ultimate goal of benchmarking and scoring the outsourced development.

At **Levi Strauss Belgium** Mr. Stevens performed a white box penetration test and code review of critical Supply Chain related applications with web front-end. Mr. Stevens reviewed the ASP.NET applications for typical application level security issues, such as improper input validation, broken access control, cross-site scripting, SQL injection flaws, improper error handling, cookie strength and weak session management. Mr. Stevens delivered the final report and gave a presentation to management.

At **ManPower Belgium** Mr. Stevens was responsible for a web application vulnerability assessment and source code review of a key 24x7 web application front-end and back-end consisting of more than 2000 Visual Basic classes with connection to a SQL server database and file-server. Mr. Stevens was responsible for the complete assignment and the final report to management.

As part of a pre-implementation due-diligence process the **Monetary Authority of Singapore (MAS)** commissioned an in-depth code-review security assessment of the new MEPS+ system, with the goal of finding vulnerabilities and developer-planted malware. MEPS+ is a national high-value and critical inter-bank payment and book-entry securities settlement system riding on the SWIFT messaging network with the following components: a Real Time Gross Settlement system, a Singapore Government Securities book-entry settlement and custody system, a Current Account system and a separate security authentication module. Mr. Stevens' role in the project was that of principal consultant. Mr. Stevens also performed large parts of the code review.

For the **SG Hambros Bank Channel Isles in Jersey** Mr. Stevens performed a black box penetration test on their critical e-Banking web-application used by their private banking clients.

### ***Information Security Governance***

For **Fluxys**, the Belgian independent natural gas transport company, Mr. Stevens temporarily worked as the interim IT Security Manager, responsible for implementing and following up their ISO 17799 based policy framework, putting security into their COBIT and ITIL based processes and advising on security issues for IT projects.

Mr. Stevens created security policies and procedures (in line with international standards such as ISO 17799, WebTrust CA and X9.79) for the Ubizen **Belgian Electronic Identity Card** contract with the Belgian government.

For the **European Investment Bank (EIB)**, based in **Luxembourg** Mr. Stevens rewrote the security policy framework based on ISO 17799 into a framework based on the Standard of good Practice of the Information Security forum (ISF).

Mr. Stevens wrote the security policy framework for the Specific Targeted Research Project (STREP) **eMajor** of the **European Union**. The objective of the project was to develop and implement an open, secure and affordable e-Government platform to support secure communication (PKI based) between municipalities, businesses and citizens.

At the **FOD Economie** (Federal Government, **Belgium**), Mr. Stevens performed a risk assessment and created a security policy framework based on ISO 17799. The FOD Economie is a paying agency associated with the European Agricultural Guidance and Guarantee Fund (EAGGF). Those agencies are required to select COBIT, ISO/IEC 17799 or the Baseline Protection Manual (BSI) as the basis for their information systems security.

For **Merak Belgium** Mr. Stevens performed a risk assessment and created a security policy framework (information security management system – ISMS) based on ISO 17799 with the ultimate goal to become ISO 27001 certified in 2007.

For the Security Operations Centre (SOC) of **NCS Singapore** Mr. Stevens wrote the policies, processes and high-level procedures based on ISO 17799, COBIT and ITIL (Change Management, Configuration Management, Incident Management, Problem Management, Release Management, Patch and Vulnerability Management).

At the **Saudi Arabian Monetary Agency** (Tadawul department, the stock-market) Ubizen did a Business and Security Assessment resulting in the Corporate Security Policy and several more low-level security policies. Mr. Stevens successfully created the security policies and performed quality assurance and customization to the specific business of Tadawul.

In the framework of the Information Systems Security Improvement Project at **Saudi Telecom Corporation**, Ubizen delivered System Security Manuals (SSM) for several highly critical systems at STC. An SSM consists of parts related to the organization (Policies and Procedures), as well as more technical parts relating to the server and DBMS configuration. Mr. Stevens wrote the organizational part of several SSMs and was also responsible for the quality assurance of others.

Mr. Stevens provided consultancy regarding Patch Application Management at **SWIFT Belgium**, was responsible for the configuration of the Symantec DeepSight Alerting application and wrote documents describing the Patch Application Management process and procedures.

Mr. Stevens designed and wrote a security policy framework for **UnifiedPost Belgium**, based on best practices and ISO 17799 (also known as BS 7799, the British Standard): Asset Classification Policy, Corporate Security Policy, Data Handling Policy, Incident Response Policy, Malicious Code Policy, Monitoring Policy, Outsourcing Policy, Password Policy and Patch Management Policy as well as a template for high quality procedures.

### ***Audit***

As a qualified VISA security assessor Mr. Stevens performed several PCI (Payment Card Industry) audits at large payment service providers, such as **Banksys Belgium** (now part of Atos Worldline), **SSB Italy**, **Sinsys Italy** and **Bankart Slovenia**. The PCI program ensures that VISA/MasterCard members, merchants, and service providers maintain the highest information security standard. The PCI standard covers technical areas as well as security management issues and an auditor needs to cover a broad domain of controls, from physically controlling access rights on HP Tandem machines, discussing application development with AS400 RPG programmers to reviewing high level security policies.

Mr. Stevens evaluated the ISO 17799 policy framework of **Rettig ICC Europe** and performed a security audit of the Paris based IT department of one of their subsidiaries.

### ***Other***

Mr. Stevens was responsible for a Ubizen **internal assignment**, consisting of creating high-level management reports for key customers regarding Service Management of Ubizen OnlineGuardian (SOC) managed security services.

Mr. Stevens was responsible for the quality assurance of the Ubizen Web/Notary and Registrar products (PKI and digital signatures) and as such created the test plans, and was involved in executing those plans.