

## Marco, Casassa Mont - Bristol, UK

MSc Computer Science, CISSP, IISP Associate, Senior IEEE Member

[marcocasassamont@gmail.com](mailto:marcocasassamont@gmail.com), <https://www.linkedin.com/in/marcocasassamont>, <http://www.marcocasassamont.com/>

### OVERVIEW

An enthusiastic, result-driven professional, principal cyber security consultant and solution architect. Team leader, lead of various IT and security programmes and projects. 20+ years experience in delivering to businesses and CTO offices, innovating, shaping vision and directions, engaging with customers and consulting. [\(ISC\)2 CISSP Certified Professional](#).

- Measurable impact at the business level. Lead and deliver strategic & technical work, including recent cyber security projects and programmes on user & entity behaviour analytics (UEBA), big data for security, threat detection & management, security analytics, security risk assessment, situational awareness and identity access management.
- 15+ years consulting experience at strategic and business levels, in cyber security and enterprise solution areas: IT, Telco, Financial/Banking, Energy, Manufacturing, Health Care, Government sectors.
- Experienced communicator at senior (CTO, VP, Director) level, within business organizations and worldwide customers.
- Managed multiparty, interdisciplinary and international security projects including UK TSB EnCoRe and EU PRIME projects.
- Experienced in engaging with and delivering to consulting teams, SOCs and cyber security defence organisations.
- In depth understanding of cyber security, attacks, kill chain & APT threats, security controls and incident management.
- Experience of security risk assessment, SW & system architectures, software solution design and development.
- Completed architecture, design and development of next generation security management solutions for enterprises and hybrid clouds by using virtualization, big data and security technologies.
- Innovator and technologist in corporate R&D (CTO Office / HP Labs). Filed more than 50 patents (18 granted patents).
- Experienced presenter at public events, industrial trade shows and conferences. Published many refereed articles & papers.
- (ISC)2 CISSP certified security professional, MSc, IISP Associate and Senior IEEE Member.
- Internal training for CSA CCSK and SANS Forensics.

### SKILLS

Analysis of complex problems; delivery of projects and solutions; identification of new business and R&D opportunities; project management; consulting; requirement gathering and specifications; architecture, solution & system design; SW development. Expertise:

- Security, Cyber security
- Big Data and Security Analytics
- Cloud Computing
- UEBA, SIEM, Event Management, Situational Awareness, Cyber Threat Intelligence
- Security Risk Assessment, Decision Support Solutions, Simulations, What-if Analysis
- AI, Machine Learning and Data Mining
- Web-based & enterprise technologies and solutions, IAM, PKI, Privacy & Policy Management, use of Cryptography
- Software Design & Development: Java, C#, C, JavaScript, Web Services, REST, SOA, UML.

### EMPLOYMENT HISTORY

**Principal Cyber Security Consultant** **09/2017 - present**  
(Cyber Security, Big Data, Analytics, Cloud)  
BMT Defence Services Ltd, Bath

**Cyber Security Startup Investigation, CISSP Certification, Consulting** **05/2017 – 08/2017**  
Investigated creation of a Startup in the cyber security space, focusing on Big Data for Security, advanced Threat Analytics and visualization. Achieved CISSP certification. Consulting.

**Principal Cyber Security Solution Architect and Lead** **2016 – 04/2017**  
(Cyber Security, Big Data, Analytics, Cloud)  
Hewlett Packard Enterprise, Bristol, UK

Principal security solution architect, technical & team lead of cyber security projects focusing on enterprise, hybrid cloud, virtualization.

- Shaping vision and directions to detect and manage advanced persistent threats (APTs) across the entire kill chain.
- Team and technical leadership. Management of roadmap and deliverables.
- Engaged with business organisations and consulting teams for solution and service delivery.
- Leading architectures, software design and development of next generation security threat detection & remediation solutions based on user & entity behaviour analytics (UEBA) and big data analytics. CTO, VPs and program manager-level interactions.
- Delivered solutions to collect big data sets (DNS, netflow, HTTP/S, etc.), perform security analytics and detect APT attacks.
- Using state-of-the-art big data technologies, including ELK, Kafka, Storm and Spark within processing & analytics pipeline.

**Principal Cyber Security Solution Architect and Lead: Master  
(Big Data for Security)**

**2013 – 2016**

**Hewlett Packard Labs (CTO Office) and Hewlett Packard Enterprise, Bristol, UK**

Technical and team lead, principal software & solution architect of Big Data for Security project. Detection of unknown security threats within organisations: collection, analysis and visualisation of massive amounts of (security) events.

- Delivered big data for security solution to HPE security business groups, productised as DNS Malware Analytics (DMA) and announced at HP Protect 2015. Integration with HPE Vertica, TippingPoint and ArcSight.
- Coordinated business, strategic and technical work with various stakeholders within and outside HPE, including customers, HPE security consulting and cyber security defense teams.
- Security consulting. Engaged in 50+ customer meetings, shared vision, created business awareness, enabled HPE security sales.
- Shaped technical vision; designed the overall architecture of backend analytics engine and data processing framework.
- Led team of developers. Researched and developed a library of new security analytics.
- Led 3 pilots/PoCs with customers and HPE world-wide SOC/Cyber Security Defense team.
- Filed patents.

**Project Manager and Coordinator of UK TSB EnCoRe Project  
(Security, IAM and Privacy Management)**

**2011 – 2012**

**Hewlett Packard Labs (CTO Office), Bristol, UK**

- Project manager and coordinator of UK (TSB co-funded) collaborative EnCoRe Project (2011-2012). Participants: QinetiQ, LSE, University of Oxford, HP Labs.
- Lead Architect and technologist (2008-2012). Successfully delivered EnCoRe reference architecture for privacy-aware Identity and Access Management along with related security software solutions.
- Coordinated and managed participants to achieve agreed goals.
- Strategic interactions, consulting and knowledge sharing with UK Cabinet Office team (Identity Assurance Program)

**Senior R&D Technical Lead: Expert  
(Situational Awareness, Security, Risk Assessment and Threat Modelling, IAM, Consulting)**

**2004 – 2012**

**Hewlett Packard Labs (CTO Office), Bristol, UK**

- Delivered strategic R&D programs and security projects involving HPE business groups in the areas of situational awareness, security, model-driven security risk assessment, IAM analytics, IAM, access control and privacy management
- Coordinated, managed and technically led teams of contractors and interns in the context of the international, multiparty and multidisciplinary EU EnCoRe project
- Led architectural, design and development work.
- Consulting with various customers, including NATO MNE7 initiative on cyber security and situational awareness.
- Filed patents. Active on publication and conference front.

**Research Scientist: Specialist  
(Security, IAM, PKI, Web Services)  
Hewlett Packard Labs (CTO Office), Bristol, UK**

**1999 – 2004**

<b>Research Scientist: Member of Technical Staff</b> (Enterprise System and Service Management) Hewlett Packard Labs, Bristol, UK	<b>1996 – 1998</b>
<b>Senior System Architect and Consultant</b> Telesoft SpA (owned by Telecom Italia/TIM), Turin, Italy	<b>1994 – 1995</b>
<b>System Architect, IT Consultant, Software Developer</b> Telesoft SpA (owned by Telecom Italia/TIM), Turin, Italy	<b>1991 – 1993</b>

## EDUCATION AND TRAINING

<b>MSc in Computer Science and Second Computer Science Degree</b> Universita' di Torino – Computer Science, Turin, Italy Top marks – 110/110 with honors Advanced data management, data mining, machine learning, AI and networking	<b>2003 - 2005</b>
<b>Bachelor's Degree, Computer Science Degree, Advanced Information Management</b> Universita' di Torino – Computer Science, Turin, Italy Top marks – 110/110 with honors Foundations of computer science, mathematics, AI, Information management, SW design & development, databases	<b>1986 - 1990</b>

## PROFESSIONAL AFFILIATIONS/MEMBERSHIPS

- (ISC)2 CISSP Certified Security Professional
- Institute of Information Security Professionals (IISP) Associate
- Senior IEEE Member

## COURSES

- SANS Institute: Forensics 572 - Advanced Network Forensics and Analysis
- Machine Learning (HPE course)
- Vertica & Analytics (HPE course)
- Baltimore Technologies: PKI and Identity Access Management
- TOGAF (HPE internal courses)
- CSA Security Guidance in Cloud Computing - CCSK (HPE internal courses)

## PUBLICATIONS

A list of publications and presentations is available at: <http://www.marcocasassamont.com/publications.htm>