

Marco, Casassa Mont - Bristol, UK

MSc Computer Science, CISSP, Senior IEEE Member, IISP/CII Sec Member

marcocasassamont@gmail.com, <https://www.linkedin.com/in/marcocasassamont>, <http://www.marcocasassamont.com/>

OVERVIEW

Principal Cyber Security Consultant and Manager. Over 25 years of experience in cyber security, solution architectures and technical solutions. Worked at technological, business, management and strategic levels for enterprise, defence, CTO and R&D organisations. Lead of cyber security and technology programs. Project & team management. Business development. Broad experience and knowledge in: cyber security solutions, cloud, big data, solution architectures, threat intelligence, defensive monitoring, SIEM/UEBA, security analytics, vulnerability management, threat & risk analysis. Expertise in AI/ML. Use of agile methodologies, Innovator (31 granted patents, 50+ filed patents). Prior to joining BMT, I was a Principal Cyber Security Solution Architect at HPE and R&D Master at HP Labs. MSc Computer Science, (ISC)2 CISSP, Senior IEEE Member, IISP/CII Sec Member.

- Led and delivered multi-million-dollar projects. Lead of strategic cyber security projects/programmes in key cyber security areas, including: SIEM/UEBA, big data for security, cyber threat detection & management, security analytics, threat intelligence, security risk analysis, situational awareness, AI/ML, IAM & privacy management.
- 18+ years consulting experience at strategic, business and technical levels, in Enterprise, Government/Defence, Telco, Financial/Banking, Energy and Manufacturing sectors.
- Experienced communicator at senior (CTO, VP, Director) level, leading interactions with business organizations, customers and partners worldwide.
- Directed multiparty, interdisciplinary, international security projects including UK TSB EnCoRe and EU PRIME projects.
- Experienced in delivering to complex organisations, SOC & cyber security defence teams.
- In depth understanding of cyber security, cyber-attacks, kill chain, APT threats, security risk assessment, security controls and incident management processes.
- Experienced use of cyber security standards, including: ISO27001-3, NIST Cyber Security Framework (CSF), NIST SP 800-53,37, etc. MITRE ATT&CK, NCSC Cyber Assurance Framework (CAF).
- Experienced Software Solution Architect, design and development lead.
- Experienced Security Solutions Architect, design and development lead for enterprises and hybrid clouds (virtualization, big data and security technologies).
- Innovator, lead technologist in corporate R&D (HP Labs/CTO Office). Filed more than 50 patents (31 granted).
- Experienced presenter: public events, industrial trade shows, conferences. Published 60+ referred articles & papers.
- MSc Computer Science, CISSP, IEEE Senior Member, Chartered Institute of Information Security (CII Sec) Associate.

SKILLS AND KNOWLEDGE

Analysis of complex problems; delivery of projects and solutions; Agile methodology; business development; identification of R&D opportunities; project and team management; leadership; consulting; architecture, solution & system design; continuous learning.

Interpersonal skills: presentation skills, client relations, decision-making, negotiation, customer engagement, problem solving, conflict management

Industry knowledge:

- Cyber security, IT Security
- Cloud Computing
- Big Data and Security Analytics
- 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, Engineering & Development
- Use of cryptography

EMPLOYMENT HISTORY

**Principal Cyber Security Consultant and Manager
(Cyber Security, Big Data, Analytics, Cloud)
BMT Defence and Security, Bath**

08/2018 - present

Principal Cyber Security Consultant. Team Manager. Roles:

- Project Manager, Team Lead & Technical Lead
- Lead Cyber Security & Solution Architect
- Cyber security consulting
- Customer friend role
- R&D & Innovation
- Bidding, Strategy & Business Development
- Enabling Agile Methodology
- Risk Analysis & Management: ISO 27001-3, NIST CSF, NCSC CAF, MITRE ATT&CK, NCSC CAF

Work and Consulting Areas: Cyber Security, Enterprise Cyber Security Solutions, Solution Architectures, SIEM, Threat Intelligence, Cloud, AI/ML, Big Data Platforms, Big Data, Cyber Security & Threat Analysis, Cyber Vulnerabilities Management, Cyber Risk Analysis, UADs, Security Controls.

Business Areas: Defence, Government, Commercial / Enterprise

**Principal Cyber Security Consultant
(Cyber Security, Big Data, Analytics)
BMT Defence and Security, Bath**

09/2017 – 08/2018

Principal Cyber Security Consultant. Roles:

- Project Management
- Technical Lead
- Lead Cyber Security & Solution Architect
- R&D & Innovation
- Enabling Agile Methodology
- Risk Analysis and Management: ISO 27001-3, NIST Cyber Security Framework (CSF)
- Bidding, Strategy, Business Development

Work and Consulting Areas: Cyber Security, Enterprise Solutions, Solution Architectures, Big Data, Big Data Platforms, Threat & Security Analytics, Cyber Risk Analysis, Vulnerability Management, Cloud.

Business Areas: Defence, Government, Commercial / Enterprise

Cyber Security Start-up Investigation, CISSP Certification, Consulting

05/2017 – 08/2017

Investigated creation of a Start-up 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
(Cyber Security, Big Data, Analytics, Cloud)
Hewlett Packard Enterprise, Bristol, UK**

2016 – 04/2017

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) Hewlett Packard Labs (CTO Office) and Hewlett Packard Enterprise, Bristol, UK	2013 – 2016
<p>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.</p>	
<ul style="list-style-type: none"> • 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) Hewlett Packard Labs (CTO Office), Bristol, UK	2011 – 2012
<ul style="list-style-type: none"> • 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) Hewlett Packard Labs (CTO Office), Bristol, UK	2004 – 2012
<ul style="list-style-type: none"> • 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
Research Scientist: Member of Technical Staff (Enterprise System and Service Management) Hewlett Packard Labs, Bristol, UK	1996 – 1998
Senior System Architect and Consultant Telesoft SpA (owned by Telecom Italia/TIM), Turin, Italy	1994 – 1995
System Architect, IT Consultant, Software Developer Telesoft SpA (owned by Telecom Italia/TIM), Turin, Italy	1991 – 1993

EDUCATION AND TRAINING

MSc in Computer Science and Second Computer Science Degree

2003 - 2005

Universita' di Torino – Computer Science, Turin, Italy

Top marks – 110/110 with honors

Advanced data management, data mining, machine learning, AI and networking

Bachelor's Degree, Computer Science Degree, Advanced Information Management

1986 - 1990

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

PROFESSIONAL AFFILIATIONS/MEMBERSHIPS

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

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 60+ publications and presentations is available at: <http://www.marcocasassamont.com/publications.htm>