Marco Casassa Mont

ISACA CISM | ISC2 CISSP and CCSP | Senior IEEE Member | CIISec | MSc, BSc Computer Science

Bristol, UK

Email: marcocasassamont@gmail.com, LinkedIn: https://www.linkedin.com/in/marcocasassamont

Overview

Principal Cyber Security Consultant, Architect and Senior Manager. A leader and technologist working at the intersection of business, cyber, technology and management. Over 25 years of experience in: cyber security for cloud, enterprise, OT; security architectures and software solutions; applied AI; trusted advisory; team leadership and management; strategy and risk management. Passionate about innovation to address business needs. Driven by results.

At Hewlett-Packard (CTO Office, Security Centre of Excellence) I shaped cyber security vision; produced cyber strategies and created business opportunities through innovation. I directed teams and projects. I architected systems, coordinated the implementation of advanced security technologies and software solutions. Key achievements:

- Generated new, multi-million-dollar business outcomes with the delivery of 20+ new technologies and solutions, driven by innovation. Named inventor of 50+ patents, 31 granted patents;
- Directed 5+ multi-million-dollar, complex, international and interdisciplinary technical projects and team;
- Managed medium-large teams to deliver security software solutions and consultancy;
- Published 60+ referred articles, presented at 30+ international events, conferences and exhibitions.

At BMT Defence & Security, UK my focus is on strategic cyber consulting, project management, business development and bids, R&D work. Key achievements:

- Provided trusted advisory to 15+ medium/large projects in detection (SIEM, UEBA, Threat Hunting), enterprise and cloud security; applied AI; IT/OT security, risk management. Enabled digital transformation programs. Defined strategies, solution architectures. Security control design and option analysis.
- Coordinated and won 10+ bids, worth multi-million pounds;
- Line management responsibilities, team leadership and mentoring. Project management.

Skills & Abilities

Leadership. Decision-making. Customer engagement. Bridging business-technology gaps. Management of complex client relationships. Negotiation, persuasion skills. Conflict management & resolution. Communication at all levels.

Expertise Areas

- Detection (SIEM, UEBA) and Threat Hunting; security analytics (AI/ML); big data (Hadoop, Elastic, Spark); threat intelligence; deception.
- Cloud security (Azure, AWS, etc.); IT and OT security; vulnerability threat management (VTM), end-point management (XDR), asset management; SOAR; UADs; IAM; PKI; Network Traffic Analysis; Privacy.
- Risk analysis; policy management. Enterprise Architecture and TOGAF.
- ISO 27001, NIST CSF, NIST security & risk guidelines, MITRE ATT&CK, NCSC CAF, CSA, OWASP, CIS.
- Security operations, cyber incident response, APT threats, protective & detective security controls.
- Agile, DevOps methodologies, tools. Software solution design and development with open-source solutions.

Work Experience

Principal Cyber Security Consultant **[2017 – present]**

BMT Defence and Security, Bath, UK [Defence, Government, Public, Commercial, R&D]

- Led 10+ customers' cyber security projects, consultant teams and developers. Provided trusted advisory. Liaised with key Customers' stakeholders and decision makers. Defined and agreed requirements. Assessed commercial solutions. Carried out option analysis. Project planning, resourcing, budget and team management.
  Areas: cloud, vulnerability management, SIEM/UEBA (Securonix, Splunk, Elastic), threat detection, network traffic analysis, UADs, threat intelligence, big data platforms, deception, AI, risk assessment.
  Outcomes: 10+ projects delivered in time by matching or exceeding customer's expectations. Key delivered projects for Defense and Government Agencies include:
  - Migration of threat detection capability to the cloud (digital transformation);
  - Risk management for critical (AWS-based) cloud solutions;
  - SIEM and UEBA option analysis and commercial solution selection;
  - Assessment of extant Cyber Security Controls (vulnerability management, XDR, asset management);
  - Cyber Vulnerability Investigation (CVI)-based Analytics (digital transformation).
- Coordinated or contributed to 10+ successfully business bids. Generated multi-million-pound wins.

- Led 5+ research and innovation activities that subsequently supported business development / bids for: cyber security, cyber for commercial maritime, Operational Technology (OT) / ICS. Use of AI/ML and analytical platforms for threat management (MITRE ATT&CK). Outcomes: won multi-million-pound bids - Defence R&D.
- Led 2 engagements with Universities and MoUs supporting joint commercial and R&D activities.
- Achieved 3 key cyber professional certifications: $(ISC)^2$ CISSP, $(ISC)^2$ CCSP and ISACA CISM.

Principal Cyber Security Solution Architect. Technical Solution Lead **[2013 – 2016]**
Hewlett Packard Labs (CTO Office) and Hewlett Packard Enterprise, Bristol, UK
[Private, Public, Commercial, Financial, Energy, Manufacturing, R&D]
Led multi-year, multi-million dollar 'Big Data for Security' project and team of 5-10 people over 3 years. Produced a new, commercial HP cyber security solution offering and security analytical capabilities.
Outcomes: delivered 1 new HPE solution, 'DNS Malware Analytics' (DMA) and related HPE consulting services. Provided new capability to detect unknown cyber security threats in enterprise and cloud:

- Engaged with 50+ customers, influenced vision, supported sales. Led 3 customer-based pilots / PoCs.
- Coordinated business, strategy and technical work with business stakeholders. Technically led SW development teams of 5-10 people.
- Created technical vision. Architected cyber analytics engines, data processing pipelines, Asset Discovery & Management; (SOAR-based) Software Defined Network (SDN) for automated incident remediation.
- Influenced CTO, VPs and program managers with roadmap and directions for next-generation advanced persistent threats (APTs) detection and UEBA solutions. 10+ granted patents.

Director and Program Manager of UK TSB EnCoRe Project. Lead Architect **[2008 – 2012]**
Hewlett Packard Labs (CTO Office), Bristol, UK [Private, Public, Academies, R&D]
Directed EnCoRe (2010-2012), a multi-million-pound (UK TSB co-funded) Project with QinetiQ, LSE, University of Oxford, HP Labs. Coordinated HP teams as lead architect and technologist (2008-2012). Outcomes:

- Delivered a reference architecture for privacy-aware IAM. Delighted UK TSB officials.
- Produced 3 security software solution PoCs for cloud and enterprise.
- 5+ patents. Influenced HP businesses and briefed UK Cabinet Office team (Identity Assurance Program).

Senior R&D Technical Lead **[2004 – 2012]**
Hewlett Packard Labs (CTO Office), Bristol, UK [Private, Public, Commercial, Financial, R&D]
Led 10+ strategic R&D programs and security projects: cloud security, economics and shared responsibility model; situational awareness; safe data sharing in the cloud; cyber security solutions; model-driven security risk assessment; IAM analytics, controls and privacy. Outcomes:

- Produced architectural, design, SW development which resulted in new HP security commercial solutions.
- 20+ consulting engagements, including NHS, DWP, NATO MNE7. 10+ patents; 20+ publications.

Senior Research Scientist (and other technical roles) **[1996 – 2004]**
Hewlett Packard Labs (CTO Office), Bristol, UK [Private, Public, Commercial, R&D]
Developed architectures and implemented R&D solutions for IAM, PKI, Web Services, advanced cryptography.
Outcomes: 5+ patents; PoCs; transferred 10+ technologies and solutions to HP Business Groups; 10+ publications.

Education

- **Professional Certifications**
  - ISACA CISM, (ISC)2 CISSP, (ISC)2 CCSP, Senior IEEE Member, UK CIISec Member
- **MSc and BSc in Computer Science**
  - Universita' di Torino – Computer Science and AI/ML, Turin, Italy. Top marks: 110/110 with honors

Thought Leadership and Innovation

- **Filed and Granted Patents:** https://patents.justia.com/inventor/marco-casassa-mont
- **LinkedIn:** https://uk.linkedin.com/in/marcocasassamont
- **Twitter:** https://twitter.com/mcasassamont
- **Google Scholar:** Marco Casassa Mont - Google Scholar
- **ResearchGate:** https://www.researchgate.net/profile/Marco-Casassa-Mont
- **DBLP:** https://dblp.org/pid/84/2474.html