Gerard Guillemas Martos - Security Engineer

> Freelance security engineer with 10 years of professional experience in the cybersecurity field. Focus in security processes, secure software/infrastructure engineering and security training. Over 7 years in Adevinta working on security automation to effectively scale security to a massive organization without significant operational burden. Background in consulting for Deloitte and Ernst & Young in the fields of security operations, incident response and ethical hacking.

	Personal	Company
Location	Barcelona, Spain	www.BoxSec.com
Mail	gerard ✉ geramail ○ com	gerard ✉ boxsec ○ com
Github	github.com/gguillemas	github.com/boxsec
LinkedIn	linkedin.com/in/gguillemas	linkedin.com/company/boxsec

Experience

BoxSec

Freelance Security Engineer
Mar 2023 - Present

Custom software, advisory and training to improve information security processes.

- Developing custom automations, tools and features to integrate security into the business.
- Establishing strong security foundations, increasing coverage and reducing operations.
- Training technical and business roles in modern and effective security practices.

Adevinta

Staff Security Engineer
Jun 2019 - Mar 2023 (3 years 10 months)

Staff Security Engineer in the Purple Team, part of the Secure area.
Working in a central organization supporting several international brands.

- Designed and developed internal security automation products.
- Advised and supported companies in integrating security into their processes.
- Focused on a scalable, self-serve and highly automated security scanning platform.
- Integrated open-source and commercial security products into our scanning platform.
- Developed a pipeline to automatically inventory scannable assets from AWS accounts.
- Developed a service to provide users with self-serve access to aggregated security metrics.
- Developed a pipeline to deploy infrastructure and run stress tests on our access gateway.

- Authored RFCs on container image scanning, authenticated scans, security monitoring...
- Led a squad defining the security metrics used to track global vulnerability remediation.
- Created a report analyzing the security status of the company across various benchmarks.
- Designed a user-friendly impact assessment methodology for users to classify AWS accounts.
- Participated in several major migrations, including internal domains, AWS, Okta and Github.
- Coordinated a major review of the interface in our main product with the central UX team.
- Maintained the code and infrastructure of our custom self-serve network access gateway.
- Microservices-based systems programming with Go and some Python/JavaScript.
- Deployment with Github, Travis and Spinnaker to AWS and Kubernetes.
- Operations with Sumologic, Datadog, Grafana and PagerDuty.

Engineering Area Lead
Sep 2018 - Jun 2019 (10 months)

Engineering Lead in the Secure area, part of Platform Services.
Working in a central organization supporting several international brands.

- Responsible for the global security area, with three teams and 15 members.
- Managed the leadership team in the area and coordinated cross-team initiatives.
- In charge of budget, headcount negotiations and adjusting the team scope accordingly.
- Worked with the TPL and TPOs on the area roadmap, objectives and long term strategy.
- Established a transparent system to distribute training budget more effectively.
- Instituted a framework to support engineers in dedicating 20% of their time to R&D.
- Member of the leadership team of Platform Services, responsible for over 100 engineers.
- Collaborated with EALs from other areas in strategic people and engineering initiatives.
- Participated in the hiring committee responsible for global engineer hiring decisions.
- Coordinated a review to improve the effectiveness of the global engineer hiring process.
- Created a program that supported over 70 engineers in receiving training from their peers.

Engineering Manger
Apr 2018 - Sep 2018 (6 months)

Engineering Manager in the Purple Team, part of the Secure area.
Working in a central organization supporting several international brands.

- Manager of a continuous security team with 6 members in Barcelona and Oslo.
- Responsible for team organization, budget, hiring, salary reviews and promotion cases.
- Worked with senior management to overhaul the security roles and their compensation.
- Product ownership of the main product of the team. NPS increase in 2018H2 from 43 to 78.
- Responsible for stakeholder relationships, external communications and the product roadmap.
- Facilitation of product and technical discussions, writing RFCs and creating documentation.
- Helped the team and our coach improve our working methodology in rituals and Jira.

Senior Security Engineer
Feb 2016 - Apr 2018 (2 years 3 months)

Senior Security Engineer in the Purple Team, part of the Secure area.
Working in a central organization supporting several international brands.

- Designed and developed internal security automation products.
- Advised and supported companies with integrating security into their processes.
- Focused on a scalable, self-serve and highly automated security scanning platform.
- Designed a distributed security scanning architecture based on AWS and Docker.
- Developed a specialized container orchestration component for security checks.
- Developed a centrally managed security rules service for multiple AWS accounts.
- Developed custom security checks to detect specific vulnerabilities and weaknesses.
- Integrated open-source and commercial security products into our scanning platform.
- Organized and coordinated an off-site CTF competition for around 100 engineers.
- Trained around 100 engineers worldwide on secure software engineering practices.
- Conducted over 150 security interviews for security and other engineering roles.
- Microservices-based systems programming with Go and some Python/Ruby/JavaScript.
- Deployment with Github, Travis and Spinnaker to AWS and Kubernetes.
- Operations with Sumologic, Datadog, Grafana and PagerDuty.

Deloitte

Senior IT Security Analyst
Jan 2015 - Feb 2016 (1 year 2 months)

Technical IT security analyst for the CyberSOC in the IT ERS area.

- Leading the e-crime team in a major bank. Malware detection, analysis and response.
- Developed tools to deobfuscate and analyze web injections from banking malware.
- Developed a script to detect online banking customers infected with web injections.
- Developed a service to extract money mules from the C&C and block outgoing transfers.
- Developed a service to enrich SIEM events with various threat intelligence sources.
- Developed a custom mail server to automatically analyze suspicious messages for the SOC.
- Performed technical testing of anti-malware solutions and developed security controls.
- Conducted forensic analysis of compromised machines, network traffic and security events.
- Reported authentication bypass and RCE vulnerabilities on the FireEye HX console.
- Participated in both real and simulated government security exercises.

Ernst & Young

IT Security Consultant
Nov 2013 - Dec 2014 (1 year 2 months)

Technical IT security consultant for the Advanced Security Lab in the ITRA area.

- Security audits of web applications, networks, firewall, Wi-Fi and NAC deployments.
- Completed an RFP and selection process for a complex large scale IPS device deployment.

- Part of the security office of an automotive client. Incident handling and malware analysis.
- Developed a library and web application to extract malicious macros from Office documents.
- Developed a Windows service and client to allow and audit temporary privilege elevation.
- Developed a web application to create, manage and visualize security indicators.

University of Barcelona

Internship
Nov 2012 - Nov 2013 (1 year 1 month)

Internship at the Data Exploitation department performing academic data mining.

- Developed database management applications in .NET and created custom queries in SQL.
- Maintained and improved public web applications in PHP for querying curated datasets.
- Automated several formatting, exporting and data validation tasks in VBScript and AutoIt.
- Internally reported vulnerabilities in the systems and applications of the university.

Education

Bachelor's Degree in Physics
University of Barcelona
2010 - 2013 (Unfinished)

Certifications

FireEye Systems Engineer
FireEye
Jan 2016

TOEIC
ETS 990/990
Jan 2015

Cryptography I
Stanford University via Coursera
Nov 2014

Certified Ethical Hacker
EC-Council
Jul 2013

Certificate in Advanced English
Cambridge English Language Assessment
Aug 2011