# Gabriel Iuga

Languages: **English / Romanian**

Security Clearances: **Nil but able to obtain**

Previous/Current Employer: **Exabeam**

Previous / Current Position: **Principal Application Security Engineer**

Education / Certificates **OSEP OSWE CRTO OSCP**

## Summary

Senior Application Security Engineer with 5 years' experience in a fully security orientated role, and 13 years' previous security experience in a mixed role (security, development and server management). I currently hold 3 Offensive Security certifications (OSEP, OSWE, and OSCP) as well as a ZeroPointSecurity certification (CRTO) which focuses on adversary simulation, active directory and command and control skills.

Seeking a challenging position, which will make best use of existing skills and expertise, whilst also providing opportunities for continuing professional development.

---

### Key Skills

• Application and network penetration tests
• Privilege escalation and lateral movement
• Building custom exploits and automation scripts
• Antivirus and EDR bypass and evasion – custom payload development
• Experience with Python / Go / C# / Rust / PowerShell / PHP / Java
• Ability to communicate across different organisational layers, including C-level

### *Personal Projects / Interests*

- Obtained OSEP - https://www.credential.net/5de67395-5e1f-40fd-a316-ddfc60810655
- Obtained OSWE - https://www.credential.net/1b0f0c98-bc6b-4176-9222-acb11b055fb0
- Obtained CRTO - https://api.eu.badgr.io/public/assertions/tRkZsPUxRoyJGVAniUvOGA
- Obtained OSCP – https://www.credential.net/7e7557d0-d7b2-452a-a445-978fd3e80ba7
- Continuous learning via HackTheBox (https://app.hackthebox.eu/profile/324095)
- Sharing knowledge and enticing others to join cybersecurity via streaming: https://www.twitch.tv/0xsyk0
- Plans on extending my knowledge through further certifications such as OSED / CRTL

**Commercial Experience**

***Exabeam (previously known as Logrhythm)***

***Principal Application Security Engineer***

August 2021 – present

- Pentest and red team engagements
  - Running internal pentests on all the company's products
    - White box pentest approach
    - Code analysis for each product
    - Supply POCs and remediation steps to the engineering teams while re-testing once the fix is in place
  - Running red team engagements on a regular basis
    - Ran assumed breached red team engagements to allow the SOC team to develop better alerts and rules
    - Developed custom payloads to bypass antivirus and installed EDRs
    - Tested data exfiltration and lateral movement
  - Purple team engagements
    - Re-runs of previous red team engagements while on call with the SOC team to allow a step-by step check of rules and alerts
    - Collaborating on rule and alert creation when and where it was required
  - Preparing payloads and C2 infrastructure
    - Writing C2 infrastructure as code (ansible) to allow easier deployment when required
    - Testing different C2 frameworks and the detection of them in the lab environment
    - Creating a lab environment to be able to test payloads (rust loaders, nim loaders) to bypass antivirus and EDRs (where possible)
- SAST / SCA / DAST
  - Managing the infrastructure required for internal scanning on all repositories with SAST/SCA/DAST tools o Managing integration between the tools and git repositories to allow PR scans and automated results submission to the engineering teams via communication platforms (Slack, Teams)
  - Triage of results and management of false positives
- AI
  - Developed an application that validates findings using AI, for true positives it creates a PR in Github with a proposed fix
- Misc
  - Collaborate with the engineering teams to include security first in the programming approach
  - Create data flow diagrams and process flow diagrams to aid in threat modelling

***Plug and Play Design***

***Head of Technology***

November 2014 – August 2021

- Infrastructure and hosting
  - Provisioned and maintained the hosting fleet (40 + dedicated servers, 30+ virtual servers) • Monitoring and incident response across the full range of servers
  - Developed internal tooling for automated tasks using Python, GoLang, Ansible, Terraform, and Packer
- Development and management
  - Travel industry – a VueJs driven front-end, connected to a Laravel back-end using an external API that provides the data (C# driven)
  - Charity – Managed a team of developers to provide a VueJS SPA and a Laravel backend in a short timeframe, integrating with third party services like Secure Trading, EazyCollect, and Podio (CRM)
  - Access Control industry – Managed the team of developers behind the website while creating a custom hosting infrastructure including Varnish caching.
  - Events industry – built the integration of a Wordpress site to Microsoft Dynamics CRM
  - Real Estate industry – Property and lease management application using Laravel, meant to be used by multiple individual landlords. Integrated the platform with third party services like Signable, GoCardless, Zoopla, and Stripe.
  - Real Estate industry – Built the integration of a Wordpress website to Zoopla and RightMove via DataFeed. • Key decision-maker on what technologies to be used for each project and instrumental in translating business needs into technical requirements.
  - Managed a team of 4-7 Software Developers
- Led and developed multiple projects in PHP with Laravel, Wordpress and Magento:
  - Retail industry – Magento ecommerce website, managing over 4,000 products. Developed complex scripts for the automation of continuous data-migration, to avoid downtime. Built the integration between the customer's ERP system, Sage200, to Magento.
  - SaaS ERP – built complex reporting using Java.
- Responsible for setup and maintenance of hosting servers using Centos 6/7 and WHM/cPanel and of a Nagios monitoring server.
- Retail industry - led and developed an ecommerce website using Magento. Implemented a custom pseudocode-to code translator, which allowed platform administrators to create complex price calculation formulas using multiple types of product variables.

***Multiple organisations: Colt Technology Services, GiftsDirect, OSF Global Services, VanRoey Automation NV, Aim4Solution***

***Web Development (Java / PHP)***

September 2008 – October 2014