Josh Rickard

SECURITY AUTOMATION ARCHITECT

☎ [redacted]

✉ josh.a.rickard@gmail.com

📍 [redacted]

👤 Linkedin.com/in/josh-rickard

💬 Twitter.com/MSAdministrator

🔗 letsautomate.it

ABOUT ME

I am a creator and problem solver focused on security automation, open-source tools and defensive security so that everyone has a fighting chance.

SKILLS

9 / 10	Security Automation
9 / 10	Python
9 / 10	PowerShell
10 / 10	Group Policy
7 / 10	DFIR
8 / 10	Architecture & Design
8 / 10	REST & SOAP APIs
8 / 10	CI / CD platforms
10 / 10	MEME game
6 / 10	AWS / Azure

EXPERIENCE

Sr. Detection Validation Engineer

Red Canary / Colorado / Oct 2022 to Jan 2023

Due to a reduction in force my position was let go. I was part of Red Canary's Detection Enablement division focusing on proving detection capabilities at scale.

- Assisted with development of a Ruby on Rails web application to streamline testing of attacker techniques and tools.
- Assisted with development of infrastructure using Terraform and Ansible to build, deploy and execute several attack testing frameworks across multiple operating systems, EDR products and more

Sr. Security Solutions Architect

Swimlane / Colorado / Dec 2018 to Oct 2022

I was part of the Swimlane research team which focuses on innovative security automation, building content and giving back to the security community.

- Built SOAR playbooks that automated complex and unique processes used by some of the largest private, public and governmental organizations in the world
- Implemented integrations with many critical security operations products like Elastic Security, AWS, CrowdStrike, Microsoft Graph and more.
- Released many open-source tools like pyattck, atomic-operator, soc-faker and more
- Contributed by writing several blogs, presenting on webinars and at conferences
- Ideation to implementation for several internal tools and frameworks, including content migration and generation, Swimmy the Slack bot, etc.

EDUCATION

BS in Computer Information Systems

Columbia College

2009 - 2012

GIAC Certified Windows Security Administrator (GCWN)

GIAC Certifications

Oct 2013 - present

GIAC Certified Forensics Analyst (GCFA)

GIAC Certifications

Sep 2014 - present

OTHER

Atomic Red Team Maintainer

Official Maintainer

Jan 2023

Tribe of Hackers: Blue Team

Featured author

Aug 2020

SC Media Reboot Leadership Awards

Awarded in the Influencer category

Sep 2019

President of Central Missouri InfraGard Member Alliance

Past director and president

Jan 2015 – Dec 2018

EXPERIENCE

Manager, Reporter Solutions Engineering

Cofense / Virginia / Dec 2015 to Nov 2018

Managed, designed and implemented features for all Cofense Reporter products which grew the product from 2 million to 15 million installs globally.

- Designed and managed day-to-day operations of new innovative products utilizing internal and external developers, from conception to market release
- Introduced automation tools for generation, verification and support of Cofense Reporter products, reducing support costs and reducing development time by 300%
- Technical Product Owner for 3 scrum teams (9 engineers & 6 quality assurance engineers)

TALKS

Conference Talks

Presented at several conferences including DerbyCon (2), CircleCityCon (2), ShowMeCon (2), WWHF (2), Hacker Halted, numerous BSides and more. You can find a full list here https://letsautomate.it/page/presentations

Webinars

Held several Swimlane webinars showcasing Swimlane use cases. You can find a partial list here https://swimlane.com/api/v1/events?searchTerm=Rickard&page=1&perPage=99&eventDate=past-events

News

Written, commented, interviewed and featured in many information security new sources from Wired to SC Magazine to ASIS. You can find a more complete list here https://letsautomate.it/page/press/