Contact

ryan@checksomebytes.com

www.linkedin.com/in/ryan-m-thompson (LinkedIn)

Top Skills

Microsoft Azure
AWS Security
Security Operations

Certifications

Elastic Certified Engineer
GIAC Advisory Board
GIAC Cloud Threat Detection (GCTD)
GIAC Certified Incident Handler (GCIH)
GIAC Cloud Forensic Responder (GCFR)

Honors-Awards

SANS SEC504 Challenge Coin
SANS FOR508 Challenge Coin
SANS FOR509 Challenge Coin
SANS FOR608 Challenge Coin
SANS SEC503 Challenge Coin

Ryan Thompson

Senior Cloud Security Researcher, SANS Instructor
Fort Collins, Colorado, United States

Summary

"While on my team Ryan initiated and completed several projects that resulted in process and tooling improvements which we use in our operations today." - Sean Leinart, Senior Manager @ Alert Logic

"It was a pleasure working and collaborating with Ryan on a daily basis at Elastic. I'll definitely miss the curiosity and constant inspiration to ask, "why?" - Brandon Devault, Education Architect @ Elastic

Experience

CrowdStrike

4 years

Senior Cloud Security Researcher (Overwatch R&D)
March 2023 - Present (2 years 11 months)

- Research and emulate adversary activity across AWS and Azure
- Build out proof-of-concept solutions for threat hunting
- Develop novel detection capabilities in the cloud control plane
- Engineer log normalization and filtering to allow for scalability without impeding threat detection

Senior Security Researcher
February 2022 - February 2023 (1 year 1 month)

- Conducted postmortem analysis of ongoing attacks by criminal and nation state actors
- Investigate advanced hands-on intrusions to extract indicators of compromise and uncover APT/criminal attack trends
- Developed automation capabilities to reduce the manual workload on researchers and to improve accuracy of analysis

SANS Institute

4 years 7 months

SEC541 Associate Instructor

March 2024 - Present (1 year 11 months)

- Instructor the SANS course SEC541: Cloud Security Threat Detection
- Manage classroom in both virtual and in-person contexts

SANS Teaching Assistant
July 2021 - Present (4 years 7 months)

Supporting SANS forensics courses including:

- SEC541 - Cloud Attacker Techniques
- FOR509 - Cloud Forensics
- FOR608 - Enterprise Forensics

Elastic
Education Engineer - Cyber Security
September 2020 - February 2022 (1 year 6 months)
Houston, Texas, United States

- Creating new courses in the domain of security analytics, liaising with instructors and other subject matter experts
- Collaborate with development teams and engineering to create and update existing course materials and documentation
- Convey domain specific knowledge in security analytics regarding the integration of security tools and the Elastic Stack

Alert Logic
2 years 8 months

Senior Security Analyst (Active Watch Enterprise)
March 2020 - September 2020 (7 months)
Houston, Texas, United States

-Create and productize hunt/investigative processes and techniques for other SOC analysts
-Build log and network detection to catch intrusion based on emerging threats
-Communicate security recommendations/findings to both technical and managerial stakeholders
-Work with leadership and the engineering team to improve and expand available toolsets

Professional Security Analyst (Active Watch Enterprise)
January 2019 - March 2020 (1 year 3 months)
Houston, Texas Area

-Monitor IDS, firewall, netflow and log correlation tools, for potential threats and create automated logic for detection

-Assist customers with Incident Response and investigations into compromises/breaches
-Tune Alert Logic proprietary security products to generate higher fidelity observables and reduce benign or “noisy” events from customer environments
-Provide mentorship to Security Analysts, and develop training program for incoming SOC analyst covering Log Correlation and Packet Analysis

Security Analyst
February 2018 - January 2019 (1 year)
Houston, Texas

- Respond to security incidents by collecting and analyzing log and network traffic data
- Leverage data from past incidents to collect indicators of compromise to improve threat detection
- Work with security engineers to improve AWS log visibility to ensure best practice according to CIS guidelines
- Continuous configuration of Security Information and Event Management (SIEM) using Regex
- Develop training program for incoming SOC analyst covering Windows, Linux, AWS, and Network logs

Hewlett Packard Enterprise
4 years

Systems Analyst
June 2015 - December 2017 (2 years 7 months)
Houston Tx

Primary administrator of direct procurement sourcing software that handles contracts, eAuctions, and supplier performance
Conducted system integration testing and oversaw user acceptance testing
Provided internal audit with contract requirements regarding SOX audits
Developed and maintained business continuity plans in case of system failures

Strategic Procurement Analyst
January 2014 - June 2015 (1 year 6 months)
Houston, Texas Area

Created functional proof of concepts and presented to management for executive buy-in
Bridge business users and technical team through creation of business requirements
Introduced and trained 150 employees on new procurement suite

Best Buy

Portable Electronics Lead

October 2008 - December 2013 (5 years 3 months)

-Responsible for training new and current employees around new services or products in the department

-Organized scheduling in department to ensure adequate coverage

-Implemented gap management to analyze and improve business opportunities

-Upheld merchandising standards in department and implemented a zoning system to divide responsibilities and provide accountability

Education

University of Houston

Bachelor of Business Administration (BBA), Supply Chain Management · (2010 - 2013)

Lone Star College System

· (2008 - 2010)