Ryan Eikanger

Minneapolis, MN
Phone: 651-366-7389 | Email: reikanger@gmail.com | Website: reika.io
LinkedIn: https://www.linkedin.com/in/reikanger/ | Portfolio: https://github.com/reikanger

Summary

Incident response specialist seeking a role in data science, machine learning, or Linux system administration. Proven ability to analyze data, communicate findings, lead under pressure, and remain calm in critical situations.

Technical Skills

Languages: Python, Shell, JavaScript, SQL

Data Science: Pandas, NumPy, Matplotlib, BeautifulSoup, Scikit-learn, TensorFlow

Databases: PostgreSQL, MySQL, MongoDB, ElasticSearch, SQLAlchemy, PyMongo

Big Data: Hadoop, MRJob, Apache Spark, PySpark

Systems and DevOps: Linux, Red Hat, NixOS, Git, Docker, Podman, Terraform, Ansible, SaltStack

Experience

Technical Manager April 2018 – Present
Mandiant (part of Google Cloud)
Minneapolis, MN
Key Accomplishments:

- Led simultaneous incidents while providing direction, a point of escalation, and guidance to key stakeholders and the engagement team
- Managed complex incident response engagements from start to finish, including directing communications and expectations between the delivery team, stakeholders, and internal and external counsel
- Conducted forensic analysis of various systems and devices, including Windows, Linux, macOS, and mobile platforms, to identify and preserve critical evidence
- Created and presented technical findings to both technical and non-technical audiences, including executive leadership and legal counsel, in written and verbal reports
- Collaborated effectively with cross-functional teams, including IT, security engineering, leadership, and legal, to ensure a coordinated and effective incident response
- Successfully contained and removed threat actors from client networks, while minimizing business disruption and data loss for clients
- Leveraged threat intelligence platforms and open-source tools to correlate incident data with known threat actors and campaigns
- Worked with external counsel to determine client regulation compliance and reporting requirements during data breach and extortion scenarios
- Developed and delivered training on incident response of Windows enterprise networks, Linux systems, and macOS systems

Incident Handler August 2016 – April 2018
Target Minneapolis, MN
Key Accomplishments:

- Developed custom tooling and methodologies to improve host- and log-based data analysis leveraging Python, Pandas, and Elasticsearch
- Administered a fleet of non-attributable systems for data collection using SaltStack
- Mentored a team of 50 incident response analysts and developed their skills, approach, and quality of documentation
- Created and delivered internal training and challenges to help build analysts' skills
- Developed and taught a memory forensics workshop for an external security conference

Consultant December 2014 – August 2016
Mandiant New York, NY
Key Accomplishments:

- Conducted thorough root cause analysis, identifying vulnerabilities, and recommending corrective actions to prevent future incidents
- Automated data enrichment and frequency analysis to increase efficiency of breach investigations
- Delivered comprehensive incident reports and analysis to clients, with actionable recommendations

Experienced Associate February 2012 – December 2014
PwC - Advisory Minneapolis, MN
Key Accomplishments:

- Installed, configured, and administered a Hadoop cluster to search 120TB of firewall log data
- Led penetration tests and security operations, and helped stakeholders understand discovered vulnerabilities
- Developed and implemented incident response plans, playbooks, and procedures, for multiple clients
- Led penetration tests and security operations, and helped stakeholders understand discovered vulnerabilities

Related Experience

SkyWatch: Flight and Weather Tracker - https://github.com/reikanger/skywatch

- A flight and weather visualization application to watch in real-time the influence of weather on flight paths of planes in the upper midwest

Crowdfunding ETL Pipeline - https://github.com/reikanger/crowdfunding-etl

- An implementation of an ETL (Extract, Transform, Load) pipeline to process and integrate crowdfunding campaign data

Mortgage Rates Exploratory Analysis - https://github.com/reikanger/mortgage-rate-insights

- An exploration of Consumer Financial Protection Bureau data to gain insights into mortgage rates by different customer classes, loan types, and demographics.

Education

Certificate, Data Science: University of Minnesota, Minneapolis, MN September 2024
Certificate, Cloud Forensics Responder: Global Information Assurance Certification (GIAC) 2023
B.S. Management Information Systems: Iowa State University, Ames, IA December 2011