

Dariia B.

Senior SecOps

SUMMARY

- Extensive experience in cybersecurity, currently working as a Security Systems DevOps Engineer at Datami, with a demonstrated history in several DevOps and DevSecOps roles, security system engineering, and network operations center roles. - Proven expertise in cybersecurity data analytics and automation, with project experience in developing authorization and authentication systems, utilizing tools such as OKTA OAuth, Salesforce demandware, Grafana, OpsGenie, Terraform, Sentry, Prometheus, and Rigor. - Proficiency in real-time big data management through Google Cloud Platform Monitoring (Stackdriver), and database development experience with MySQL, MSSQL, and Couchbase. - Skilled in software development practices and CI/CD toolsets, including Jenkins, Git, Docker, and Kubernetes, vital for MVP development in a fast-paced cybersecurity environment. - Significant experience in managing and responding to cybersecurity incidents in Network Operations Centers, beneficial for developing and implementing SIEM, SOAR, and XDR platforms. - Availability starting from 15/06/2023

TECHNICAL SKILLS

Main Technical Skills	AWS, GCP
Programming Languages	C++, Java, PHP, Python
JavaScript Frameworks	Node.js
Salesforce Ecosystem	Salesforce
Databases & Management Systems / ORM	AWS ElasticSearch, Couchbase, Memcached, Microsoft SQL Server, MySQL, Redis, Sphinx
Cloud Platforms, Services & Computing	AWS, GCP, PagerDuty
Amazon Web Services	AWS CloudWatch, AWS EC2, AWS ElasticSearch, AWS S3
Azure Cloud Services	Azure Kubernetes
Google Cloud Platform	Google App Engine, Google Cloud Compute Engine, Google Cloud Identity, Google Cloud Monitoring, Google Cloud Storage
Web/App Servers, Middleware	Apache HTTP Server, Internet Information Services (IIS), Nginx
Collaboration, Task & Issue Tracking	Atlassian Confluence, Jira
Version Control	BitBucket, Git

Virtualization, Containers and Orchestration	Docker, Kubernetes, Terraform
Logging and Monitoring	Grafana, Nagios, Opsgenie, Prometheus, Sentry
Deployment, CI/CD & Administration	Jenkins, Jenkins pipeline
Operating Systems	Linux, Windows
Message/Queue/Task Brokers	RabbitMQ
Platforms	Salesforce

EXPERIENCE

Security systems devops engineer/Secops

May 2023 - Present

Security systems devops engineer/Secops, Datami

Dec-2022 – April 2023

TechOps Engineer

Mar-2021 - Dec-2022

Security Systems Engineer

Nov-2020 - Jan-2021

Security Engineer, Network Operations Center

Aug-2019 - Sep-2020

NOC agent, Network Operations Center

Jul-2018 - Aug-2019

PROJECTS

TechOps Engineer

Description: In my previous roles, I have gained significant experience in using Salesforce demandware, a cloud-based e-commerce platform that enables businesses to create and manage their online stores. Additionally, I have expertise in utilizing Grafana to develop visually appealing and informative dashboards to help teams monitor and analyze system performance.

Furthermore, I have implemented an all-in-one solution using OpsGenie for managing infrastructure alerts, routing, and on-call scheduling. The solution has been in use for over a year and is the primary tool used by all teams to handle alerts and ensure seamless operations.

I have also worked with Google Cloud Platform Monitoring, specifically Stackdriver, to monitor and manage infrastructure performance and identify potential issues in real-time.



Additionally, I have used Terraform to manage Identity and Access Management (IAM) for various systems.

As part of my experience in software development, I have used Sentry to monitor and track errors in applications, as well as Prometheus and Rigor for monitoring system performance and ensuring optimal functionality.

Finally, I have extensive experience with various CI/CD toolsets, including Jenkins, Git, Docker, and Kubernetes, which I have used to automate software development processes, manage source code, and deploy software applications.

Overall, my experience with these tools and technologies has equipped me with a comprehensive understanding of software development and DevOps practices, as well as cloud computing and infrastructure management

Responsibilities:

- Design and create Graphana data visualizations (reports and dashboards) as required to support business needs
- Analyze datasets and reports to ensure data accuracy
- Performance tuning - Optimize dashboards to render faster
- Strong knowledge and work in writing SQL queries
- Experience with Tableau Server Monitoring Tool, Tableau Content Migration tool
- Track and communicate project status, issues, risks, and decisions
- Keeping knowledge base up to date(Confluence + notification channel creation to keep everyone on single page)
- I've implemented a all-in-one solution for all of the infrastructure alerts, routing and on-call scheduling - OpsGenie. Currently tool is being used for >1 year and this is a main go-to for all the teams
- In addition to my technical skills and responsibilities, I have also developed strong communication and collaboration skills throughout my work experience. I have worked closely with cross-functional teams, including developers, quality assurance engineers, and project managers, to ensure that systems are running efficiently and effectively. This has allowed me to gain a deep understanding of the importance of teamwork and effective communication in achieving project success
- During my time working with these tools and technologies, I have also developed a strong sense of problem-solving and analytical skills. I am able to quickly identify and troubleshoot issues that arise(that's my thing), and develop effective solutions to mitigate them. This has allowed me to maintain uptime and minimize system downtime, which is crucial in a fast-paced, constantly evolving tech environment
- Furthermore, I am a fast learner and am always seeking to expand my knowledge and expertise in new areas. I stay up-to-date with the latest trends and advancements in technology, and am constantly seeking out opportunities to develop my skills and knowledge base. New technology? Just let me know and I'll make it my deep dive evening routine
- Overall, my work experience has provided me with a comprehensive skillset in software development, DevOps, cloud computing, and infrastructure management. I am confident in my ability to deliver high-quality work, collaborate effectively with teams, and adapt to new technologies and environments

Technologies: Salesforce demandware, Graphana, OpsGenie, Google Cloud Platform Monitoring(Stackdriver), Terraform, Sentry, Prometheus, Rigor.

CI/CD toolset: Jenkins, Git, Docker, Kubernetes., Salesforce demandware, Graphana(made dashboard), OpsGenie(I've implemented a all-in-one solution for all of the infrastructure alerts, routing and on-call scheduling - OpsGenie. Currently tool is being used for >1 year and this is a main go-to for all the teams.) , Google Cloud Platform Monitoring(Stackdriver), Terraform(IAM management), Sentry, Prometheus, Rigor.



DevSecOps

Description: Equifax has engaged the Engineer to assist with creating a PoC for evaluating an Entitlement Master solution.

Authorization and Authentication system solution development based on OKTA OAuth. Entitlements are used for authorization purposes by applications. Solution contains APIs to perform CRUD operations in sync and async manner

Responsibilities:

- Created a working demonstration solution on GCP environment
- Authorization server configuration
- Authentication server configuration
- Authentication and Authorization token enrichment system
- Consultancy

Technologies: Okta, Google Cloud Platform, ngrok, Python(Flask)

DevOps engineer

Description: The customer is a recognized leader in the OTT TV (Over the Top TV), OVP (Online Video Platform), EdVP (Education Video Platform), and EVP (Enterprise Video Platform) markets

Responsibilities:

- Network, Infrastructure, Services monitoring
- Respond to incidents according to the incident management policy
- Finetune checks and alerts thresholds
- NOC toolset maintaining
- Service monitoring during the maintenances
- Performance reports (i.e. uptime, response times and services status)
- Production quality control (end-users service level monitoring and ability to check it after changes take place)
- Keep and update a directory of all 3rd parties (store partners contacts and keep escalation schemas up to date)
- Communication, coordination, collaboration

Technologies: MySQL, MSSQL, Couchbase., OpsGenie alerts and incidents management platform; Prometheus, Grafana, Kibana; AWS Cloudwatch for native AWS environments.

External availability monitoring using Dotcom-Monitor and Pingdom; Witbe robots for FE end-to-end scenarios monitoring; Youbora for end-user experience analytics; Logz.io as central logs and traffic aggregator .

Jira and Confluence for issue tracking and internal knowledge base., Linux and Windows servers on-premises and deployed in the cloud environments (AWS). Apache, Nginx, IIS, MySQL, MSSQL, Couchbase, Elasticsearch, Redis, Memcached, Sphinx, RabbitMQ, Celery. Components on C++, JAVA, PHP, Node.js, Python. CI/CD toolset: Jenkins, Git, Docker, Kubernetes

NOC Agent, GeeksForLess, <https://geeksforless.com>

Description:Customer: Leading provider of private label web services and business communication tools. Hosting NOC agent monitors and performs technical analysis of issues and outages as they occur across the system. Then, performs research to troubleshoot and, depending upon complexity, escalates the issue to higher-level systems administrators and service owners. The NOC agent may also perform basic system administration tasks such as network/system troubleshooting and execute various scripts.



Acting as a link in-between Technical Support and Admins, helps to address the escalated requests and prioritized issues. As the secondary task, acting as Abuse Postmaster

Responsibilities:

- Nagios alerts monitoring and handling issues using 24/7 system health monitoring via webbased tool
- Events initial triage and logging
- Incide
- Communication with service owners (Web, Mail, Windows, DB, Routing, etc)
- Secondary responsibilities– Abuse duties
- Deliverability and Outbound Blocking Issues
- Monitor & Respond to Abuse Email communications
- Ticket Response
- Abuse Escalations
- Monitor Outbound Email Abuse
- Monitor for Web Abuse
- Review Spam Complaints and Feedback
- Spam Filter Remediation
- Pre-screen new account sign ups

Technologies: Nagios, Zenoss, PagerDuty, Jira, Confluence, Corporate system for managing hosting solutions., Logging and Monitoring, Hosting

EDUCATION

Google: Associate Cloud Engineer
2020

TRAINING COURSES

Discipline: Google Cloud Platform Fundamentals: Core Infrastructure, Architecting with Google Kubernetes Engine:Foundations, Web Application Security Testing with OWASP ZAP, Managing Security in Google Cloud Platform, Penetration Testing, Incident Response and Forensics, Python for Data Science and AI, Google Cloud DevOps and SREs (GCP DevOps Engineer Track Part2), Google Professional Cloud DevOps Engineer Certification PathIntroduction (GCP DevOps Engineer Track Part 1), Google Cloud Associate Cloud Engineer

