MALCOLM GARSTIN

Automation and CyberSecurity Engineer 💻

📞 +17708992825
🔗 https://github.com/malcolm-garstin
⭐ This is not an exhaustive list of all experience.

@ malcolm@garstin.io
📍 Douglasville, GA.

EXPERIENCE

CyberSecurity Engineer II

The Home Depot

📅 01/2022 📍 Atlanta, GA

- GitHub, RHEL, Ubuntu, Windows, Podman, Ansible, Python, GCP, API integration, ServiceNow, SolarWinds
- Manage and Automate GCP Infrastructure
- Infrastructure Automation via Git, Python Ansible (AAP), Python, Bash, Podman
- Palo Alto, Cisco, Akamai, Network Infrastructure Automation via Ansible AAP and Python
- Automate and maintain SolarWinds monitoring and alerting

Cybersecurity Lab Administrator

PwC

📅 01/2018 - 01/2022 📍 Lithia Springs, GA

- Manage all Incident Response Linux and Windows servers and endpoints utilizing Simplivity/VMWare
- Automation using Git, Ansible (AAP), SaltStack, Python, Bash, VMWare CLI, Powershell, Docker, Terraform
- Scale and deploy Incident Response applications such as IDA Pro, Magnet Forensics, Log2Timeline and others.
- Maintain team assets and encrypted evidence

Senior Systems Engineer

Vertisys Corp

📅 03/2016 - 09/2017 📍 Marietta, GA

- Linux, Cisco, VMWare, Windows, SAN, Horizon View, CyberSecurity, Automate, Connectwise
- Administration of all 50+ client Linux and Windows environments utilizing VMWare Hypervisor technology
- Infrastructure, application and endpoint automation
- Cisco, Dell and HP network infrastructure management Fiber, 10gb, etc
- InfoSec - patching, remediation, and custom report generation

Senior Systems Engineer

ZeroFail Southeast

📅 03/2015 - 03/2016 📍 Alpharetta, GA

- Linux, Windows, VMWare, Switching/Routing, SAN/NAS, Labtech (Automate), Datacenter
- Management of all Linux and Windows environments utilizing VMWare Hypervisor technology
- Managing helpdesk employees and senior level escalation point
- Management of all internal and client-based networking, storage and backups
- Manage automation administration, infrastructure and customer implementation
- Administrate, design, and maintain disaster recovery and global failover technology with VMWare

Systems Engineer

Next Evolution IT

📅 06/2014 - 03/2015 📍 Marietta, GA

- Successfully managed other engineers in the field
- Manage ticketing and monitoring RMM environment
- Manage all Windows and Linux server environments for clients (IIS, SQL, File/Print and internal apps)

Systems Administrator

Georgia Softworks

📅 02/2014 - 05/2014 📍 Dawsonville, GA

Systems Engineer

Dynasis

📅 04/2013 - 02/2014 📍 Alpharetta, GA

Systems Administrator

Netcom Inc

📅 05/2012 - 04/2013 📍 Roswell, GA

SKILLS

GCP | Ansible | Nginx | Aspera

Terraform | AWS | Azure | Bash

Palo Alto | Cisco | Incident Response

Confluence | Jira | Cybersecurity | DevOps

CyberArk | Disaster Recovery

Docker and Podman | ELK Stack | VMWare

CI/CD | GitOps | SSO and Oauth | Github

Gitlab | Ansible Automation Platform | Hyper-V

RHEL | Ubuntu | Forensics | Linux

DevSecOps | Kali | Threat Mitigation

ServiceNow | ITIL | Powershell | Python

APIs | Networking | Routing | Regex

SUMMARY

👌 Expertise in security automation. Expert in increased efficiency and scalability for customers. Proactive Threat Management. Integration skills via API and Python and other automation tools.

⚙️ Reducing the need for manual intervention and enabling quicker response times, my automation skills help lower operational costs

🤔 Adaptability to New Threats. Data-Driven Decision Making. Enhancing Compliance and Reporting. Problem-Solving Mindset.

📄 All of these skills I have honed over almost 2 decades.

KEY ACHIEVEMENTS

💲 **Saved $$$**
Fully automated the Palo Alto upgrade process for Home Depot, saving the company millions of dollars in man hour costs

💎 **Saved even more $$$**
Have saved multiple companies millions of dollars automating various tasks, either server, application or integration/API based

⚙️ **Expert Installations**
Install and implement Ansible Automation Platform dozens of times over 3 companies.

👑 **CyberSec Controls**
Implemented a full CyberSecurity Incident Response and Forensics business model gaining hundreds of millions in revenue for the company.