ROMEL FERDOUS

CYBERSECURITY AND IT INFRASTRUCTURE

Security Monitoring and SIEM Integration

Alliance Building Services | Selected work experience

I support multi-client environments through security log monitoring, Wazuh integration and customization, incident investigation, firewall troubleshooting, and operational automation.

Work performed

- Integrate and customize Wazuh log collection across FortiGate, Palo Alto and SonicWall firewalls, enterprise switches, and Windows/Linux systems.
- Review security and infrastructure logs, investigate anomalies, tune alerts, and support incident response with documented findings and remediation actions.
- Troubleshoot firewall and connectivity issues, review firewall rules, and support vulnerability remediation and secure configuration baselines.
- Use PowerShell, Python and Bash for operational automation, and support workflow documentation in Simpro.

Tools and strengths

Wazuh, Splunk, centralized syslog, Palo Alto, Fortinet, SonicWall, Windows, Linux, PowerShell, Python and Bash.

Relevant opportunities

Cybersecurity engineering, security operations, SIEM administration and security infrastructure.

NYC-area hybrid or U.S.-remote work from New York

Recruiters and hiring managers: message me on LinkedIn.
linkedin.com/in/romelferdous

ROMEL FERDOUS

CYBERSECURITY AND IT INFRASTRUCTURE

Systems and Cloud Administration

PeopleNTech Institute of IT | Systems Administrator (Contract)
September 2021 - October 2023

I supported the institute's server, cloud, virtualization and remote-user environments, combining systems administration with security, troubleshooting and operational documentation.

Work performed

- Implemented Microsoft 365, Microsoft Azure, Amazon Web Services and Microsoft Intune within the institute's IT environment.
- Maintained Windows and Linux servers and virtualized lab infrastructure, and supported remote users and cybersecurity learning environments.
- Managed backup automation, patching, availability, configuration records and change-management documentation.
- Supported secure remote connectivity, diagnosed infrastructure issues, and coordinated system changes with instructors and technical teams.

Tools and strengths

Windows Server, Linux, Microsoft 365, Azure, AWS, Intune, virtualization, backup automation, patching and technical documentation.

Relevant opportunities

Systems administration, cloud infrastructure, security infrastructure and IT operations.

NYC-area hybrid or U.S.-remote work from New York

Recruiters and hiring managers: message me on LinkedIn.
linkedin.com/in/romelferdous