



Systems Administrator - Global Incidents & Response

Global L3 Ops - Windows Linux Networks

Job Information

Hiring Company

EIRE Systems K.K.

Job ID

1486888

Industry

Investment Banking

Company Type

Large Company (more than 300 employees) - International Company

Job Type

Contract

Location

Tokyo - 23 Wards, Chiyoda-ku

Train Description

Marunouchi Line Station

Salary

6 million yen ~ 9 million yen

Refreshed

July 19th, 2024 17:41

General Requirements

Minimum Experience Level

Over 1 year

Career Level

Mid Career

Minimum English Level

Fluent (Amount Used: English Only)

Minimum Japanese Level

None

Minimum Education Level

Bachelor's Degree

Visa Status

Permission to work in Japan required

Job Description

- Ⓞ Global systems operations (Windows, Linux/Unix, Networking), and automation solutions support
- Ⓞ Consultant position dedicated to a Major Global Financial Institution
- Ⓞ Location: Tokyo, Japan

EIRE Systems partners with a major financial institution in Tokyo, providing technical expertise for tier-3 systems operations and development, supporting a range of Workplace Technology systems infrastructure and applications.

Incident and Response manages detection, troubleshooting, reporting and resolution incidents that impact the global Workplace Technology environment.

As a member of this team, working on-site at a major global financial institution, you will have the opportunity to:

- Serve as the focal point for large incidents including providing awareness and debriefing to senior management
- Manage time-sensitive incidents and investigations requiring follow-the-sun coordination
- Work with and become proficient in a variety of enterprise technology from Microsoft, IBM, HP, Adobe, Google etc;
- Work with and be part of a talented global team, employing a "Follow the Sun" support model
- Collaborate with many other technical teams including networking, help-desk, desk-side support, server support, firewall, security, Unix, SQL, Web, storage and development teams.
- Provide operational oversight and ensure consistency in the tracking and remediation of incidents impacting key Business Unit stakeholders.
- Proactively participate in the continuous review of incidents and root causes, in order to highlight control gaps across the organization or process gaps within the team.
- Provide on call and out of hours support - we provide global coverage for incidents 24/7 in a follow-the-sun model - this position provides coverage during Japan weekday operating hours and will cover for escalations on one weekend every few months on a rotation basis.

**** Applicants must be available to work full-time in Japan and be we willing to commute to and work onsite at our client's offices in central Tokyo.**

Required Skills

Experience Required:

- To be best prepared for this role, you should have a background in Microsoft Windows operations or system administration, ideally in a demanding enterprise organization.
- Experience with one or more enterprise operations tools, such as Wireshark or Splunk would be a great help.
- Experience working with SAS Cloud providers like Microsoft, Google, Adobe, AWS and others.
- ITIL certification, Microsoft Certifications for Windows (Associate or Expert level)

Required Technical skills:

- Windows 2012/2016/2019/2022 server skills
- Windows Desktop (Windows 10/Windows 11)
- Active Directory skills
- PowerShell Scripting skills
- Wireshark
- Splunk
- Extrahop
- Sysinternal tools

This opportunity may be a great fit for you if you are:

- Curious, self-directed, self-motivated and highly reliable. Many of the issues we face are unique and complex and require creative thinking, perseverance, patience and a willingness to ask questions in order to arrive at a solution.
- A self-starter with good interpersonal skills to facilitate working with end-users and other IT colleagues.
- Mature enough to be able to execute job functions with minimal guidance.
- Confident to effectively host calls with senior members of the Firm, translate complex technical problems, and develop quick response plans to information security incidents.
- Very strong in verbal and written English communication; able to effectively communicate with technical / non-technical personnel including senior management.
- Comfortable taking ownership of complex situations and conscientious to see them through to resolution in timely fashion

Company Description