


# Drive Cyber Security Operations Through Data & Insights

**English Main Cyber Security Data Analyst**

## Job Information

**Recruiter**
Michael Page

**Job ID**
1623783

**Industry**
Internet, Web Services

**Job Type**
Temporary

**Location**
Tokyo - 23 Wards

**Salary**
6 million yen ~ 8 million yen

**Refreshed**
November 20th, 2026 15:05

## General Requirements

**Career Level**
Mid Career

**Minimum English Level**
Fluent Level

**Minimum Japanese Level**
Basic Level

**Minimum Education Level**
Bachelor's Degree

**Visa Status**
Permission to work in Japan required

## Job Description

Join a cybersecurity operations team where you will transform operational data into actionable insights that improve detection, response, automation, and overall security effectiveness. This role combines data analytics, business analysis, stakeholder management, and process improvement to support strategic and operational decision-making.

**Client Details**

Our client is a large-scale global technology organization operating a diverse portfolio of digital platforms and online services. Their cybersecurity function is responsible for protecting mission-critical systems and ensuring operational resilience across a complex international environment.

**Description**

Operational Performance Reporting & Analytics

- Define and maintain key operational metrics including alert volume, triage efficiency, detection and response timelines, false-positive rates, and automation impact.
- Build and enhance dashboards and reports that measure operational performance and progress against business

objectives.
- Analyze data from monitoring, ticketing, and logging systems to identify trends, bottlenecks, and recurring operational challenges.
- Monitor data quality, ingestion trends, and reporting accuracy while providing recommendations to relevant teams.
- Present actionable insights and recommendations to managers and senior stakeholders.

Business Analysis & Process Improvement

- Gather and document business and operational requirements through stakeholder interviews, workshops, and observation.
- Create functional specifications, process flows, user stories, and use cases.
- Map current and future operational processes and identify areas for optimization.
- Evaluate manual activities and develop data-backed recommendations for automation opportunities.
- Prioritize initiatives based on business value, operational impact, risk reduction, and feasibility.

Strategy, Planning & Performance Management

- Support strategic planning, roadmap development, and operational improvement initiatives.
- Develop ROI and cost-benefit analyses for technology investments, tooling, automation projects, and resource planning.
- Support workforce and capacity planning activities across multiple teams and regions.
- Track key initiatives, identify risks, and provide recommendations to maintain momentum.

Stakeholder Collaboration

- Work closely with security operations teams, engineers, platform specialists, and business stakeholders.
- Facilitate communication between technical and non-technical audiences.
- Support project planning, execution, reporting, and documentation activities.
- Contribute to operational reporting, training tracking, and strategic documentation.

**Job Offer**

- Opportunity to influence cybersecurity operations through data and strategic insights.
- Exposure to large-scale, global technology and security environments.
- Collaboration with cross-functional teams across engineering, operations, and business functions.
- International and highly collaborative work environment.
- Standard working hours: 9:00 AM - 5:30 PM.

To apply online please click the 'Apply' button below. For a confidential discussion about this role please contact Serena Wu on +81 3 6627 6137.

## Required Skills

Required Qualifications

- Bachelor's degree in Business Administration, Computer Science, Information Systems, Data Science, or a related field (or equivalent experience).
- Minimum 2 years of experience as a Business Analyst, Data Analyst, or similar role.
- Experience gathering and documenting business requirements.
- Experience with process analysis and improvement initiatives.
- Proven experience creating reports, dashboards, and analytical insights.
- Strong analytical and problem-solving abilities.
- Excellent communication skills with the ability to explain data to non-technical stakeholders.
- Proficiency with Microsoft Office tools including Excel, PowerPoint, Word, and Visio.
- Working knowledge of SQL or similar query languages.
- Familiarity with Agile, Waterfall, or related delivery methodologies.
- Business-level English communication skills.

Preferred Qualifications

- 5+ years of experience in Business Analysis or Data Analytics.
- Experience within cybersecurity, security operations, IT operations, or service management environments.
- Experience with Jira, Confluence, Tableau, or Power BI.
- Familiarity with Python, R, KQL, or similar analytical technologies.
- Knowledge of data modeling and database design.
- Understanding of security operations concepts such as incident response, alert triage, and detection processes.
- Business Analysis certifications such as CBAP or CCBA.
- Master's degree in a related discipline.

## Company Description

Our client is a large-scale global technology organization operating a diverse portfolio of digital platforms and online services. Their cybersecurity function is responsible for protecting mission-critical systems and ensuring operational resilience across a complex international environment.