SOC Analytical Lead (SIEM)
Location: Wellington SOC

InPhySec is currently looking for an experienced SIEM analyst to provide tradecraft and technical leadership with our Security Operations Centre (SOC). As part of our Managed Security Services (MSS), we are developing our SIEM services and require a SOC Analytical Lead to focus primarily on driving this work forwards. The right person will benefit from a competitive salary package.

Role & Responsibilities
The role of the SOC Analytical Lead (SIEM) is an expert-level role within the SOC, taking the lead on developing and embedding SIEM analytical tradecraft and processes. You will work to support the SOC Manager and with Shift Supervisors and analysts to deliver technical expertise across the SOC. You will be expected to work both independently and also as part of a larger team, and will primarily:

- With the data analytics team, develop and document analytical tradecraft for SIEM.
- Develop and document SOPs, processes and standards for SIEM, including security event detection, triage and investigation, and customer reporting.
- Lead internal technical engagement with other teams within InPhySec where required, developing and documenting and implementing process and procedure.
- Lead monitoring of SIEM as a security service, performing triage and investigation of security events, and providing detections in line with Service-Level Agreements (SLAs), focusing particularly on advanced technical analysis.
- Train and mentor other analysts in SIEM tradecraft, coordinating training and certification for all required SIEM technologies (particularly Elastic/Kibana).
- Peer review/QA SIEM triaging, detection notes, reports and shift write ups.
- Contribute to SOC professionalisation, specifically providing input to embed and improve SIEM analytical tradecraft in the career pathway and development programme.
- Contribute to incident response and investigation where SIEM capability is required.
- Support and collaborate on deployment onboarding/offboarding.
- Develop and document SIEM threat hunting tradecraft and train/mentor SOC analysts.
- Lead engagement with customers, handling SIEM security enquiries, providing security reports and detection advisories, and helping troubleshoot deployment/detection issues.
- Contribute to general office administration and the improvement of processes and SOPs
- Maintain an up-to-date awareness of cybersecurity trends and threats.

Skills and Experience

You must have:

- At least 5 years working in a SOC/cyber security environment, with a minimum of 3 years focusing on SIEM analysis

- Knowledge of SIEM tools/platforms/processes – experience with Elastic Security/Kibana would be a particular advantage
- Experience monitoring client infrastructure and traffic, identifying incidents and vulnerabilities, performing analysis and investigation, determining severity, reporting security events and determining required response and remediation.
- Experience identifying incidents and subsequent analysis and investigation to determine severity and response required.
- Expert-level technical troubleshooting and analytical skills
- Excellent written and oral communication skills
- Familiarity with development and application of IT policies, SOPs and standards
- Mentoring/training experience, with a proven track record of working with other staff to help develop them and their technical skills and expertise
- Ability to digest complex security information and generate relevant reports/views of that information to stakeholders, both technical and non-technical.
- Ability to work independently and lead the work of others

Desirable skills and experience:

- Bachelor's degree in a technical discipline (e.g. CompSci/Engineering/…)
- Formal IT security qualifications (e.g. CompTIA Security+, CISSP, CEH, CSTA, etc)
- Experience in a senior SIEM focused role

Hours

The expected hours for this role fall within regular business hours (08:00-17:00). InPhySec maintains an incident response capacity, as such there may be an occasional requirement to work on an on-call basis or provide some out of hours support and at short notice.

Security Vetting

All successful applicants will be required to pass and maintain security vetting. There may be a requirement to also undergo security clearance.

How to apply

To apply for this position please email your CV with a cover letter to careers@inphysec.co.nz