Senior Cloud Security Engineer

Job Description

At Lanware, we aim to be the leading technology service provider to the financial world. We enable our customers to drive their businesses by being a trusted technology partner. We place service before sales. We're flexible without compromising standards. We're highly selective in our people, the technology used, the industry and our customers. Lanware security professionals help us be the market leader by providing a robust, secure service, meeting the high standards our customers expect in the heavily regulated world in which they operate.

If you're looking to join Lanware as a Senior Cloud Security Engineer, you will have a strong focus on security, having worked in a similar position for a minimum of four years. You will be a self-starter with the ability to own problems through to completion and provide timely, professional feedback to customers or other teams as needed. This role requires someone with a strong infrastructure background and experience in the core technologies in use at Lanware along with the Public Cloud (Microsoft Azure) which is rapidly being adopted by the Lanware client base, and driving change in Lanware's security approach.

Being an effective senior security engineer means not only keeping up to date with the current threat landscape but actively staying at the cutting edge through training and self-study. As such, you should possess or be working towards accreditations such as AZ-500, CEH, CCNA: Security, CCNA: CyberOps or SSCP.

As a member of the Cloud Infrastructure Team you will be involved in technical decisions at a senior level within Lanware and will be relied upon to work with our financial sector customers, inspiring confidence in the solutions you implement. You will be based at our headquarters in Central London unless working from home or at client site.

Key responsibilities

- Providing input to the management of security across Lanware and our customers;
- Dealing with the output from a variety of security products, remediating events and incidents;
- Ownership of major vulnerabilities, coordinating with other teams for emergency patching;
- Ownership of all 'cyber' incidents;
- Providing information into clients and client relationship managers around security media coverage or in response to events and incidents;
- Undertaking security related project work;
- Liaising with 3rd parties and arranging vulnerability assessments / penetration tests;
- Running a variety of security tests for customers (e.g. Phishing);
- Assisting in the development of security tools and security related automation;
- Generating and delivering security reports to customers;
- Managing and generating security documentation including the creation / maintenance of internal standards;
- Attending industry events / maintaining professional qualifications;
- Undertaking out of hours work and forming part of the security 'on-call' rotation;
- Supporting the presales and account management as needed;
- Providing consultancy on client security posture and strategy;
- Ensuring compliance with Lanware policies and procedures relating to information security management;
- Reporting any observed or suspected security weaknesses in the systems or services that Lanware provides;
- Ensuring all security products and SIEM are operating effectively and reliably;
- Supporting the developing of Lanware's cyber security service strategy and capabilities;
- Being part of the Information Security Management Committee and helping maintain ISO 27001;
- Researching new security technologies to support the ongoing development of Lanware products and services.

Ideal candidate profile

- Builds strong relationships with customers, key contacts and suppliers;
- Embraces a culture of best practice, process, compliance and continuous improvement;
- Possesses commercial awareness and knowledge of the wider managed service marketplace;
- Demonstrates flexibility and a committed work ethic with a drive to go beyond the status quo;
- Holds a proven track record of success in contributing to a team-oriented environment – collaborating across disciplines;
- Understands service support and delivery in an ITIL based environment;
- Has recent experience of working in a security focused role;
- Has 4 years industry experience in an infrastructure engineering capacity.

Skill Requirements

Essential

- Awareness of Data Centres and communications rooms;
- Awareness of administering with Linux OS;
- Experience with administering Microsoft products including Windows Server, AD, Exchange;
- Experience with administering Microsoft Azure Cloud services (Security, Networks & Infrastructure) & Office 365 Stack (Exchange Online, SharePoint, Teams);
- Experience with current Cyber threats analysis and risk management (CVE, CVSS);
- Experience with current Cyber defences;
- Experience with Firewalls, in particular Cisco;
- Experience with Cloud Identity Access Management (Azure, GCP, Duo);
- Experience with Cryptographic mechanisms (Encryption, PKI, SSL/TLS);
- Experience and adherence to Cybersecurity Frameworks and Compliance Plans (CIS, NCSC & NIST);
- Experience with common scripting languages (Python / PowerShell / HTML / JSON);
- Extensive experience with Antivirus products (ATP / Trend Micro / Sophos);
- Extensive experience with Security Information and Event Management (SIEM) Tools;
- Extensive experience with managing cyber incidents within a SOC;
- Extensive experience with IPS/IDS.

Desirable

Experience working with the following technologies:

- SIEM Tools such as Azure Sentinel or Splunk;
- Cisco Umbrella / Mimecast W1 Web Security;
- Darktrace / Cylance;
- Vulnerability Scanners (Nessus);
- Symantec.Cloud (MessageLabs) / Mimecast;
- Cisco AMP;
- Wireshark / Network Packet Inspection;
- Awareness of network security architecture concepts, including topology, protocols, components, and principles (e.g., application of defence-in-depth);
- VPN Technologies;
- Citrix XenDesktop / XenApp;
- SQL;
- Microsoft Configuration Manager / Microsoft Endpoint Manager.

Qualifications

Essential

- ITIL Foundation;
- CCNA: Security;
- Microsoft Azure Security Technologies (AZ-500);
- Systems Security Certified Practitioner (SSCP).

Desirable

- Microsoft Azure Architect Design (AZ-304);
- CCNA: Cyber Ops;
- Certified Ethical Hacker Certification (CEH);
- GIAC Security Essentials Certification (GSEC).

Role Split

- Security operations 50%
- Security projects 30%
- Security consultancy 20%

Additional information

- All candidates must be willing to work in London;
- This role may necessitate some varied working hours to accommodate project work;
- The role may involve the manual handling of company/client equipment from time to time.