Security Team – Senior 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 security focused Senior Engineer, you will have a strong focus on security, having worked in a similar position for a minimal of 12 months. This is a new, dynamic team which requires 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 looking to specialise in security.

Being an effective 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 CEH, Security+, CCNA: Security, CCNA: CyberOps or SSCP.

As a member of the Technical Management & Consultancy 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.

Key responsibilities include

- Providing input to management of security across Lanware and our customers.
- Dealing with the output from a variety of security products, remediating events and incidents.
- Owner of major vulnerabilities, coordinating with other teams for emergency patching.
- Ownership of all 'cyber' incidents
- Providing information into Business Relationship Managers around security media coverage or in response to events and incidents.
- 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 form part of the security 'on-call' rotation.
- Support the presales process as needed.
- 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 provide.

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.
- Demonstrable flexibility and 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 5 years industry experience in an infrastructure engineering capacity.

Skill Requirements

Essential

- Detailed understanding of current Cyber threats.
- Detailed understanding of current Cyber defences.
- Understanding of Firewalls, in particular Cisco.
- Comfortable administering Microsoft Systems including Windows Server, AD & Exchange.
- Understanding of network infrastructure.
- Familiarity with data centres and communications rooms.
- Experience managing cyber incidents.
- Experience working with IPS/IDS.
- Proficient in common scripting languages (Python / PowerShell).
- Basic experience with HTML.
- Experience with Linux.

Desirable

Experience working with the following technologies:

- SIEM Tools;
- Cisco Umbrella / Cloud Web Security;
- Darktrace / Cylance;
- SQL;
- Symantec.Cloud (MessageLabs) / Mimecast;
- Trend Micro;
- Cisco AMP;
- Wireshark / Network Packet Inspection;
- Microsoft SCCM;
- PKI;
- VPN Technologies;
- Citrix XenDesktop / XenApp.

Qualifications

Essential

- CCNA: Security;
- Security+.

Desirable

- ITIL Foundation;
- MCSE;
- CCNA: Cyber Ops;
- CCNP: Security
- CCNA;
- CEH;
- CISSP / SSCP.

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.