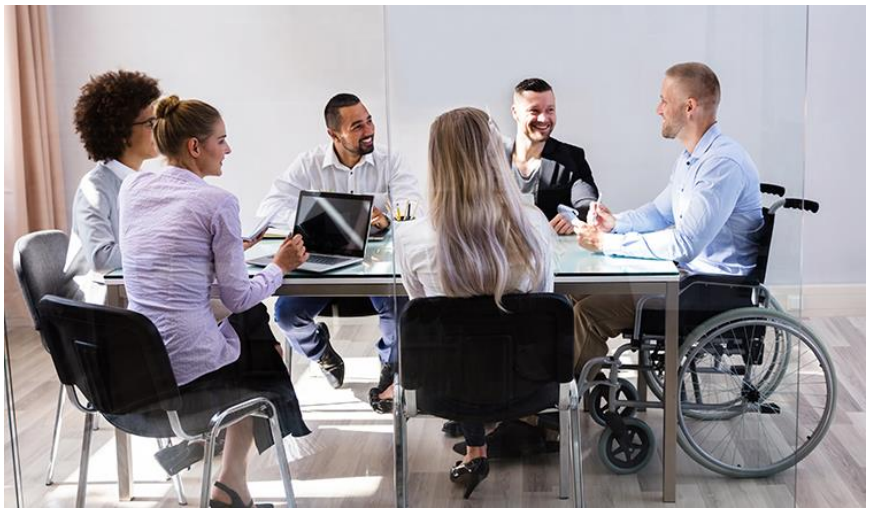
UNIVERSITY of BRADFORD

Vulnerability Remediation Analyst
in IT Services
Directorate of Infrastructure



UNIVERSITY of BRADFORD

Brief summary of the role

Role title:	Vulnerability Remediation Analyst
Grade:	6
Vacancy reference:	
Faculty or Directorate:	Infrastructure
Service or Department:	IT Services
Location:	On campus, Hybrid or Remote to suit candidate
Reports to:	Vulnerability Remediation Team Leader
Responsible for:	Vulnerability Remediation Analysts
Work pattern:	36.25 hours per week, Monday to Friday (core hours)
Specific notable requirements for the role:	Ability to work outside core hours at weekend or in the evenings on a planned basis to ensure patches are applied correctly out of hours on critical systems
Possible adjustments:	We are open to any request for adjustments to support your needs around working hours flexibility, training, and mentoring, which would enable you to succeed in this role

UNIVERSITY of BRADFORD

Main purpose of the role

The Vulnerability Remediation Analyst in the Infrastructure Platform Services Team delivers vulnerability remediation for customer facing and backend technology. Providing support and administration to implement, maintain and administer patching and remediation on our infrastructure and desktop platforms to support our business processes. This is a critical role to protect the security of our IT systems.

Main duties and responsibilities

Note: The list below may vary to include other reasonable requests (as directed by University management) which do not change the general character of the job or the level of responsibility entailed.

1. Responsible for ensuing that patches are applied to the University's IT systems in a timely manner and escalating to IT Management where this is not occurring.
2. Following security policies, standards and procedures relating to patching and remediation
3. Following processes and activities for OS, application and other software patching and remediation.
4. Work with IT Security, Customer Services, Application Development and Support and Infrastructure teams on a daily basis regarding scheduling of patches and software updates.
5. Monitor the implementation of patches.
6. Compile patching data and success rates to present to the Vulnerability and Remediation Team Leader in the form of weekly/monthly reports and dashboards.
7. Complete technical remediation tasks related to patching as dictated by the Vulnerability and Remediation Team Leader.
8. Use Software Tools to implement patches to a variety of systems using own initiative to solve technical issues which arise when implementing patches.
9. Create reports and dashboards on patching success which will be shared with the IT Senior Leadership Team.
10. Provide advice on the application of patches liaising with software vendors as to approach.

11. Adhere to the departments software patching processes, being aware of the correct patch versions of systems being deployed for all IT software.

12. Speak to suppliers about patch levels and how these can be better deployed making subsequent recommendations to IT Management.

UNIVERSITY of BRADFORD

Role holder: essential and desirable attributes

Qualifications

Essential	• Level 3 qualification in an IT discipline or equivalent work experience
Desirable	• Patch Management Tool Certifications

Experience, skills, and knowledge

Essential	• Experience working with an Incident Management System (such as IPcenter, BMC Remedy, or Service Now). • Manage Windows patch content utilizing WSUS • The ability to communicate both technical and non-technical material to staff and management at all levels of an organization. • Basic System Administration experience in a large environment • Working knowledge of MS Office products (Word, Excel, Access, PowerPoint, Visio, SharePoint) • Basic understanding of core Infrastructure Platforms (Wintel, Linux, VMWare, AiX)

Commented [RH1]: WSUS is not used for the majority of patching. We have moved onto Manage Engine Desktop Central

Desirable	• Basic understanding of UNIX systems. (RedHat 5,6,7) • Basic understanding of Windows systems. (2008/R2, 2012/R2, 2016) • Experience of Patching Automation tools • Experience using Manage Engine patching tools • Working knowledge of at least one scripting language (powershell, perl, python, bash, etc)

Commented [DW2]: Unix/Linux (e.g. Solaris; RedHat/CentOS; Ubuntu; SUSE etc.)

Commented [DW3]: (e.g. Windows client OSs Windows 10/11; Windows Server OSs 2008 and above).

Personal attributes

Essential	• Strong verbal and written communication skills
Desirable	• Insert a list of the desirable personal attributes of the role holder

UNIVERSITY of BRADFORD

Information about the University of Bradford

Values

We will be an organisation that embodies our values in everything we do. These values are:

- **Excellence** is at the heart of everything we do.
- **Trust** is the foundation of our relationships, underpinned by integrity in everything we do.
- We give invention light and celebrate creativity and **innovation**.
- **Inclusion** - diversity is a source of strength and must be understood, valued, supported, and leveraged.

Embedding these values across the University will shape our culture and drive our performance.

It is the responsibility of every employee to uphold the University values.

Equality, Diversity, and Inclusion (EDI)

The University of Bradford is widely recognised as an Equality, Diversity, and Inclusion (EDI) leading institution.

Our EDI vision is to bring about, and be recognised as an exemplar of transformational diversity, inclusion, and social mobility and emphasise the critical role of leadership in embedding intersectional EDI in order to make our diversity count and deliver impact.

It is the responsibility of every employee to act in ways that support equality, diversity, and inclusivity and to work within the spirit and detail of the law, including the Equality Act 2010 and the Human Rights Act 1998.

The University provides a range of services and employment opportunities for a diverse population. Employees will treat all students and colleagues with dignity and respect irrespective of their background.

Employees are responsible for ensuring the University develops a culture that promotes equality, values diversity, and supports inclusivity. This responsibility includes services and functions the University provides and commissions, to students, colleagues, partners in other organisations, visitors, and members of the public.

Training

Employees must complete any training that is identified as mandatory to their role. Training should be accessed locally by agreement with line managers and through the University's People and Organisational Development Service.

Mandatory training must be completed on commencement of the role, without delay.

Health, safety, and wellbeing

Health and Safety is a partnership between employee and employer each having responsibilities, as such all employees of the University have a statutory duty of care for their own personal safety and that of others who may be affected by their acts or omissions. It is also the responsibility of all employees, that they fulfil a proactive role towards the management of risk in all of their actions. This entails the risk assessment of all situations, the taking of appropriate actions and reporting of all incidents, near misses and hazards.

All employees have a duty to report any practice that you consider compromises standards of health and safety and risk. The Code of Practice on Public Interest Disclosure (Whistleblowing) details the process and advises on the protection from unfair treatment for an individual who raises such concerns.

Employees are required to co-operate with management to enable the University to meet its own legal duties and to report any circumstances that may compromise the health, safety and welfare of those affected by the University's undertakings.

Managers should note they have a duty of care towards any staff they manage; academic staff also have a duty of care towards students. As part of this you will need to ensure you are familiar with any relevant Health and Safety policies and procedures; seeking advice from the Central University Health and Safety team as appropriate.

Information governance

Employees have a responsibility for the information and records (including student, health, financial and administrative records) that are gathered or used as part of their work undertaken for the University. This may be in paper, electronic, or other formats.

An employee must consult their manager if they have any doubts about the appropriate handling of the information and records with which they work.

This means that employees are required to uphold the confidentiality of all data, information and records and to ensure they are recorded to appropriate data standards and

to the relevant electronic system or manual filing system in order to maintain their accessibility and integrity.

To support these requirements all employees must adhere to data protection legislation and the University's policies and procedures in relation to information governance and information security at all times.

Additionally, employees will be required, when and where appropriate to the role, to comply with the processing of requests under the Freedom of Information Act 2000.

All employees will be given the necessary training to enable them to adhere to these requirements.

Criminal record disclosures and working with vulnerable groups

Depending on the defined nature of your work and specialist area of expertise, your role may be exempt from the provisions normally afforded to individuals under the Rehabilitation of Offenders Act 1974. In these circumstances, the University may obtain a standard or enhanced disclosure through the Disclosure and Barring Service (DBS) under the Rehabilitation of Offenders Act 1974 (Exceptions) Order 1975 (as amended) and, in certain circumstances, the Police Act 1997.

Suitable applicants will not be refused positions because of criminal record information or other information declared, where it has no bearing on the role (for which you are applying) and no risks have been identified against the duties you would be expected to perform as part of that role.

During the course of your employment, you must notify your line manager if you are charged with a criminal offence (excluding motoring fixed-penalty convictions). Failure to notify the University of a criminal conviction could lead to withdrawal of a job offer where employment has not commenced, or disciplinary action for employees in post. All employees of the University who have contact with children, vulnerable adults, service users and their families must familiarise themselves, be aware of their responsibilities and adhere to the University's policy and policies and the Safeguarding Vulnerable Groups Act 2006. Where appropriate, employees will be given the necessary training to enable them to adhere to these requirements.

University policies and procedures

The University operates a range of policies, procedures and formal guidance (available on the University intranet and ServiceNow). All employees must observe and adhere to the provisions outlined in these documents.