Data exfiltration attacks: security checklist

□ **Identity protection**

- □ Implement multi-factor authentication (MFA) across all systems
- □ Regularly review and limit user permissions, especially for contractors and external partners
- □ Monitor user behaviour and correlate with data movements (e.g. accessing data at unusual times)
- □ Use identity management tools to track endpoint, network, and application access

□ **Monitoring and detection**

- □ Deploy a Security Information and Event Management (SIEM) system to correlate log sources (e.g. endpoints, mobile devices, cloud services)
- □ Establish normal user and network behaviour patterns for baseline monitoring
- □ Set up alerts for unusual data transfers, login times, or access to sensitive files
- □ Regularly audit network traffic for unexpected spikes or anomalies

□ **Endpoint and device security**

- □ Monitor endpoints for unauthorised device connections and access attempts
- □ Implement encryption for sensitive data stored on endpoints
- □ Secure all mobile and remote devices with strong passwords, encryption, and remote wipe capabilities
- □ Limit the use of external storage devices (e.g. USBs) or block them entirely

□ **Cloud services and third-party application management**

- □ Regularly review cloud services and application permissions, revoking those that are unnecessary or excessive
- □ Ensure that third-party API permissions are tightly controlled
- □ Monitor for unauthorised uploads to external file-sharing platforms (e.g. Google Drive, Dropbox)
- □ Ensure all third-party applications are authorised and verified

Data exfiltration attacks: security checklist

□ **Incident response and planning**

- □ Develop and regularly test an Incident Response Plan
- □ Ensure the ability to identify what data has been exfiltrated and which customers are affected within 24 hours of an incident
- □ Prepare for slow exfiltration attempts by monitoring long-term data movements
- □ Conduct regular drills to ensure the team is ready for rapid response

□ **Phishing and social engineering defence**

- □ Train employees to recognise phishing attacks and social engineering tactics
- □ Regularly conduct phishing simulations and refresher courses on cybersecurity best practices
- □ Implement email filtering systems to block phishing emails and malicious attachments
- □ Ensure compromised credentials are immediately revoked and reset

□ **Data classification and access control**

- □ Classify sensitive data and limit access to those who need it
- □ Monitor access to sensitive data, ensuring it aligns with the user’s role
- □ Set up alerts for any attempts to access data outside of normal business hours or from unusual locations
- □ Regularly review who has access to critical data and adjust permissions as needed

□ **Addressing insider threats**

- □ Monitor user activity for suspicious behaviour, such as accessing data they don’t typically work with
- □ Implement policies to detect and investigate unauthorised data movements or leaks
- □ Provide regular training for employees on the risks of insider threats
- □ Limit access to data during staff changes or periods of high turnover, especially in complex supply chains