DigitalXRAID
CYBER SECURITY EXPERTS

How Microsoft Security products address key DCC controls

DCC Control Area (Def Stan 05-138)	Relevant Microsoft Security Product
Identity & Access Management – Enforcing MFA, privileged access controls and role-based access	Microsoft Entra ID (Azure AD), Microsoft Entra ID Protection
Endpoint Protection – Malware protection, secure device configuration and patch management	Microsoft Defender for Endpoint, Microsoft Intune
Threat Detection & Security Monitoring – Monitoring network behaviour, reviewing security event logs and detecting anomalies	Microsoft Sentinel (SIEM), Microsoft Defender XDR
Incident Response – Detecting, responding to and recovering from cyber security incidents	Microsoft Sentinel (SOAR/automated playbooks), Microsoft Defender XDR
Vulnerability Management – Identifying and remediating vulnerabilities across systems and devices	Microsoft Defender Vulnerability Management
Data Protection & Information Controls – Controlling the flow, classification and protection of sensitive defence information	Microsoft Purview (Information Protection & DLP)
Email & Collaboration Security – Protecting against phishing, malicious attachments and social engineering	Microsoft Defender for Office 365
Remote Access & Network Controls – Controlling and monitoring remote access to systems	Microsoft Entra Conditional Access, Microsoft Intune
Audit Logging & Evidence – Maintaining audit trails and producing evidence of security controls in operation	Microsoft Sentinel, Microsoft Purview Audit