THREAT CATALOGUE 1/5

Scan the QR code to find a step-by-step guide for this tool, digital business development cases and further inspiration at dbd.au.dk

ID	THREAT NAME	CATEGORY	DESCRIPTION	STRIDE	CIA
T01	Physical Tampering	Device Hardware	Attempts to physically manipulate or damage the device.	Tampering	Integrity, Availability
T02	Eavesdropping	Communication Protocol	Intercepting communications between the device and the network.	Information Disclosure	Confidentiality
T03	Man-in-the-Middle Attacks	Network Infrastructure	Intercepting and altering communications between two parties without their knowledge.	Tampering, Information Disclosure	Confidentiality, Integrity
T04	Brute Force Attacks	Application	Repeatedly trying different credentials until the correct ones are found.	Elevation of Privilege	Confidentiality
T05	Phishing	Application	Deceptive tactics to trick users into revealing sensitive information.	Spoofing, Information Disclosure	Confidentiality
T06	Denial of Service	Device Hardware	Overwhelming the device or network to render it non-functional.	Denial of Service	Availability
T07	SQL Injection	Cloud-based System	Inserting malicious SQL statements into input fields to run against a database.	Elevation of Privilege	Integrity
T08	Firmware Manipulation	Device Hardware	Tampering with device firmware, potentially introducing malicious functionalities.	Tampering	Integrity, Availability
T09	Cloud Misconfiguration	Cloud-based System	Improperly configured cloud services that could expose sensitive data.	Information Disclosure	Confidentiality
T10	Weak or Stolen Credentials	Application	Utilizing weak passwords or stolen login information.	Spoofing	Confidentiality
T11	Expired Certificates	Communication Protocol	Using outdated certificates, undermining system security.	Spoofing, Information Disclosure	Confidentiality, Integrity
T12	Network Sniffing	Network Infrastructure	Passive interception of information being transmitted over the network.	Information Disclosure	Confidentiality

THREAT CATALOGUE 2/5

Scan the QR code to find a step-by-step guide for this tool, digital business development cases and further inspiration at dbd.au.dk

ID	THREAT NAME	CATEGORY	DESCRIPTION	STRIDE	CIA
T13	Malware Infection	Application	Introduction of malicious software into the application or system.	Tampering, Elevation of Privilege	Integrity, Availability
T14	Unauthorized Access	General System	Gaining access to parts of the system without proper permissions.	Elevation of Privilege	Confidentiality, Integrity
T15	Insecure Interfaces	Cloud-based System	Poorly designed and secured application interfaces that can be exploited.	Elevation of Privilege, Information Disclosure	Confidentiality, Integrity
T16	Brute Force Attacks	Communication Protocol	Gaining information from the system based on information leaks from physical implementations.	Information Disclosure	Confidentiality, Integrity
T17	Insecure Default Configurations	Device Hardware	Default settings that are easily exploitable if not changed by the user.	Elevation of Privilege, Tampering	Confidentiality, Integrity, Availability
T18	Rogue Gateway Devices	Gateway	Unauthorized gateway devices introduced to capture or manipulate data.	Spoofing, Tampering	Confidentiality, Integrity
T19	Application Layer Attacks	Application	Targeting application-level processes and services.	Elevation of Privilege, Information Disclosure	Confidentiality, Integrity
T20	Inadequate Logging & Monitoring	Cloud-based System	Insufficient tracking or auditing, allowing malicious activities to go unnoticed.	Repudiation	Integrity, Availability
T21	Remote Code Execution	Cloud-based System	Exploiting vulnerabilities to run arbitrary malicious code.	Elevation of Privilege	Integrity, Availability
T22	Data Exposure	Cloud-based System	Unintentional exposure of data due to software flaws or misconfigurations.	Information Disclosure	Confidentiality
T23	Insufficient Encryption	Communication Protocol	Data being transmitted without adequate encryption or using weak encryption standards.	Information Disclosure	Confidentiality

THREAT CATALOGUE 3/5

Scan the QR code to find a step-by-step guide for this tool, digital business development cases and further inspiration at dbd.au.dk

ID	THREAT NAME	CATEGORY	DESCRIPTION	STRIDE	CIA
T24	Supply Chain Attacks	General System	Targeting less secure elements in the supply chain to compromise security of the main system.	Spoofing, Tampering	Integrity, Availability
T25	Hardware Malfunctions	Device Hardware	Failures or malfunctions of physical components of the device.	Tampering, Denial of Service	Availability
T26	Session Hijacking	Application	Stealing or predicting session tokens to impersonate users.	Spoofing, Information Disclosure	Confidentiality, Integrity
T27	Social Engineering	General System	Manipulating individuals into revealing confidential information or performing specific actions.	Spoofing, Repudiation	Confidentiality, Integrity
T28	Cross-site Scripting (XSS)	Cloud-based System	Injecting malicious scripts into web pages viewed by other users.	Tampering, Information Disclosure	Confidentiality, Integrity
T29	Insecure Data Storage	Application	Storing sensitive data without proper security measures on mobile devices.	Information Disclosure	Confidentiality
T30	Cross-Site Request Forgery (CSRF)	Cloud-based System	Tricking users into perform-ing actions without their knowledge or consent.	Spoofing, Tampering	Confidentiality, Integrity
T31	Unsecured APIs	Cloud-based System	APIs exposed without necessary security measures, allowing unauthorized access or actions.	Elevation of Privilege, Information Disclosure	Confidentiality, Integrity
T32	Credential Stuffing	Application	Using breached username/ password pairs to gain unauthorized access.	Spoofing, Elevation of Privilege	Confidentiality
T33	Insufficient Network Segmentation	Network Infrastructure	Lacking separation between different parts of the network, allowing lateral movement.	Elevation of Privilege	Confidentiality, Integrity, Availability

THREAT CATALOGUE 4/5

Scan the QR code to find a step-by-step guide for this tool, digital business development cases and further inspiration at dbd.au.dk

ID	THREAT NAME	CATEGORY	DESCRIPTION	STRIDE	CIA
T34	Zero-Day Exploits	General System	Exploiting vulnerabilities that are unknown to the vendor or unpatched.	Tampering, Elevation of Privilege	Confidentiality, Integrity, Availability
T35	Insecure Network Configuration	General System	Poorly configured networks can expose the system to a myriad of attacks.	Elevation of Privilege, Information Disclosure	Confidentiality, Integrity, Availability
T36	API Key Exposure	Cloud-based System	Unprotected API keys that can be accessed and misused to interact with cloud services.	Information Disclosure	Confidentiality
T37	Firmware Downgrade Attacks	Device Hardware	Attackers forcibly downgrade firmware to a vulnerable version.	Tampering	Integrity, Availability
T38	Reverse Engineering	General System	Decompiling software to understand its inner workings and potentially exploit it.	Information Disclosure	Confidentiality, Integrity
T39	Weak Cryptographic Algorithms	Communication Protocol	Use of outdated or weak cryptographic standards that can be exploited.	Information Disclosure	Confidentiality
T40	Misconfigured Firewall	Network Infrastructure	Poorly configured firewalls that expose the system to various network threats.	Elevation of Privilege	Confidentiality, Integrity, Availability
T41	IoT Device Shadowing	Device Hardware	Unauthorized devices mimicking legitimate ones to intercept or inject data.	Spoofing	Confidentiality, Integrity
T42	Data Integrity Attacks	Cloud-based System	Manipulating data without the user's knowledge leading to misinformation or malfunctions.	Tampering	Integrity
T43	Privilege Escalation	Application	Gaining higher access rights illicitly, allowing more system control.	Elevation of Privilege	Confidentiality, Integrity, Availability
T44	Backup Data Exposure	Cloud-based System	Unsecured backups being accessed or leaked.	Information Disclosure	Confidentiality

THREAT CATALOGUE 5/5

Scan the QR code to find a step-by-step guide for this tool, digital business development cases and further inspiration at dbd.au.dk

ID	THREAT NAME	CATEGORY	DESCRIPTION	STRIDE	CIA
T45	Insufficient Patch Management	General System	Failure to update and patch system components regularly, leading to vulnerabilities.	Elevation of Privilege	Integrity, Availability
T46	URL Redirection Attacks	Application	Redirecting users to malicious websites through the app, potentially harvesting data or deploying malware.	Spoofing, Information Disclosure	Confidentiality, Integrity
T47	Cloud Vendor Vulnerabilities	Cloud-based System	Threats posed due to vulnerabilities in third-party cloud service providers.	Elevation of Privilege	Confidentiality, Integrity, Availability
T48	Signal Jamming	Communication Protocol	Disrupting the communication signals to prevent the device from functioning.	Denial of Service	Availability
T49	Cloud Data Breaches	Cloud-based System	Unauthorized access to cloud-stored data due to various vulnerabilities.	Information Disclosure	Confidentiality
T50	Insecure Endpoints	Network Infrastructure	Weakly protected network entry and exit points which can be exploited.	Elevation of Privilege	Confidentiality, Integrity, Availability