Policy document-

Cyber bullying Policy

A screenshot of a cell phone

Description automatically generated

A screenshot of a cell phone

Description automatically generated

Indicators of Compromise

A screenshot of a cell phone

Description automatically generated

|  |  |
| --- | --- |
| 1. | Database Dumps/Backup Files: MySQL-Format Database Dump |
|  | |  |  |  |  | | --- | --- | --- | --- | | 1.1 | |  | | --- | | Database Dumps/Backup Files: MySQL-Format Database Dump (Wide) (1675823) - Disabled | | Detection of textual MySQL-format database dumps using lenient heuristics. For example: CREATE TABLE `users` (`username` varchar(16) NOT NULL,`password` varchar(16) NOT NULL, PRIMARY KEY (`id`) ); INSERT INTO `users` VALUES ('John','QWERTY12'),('Jane','QWERTY13');. | | | 1.2 | |  | | --- | | Database Dumps/Backup Files: MySQL-Format Database Dump (Default) (1675823) | | Detection of textual MySQL-format database dumps using strict heuristics. For example: CREATE TABLE `users` (`username` varchar(16) NOT NULL,`password` varchar(16) NOT NULL, PRIMARY KEY (`id`) ); INSERT INTO `users` VALUES ('John','QWERTY12'),('Jane','QWERTY13');. | | |
| 2. | |  | | --- | | Database Dumps/Backup Files: Microsoft Tape Format (1675823) | | Detection of Microsoft Tape Format (MTF) backup files used by the backup utilities included in Microsoft SQL Server, and by other Microsoft Windows software, such as NTBackup and Backup Exec. | |

|  |  |
| --- | --- |
| 1. | Encrypted Files: Archive |
|  | |  |  |  |  | | --- | --- | --- | --- | | 1.1 | |  | | --- | | Encrypted Files: B1 File (1675823) | | Detects password-protected B1 archives. | | | 1.2 | |  | | --- | | Encrypted Files: RAR File (1675823) | | Detects password-protected RAR archives. | | | 1.3 | |  | | --- | | Encrypted Files: RAR5 File (1675823) | | Detects password-protected RAR5 archives. | | | 1.4 | |  | | --- | | Encrypted Files: ZIP File (1675823) | | Detects password-protected ZIP archives. | | |
| 2. | Encrypted Files: Microsoft Office File |
|  | |  |  |  |  | | --- | --- | --- | --- | | 2.1 | |  | | --- | | Encrypted Files: Microsoft Access Database File (Legacy) (1675823) | | Detects password-protected Microsoft Access Database files (.mdb) that were created before Office 2007 according to internal file properties. | | | 2.2 | |  | | --- | | Encrypted Files: Microsoft Excel Binary File (Legacy) (1675823) | | Detects password-protected Microsoft Excel Binary files (.xls) that were created before Office 2007 according to internal file properties. | | | 2.3 | |  | | --- | | Encrypted Files: Microsoft Office Encrypted File (OOXML) (1675823) | | Detects password-protected Office Open XML files according to internal file properties. Open XML files include Word, Excel, PowerPoint and other Office documents created in Office 2007 or later. | | | 2.4 | |  | | --- | | Encrypted Files: Microsoft OneNote Encrypted File (1675823) | | Detects password-protected Office OneNote files (.one) according to internal file properties. | | | 2.5 | |  | | --- | | Encrypted Files: Microsoft PowerPoint Binary File (Legacy) (1675823) | | Detects password-protected Microsoft PowerPoint Binary files (.ppt) that were created before Office 2007 according to internal file properties. | | | 2.6 | |  | | --- | | Encrypted Files: Microsoft Word Binary File (Legacy) (1675823) | | Detects password-protected Microsoft Word Binary files (.doc) that were created before Office 2007 according to internal file properties. | | |
| 3. | |  | | --- | | Encrypted Files: PDF File (1675823) | | Detects encrypted PDF (note: will detect PDFs that are encrypted, although they may still be visible). | |
| 4. | Encrypted Files: PGP File |
|  | |  |  |  |  | | --- | --- | --- | --- | | 4.1 | |  | | --- | | Encrypted Files: PGP Encrypted File (1675823) | | Detects PGP encrypted data. | | | 4.2 | |  | | --- | | Encrypted Files: PGP Signed and Encrypted File (1675823) | | Detects PGP signed and encrypted data. | | |
| 5. | |  | | --- | | Encrypted Files: Unknown Encrypted Format (1675823) | | Detects encrypted files of unknown format. | |

Employee Discontent

A screenshot of a cell phone

Description automatically generated

|  |  |  |  |
| --- | --- | --- | --- |
| 1. | |  | | --- | | CV and Resume in English (1675823) | | Detection of resumes and CVs in English, using location-sensitive lexical analysis of terms and patterns common in such documents. | |

|  |  |
| --- | --- |
| 1. | Disgruntled Employee |
|  | |  |  |  |  | | --- | --- | --- | --- | | 1.1 | |  | | --- | | Disgruntled Employee (Default) (1675823) | | Detects expressions that are indicative of disgruntled employees. Only one expression is needed to trigger this rule. By default this rule is applied only to web channels. You can add more channels on the Destination page when editing or creating a new policy. | | | 1.2 | |  | | --- | | Disgruntled Employee (Narrow) (1675823) - Disabled | | Detects expressions that are indicative of disgruntled employees. Two or more expressions are needed to trigger this rule. By default this rule is applied only to web channels. You can add more channels on the Destination page when editing or creating a new policy. | | |

|  |  |
| --- | --- |
| 1. | Self CV/Resume Distribution: English |
|  | |  |  |  |  | | --- | --- | --- | --- | | 1.1 | |  | | --- | | Self CV/Resume Distribution: English (Wide) (1675823) - Disabled | | Rule for detecting distribution of a person's own CV or resume by first identifying a document as a CV or resume, then comparing the employee's user name to the document owner's name and email address, as extracted from the opening section of the document. In this rule, the comparison of the email address to user name has relatively liberal criteria. For example, a CV document that contains the line "Email: jsmith123@gmail.com", that is sent from address johnsmith@companymail.com, will generate an incident. | | | 1.2 | |  | | --- | | Self CV/Resume Distribution: English (Default) (1675823) | | Rule for detecting distribution of a person's own CV or resume by first identifying a document as a CV or resume, then comparing the employee's user name to the document owner's name and email address, as extracted from the opening section of the document. For example, a CV document that starts with the line "CV of Dr. John M. Smith", that is sent from address jsmith@companymail.com, will generate an incident. | | |

SOURCE CODE POLICY

A screenshot of a cell phone

Description automatically generated

A screenshot of a cell phone

Description automatically generated

Git Hub Policy

Track more the 2 kb data in git hub site upload

A screenshot of a social media post

Description automatically generated

A screenshot of a cell phone

Description automatically generated

ENDPOINT APPLICATION FOR TRACKING

A screenshot of a social media post

Description automatically generated