Metadata for Section [Three]

Section Description: Describe what this section intends to cover

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Video Number** | **Video Title** | **Problem / Solution (Not more than 50 words)** | **Step 1 (Not more than 10 words)** | **Step 2(Not more than 10 words)** | **Step 3(Not more than 10 words)** |
| 1.1 | What is an insider threat? | Networks are hit by attackers all the time. Sometimes these attacks are not random people or outside attackers. Understanding what a insider threat is and how to deal with it is essential. | Malicious and unwitting insiders exist. | Account auditing and control is important. | User training will help with unwitting insider attacks. |
| 1.2 | Why employee training is important and some tips | Your employees tend to outnumber your IT and security teams. Your employees also tend to be the primary target for attacks. Keeping them trained can help them and you. | Trainings should be engaging. | Trainings should be relevant and easy to understand. | Gamification and recognition can help keep trainings engaging. |
| 1.3 | Why you need to strike a balance between security and ease of use | Having a too restrictive network can not only prevent your employees from doing their day to day jobs, but also create resentment. | It is far easier to create a restricted account first, than to take away later. | You should be mindful of what employees need. | Keep a balance between network security and usability. |
| 1.4 | Employee reporting | Enabling employees to easily report issues will help with your overall security posture. | Reporting should be easy and anonymous if need be. | Punishment and ridicule of reporting is a bad idea. | Reporting can be a double edge sword. |
|  |  |  |  |  |  |