**Implementation Report: Spoof Intelligence Insight**

**Introduction**: Spoofing attacks pose significant threats to organizational cybersecurity, with attackers impersonating legitimate entities to deceive recipients and initiate malicious activities such as phishing or spam. To combat these risks, Microsoft 365 offers spoof intelligence as part of its defense mechanisms, automatically protecting inbound email messages against spoofing in Exchange Online organizations or standalone Exchange Online Protection (EOP) environments. This report outlines the implementation of spoof intelligence insights to enhance the overall security posture of the organization.

**Implementation Steps:**

1. **Access Spoof Intelligence Insight:**
   * Navigate to the Microsoft Defender portal at [https://security.microsoft.com](https://security.microsoft.com/).
   * Go to Email & Collaboration > Policies & Rules > Threat policies > Tenant Allow/Block Lists in the Rules section.
   * Alternatively, use the direct link: <https://security.microsoft.com/tenantAllowBlockList>.
2. **Select Spoofed Senders Tab:**
   * On the Spoofed senders tab, review the spoof intelligence insight, which provides information about detected spoofing activities, including insight mode and what-if mode.
3. **View Spoof Intelligence Details:**
   * Click on View spoofing activity in the spoof intelligence insight to access the Spoof intelligence insight page.
   * Detailed information about spoofed senders, including spoofed user, sending infrastructure, message count, last seen, spoof type, and action, is displayed.
4. **Navigate Spoof Intelligence Insights:**
   * Use the Spoof intelligence insight page to sort entries by various columns and utilize filtering options based on spoof type and action.
   * Export the list of spoof detections to a CSV file for further analysis if necessary.
5. **Review Spoof Detection Details:**
   * Upon selecting a spoof detection, a details flyout opens, providing comprehensive information about the spoofed sender, including why it was detected, domain summary, WhoIs data, Explorer investigation, and similar emails.
6. **Override Spoof Intelligence Verdict:**
   * Users can override the spoof intelligence verdict by selecting one or more entries from the list and choosing to allow or block spoofing through bulk actions or individual selection.

***Note:*** *About Allowed Spoofed Senders: Understand that messages from allowed spoofed senders are permitted only using specific combinations of spoofed domains and sending infrastructures, enhancing security while allowing legitimate spoofed messages.*

**Conclusion**: The implementation of spoof intelligence insights within the organization's Microsoft 365 environment represents a proactive measure to mitigate the risks associated with spoofing attacks. By leveraging advanced threat detection capabilities and robust spoofing detection mechanisms, the organization strengthens its overall cybersecurity posture and protects against email-based threats. Continuous monitoring, periodic reviews, and employee awareness initiatives will be essential to maintaining the effectiveness of spoof intelligence insights and safeguarding organizational assets against evolving cyber threats

**Appendix:**

In addition to implementing spoof intelligence insights, we actively monitored and managed spoofing incidents within our Microsoft 365 environment. Below is a compiled list detailing the spoof emails detected, along with the corresponding actions suggested by the company and implemented to mitigate potential threats.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Spoofed user | Sending infrastructure | Count | Last seen | Spoof type | Action | Changes  Suggested  By TAP |
| vyrix.pro | google.com | 2 | 2024-02-27T15:08:49.000Z | External | Allow | block |
| lpthatconverts.com | google.com | 2 | 2024-02-29T01:16:47.000Z | External | Allow | block |
| gmail.com | 168.167.100.0/24 | 1 | 2024-02-12T20:12:41.000Z | External | Block |  |
| 2fa.io | nxcli.net | 1 | 2024-02-28T14:44:24.000Z | External | Block |  |
| taurusquest.com | zcsend.in | 1 | 2024-02-06T18:02:39.000Z | External | Block |  |
| emotionalintelligencecourse.com | mcdlv.net | 1 | 2024-02-11T03:17:58.000Z | External | Block |  |
| datadriven-solutions.co | salesforce.com | 1 | 2024-02-13T18:29:57.000Z | External | Block |  |
| wcb.ab.ca | cp20.com | 1 | 2024-02-02T15:02:38.000Z | External | Block |  |
| ricepoint.com | ipost.com | 1 | 2024-02-20T05:10:17.000Z | External | Block |  |
| nero.be | hlev.gob.pe | 1 | 2024-02-18T13:42:47.000Z | External | Block |  |
| accufin.live | salesforce.com | 1 | 2024-02-16T19:15:24.000Z | External | Block |  |
| roocruit.com | 52.128.42.0/24 | 1 | 2024-02-27T14:14:01.000Z | External | Block |  |
| leads-marketing.net | salesforce.com | 1 | 2024-02-08T18:10:19.000Z | External | Block |  |
| podpire.com | sendgrid.net | 1 | 2024-02-03T22:42:51.000Z | External | Block |  |
| bestwesternstalbert.com | tcgms.net | 1 | 2024-02-27T00:18:22.000Z | External | Allow | fine |
| healy.world | outlook.com | 1 | 2024-02-01T23:41:33.000Z | External | Allow | fine |
| studiosparqs.com | google.com | 1 | 2024-02-07T11:53:23.000Z | External | Allow | fine |
| mabarnk.com | google.com | 1 | 2024-02-15T13:24:55.000Z | External | Allow | block |