PROOFPOINT

COURSE CONTENT

1. **Introduction to proofpoint**
2. **Protection server Foundation**
3. **Message flow**
4. **SMTP filtering and outbound threats**
5. **Protection server Administration**
    - Clusters and modules
    - Navigation
    - User management
    - End user services
6. **Protection server Configuration**
    - Policy Routes
    - Rules
    - Dispositions
    - Quarantine
    - Delivery Method
7. **Targeted Attack Protection:**

Targeted attack protection is a part of advance email protection in our Proofpoint solution. We can use this to analyzing a content and analyzing an emails that incoming into our organization. We can use this TAP to looking at

8. **Malicious URL's.**
9. **Malicious Attachments.**
10. **Imposter Email.**

Once we receive an URL phishing or attachment defense alert in TAP below are the things SOC team should investigate in TAP console.

11.1. Header

11.2. Description

11.3. Spread & Targeting

11.4. Attack Progression

11.5. Affected VIP's

11.6. Forensics

11.7. At Risk Users

11.8. Impacted User

11.9. Intended User

12. Threat response AutopullFOundation TRAP

13. Purpose of TRAP and how TRAP detects and pulls threats from mailbox

14. Email fraud defense Foundation

15. Email fraud defense Authentication

- SPF
- DKIM
- DMARC
- Email Protection