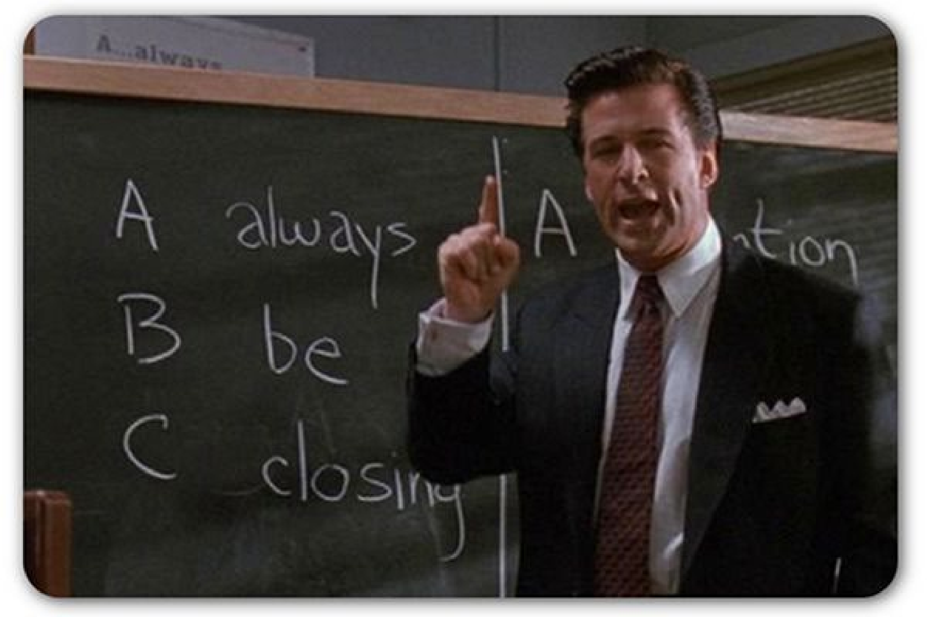
Pricing and Packaging

Pricing

- Let’s talk about vendors and toilet paper
- EDR is EDR, very little differences
- Little need for “expensive” solutions
- Open source NDR (Security Onion)
- SIEM/EDR mix (Elastic)
- Logging the right things
- Ignoring security is a bad idea
- Your competitors are doing it



Create a Community

Don't sell

- “Selling” feels like “Selling”
- Create awareness and training
- Open to the community
- Invite other firms
- Advertise
- Forget ABC
- Education first, sales second

Create a Community

- Create spaces your customers what to be
- Conference with a hot topic
- Small webcasts
- Community Outreach
- “Hotline” with questions
- Keep it non-technical
- Insurance and compliance drivers
- Not just your customers

Sales Messaging

Message

- This should not be an “Upsell”
- Keeping up with attacks
- Back to conferences and community
- Scary story in a sales call vs. in a presentation
- Bringing customers into compliance and in proper standing with cyber insurance

“We are not a target”

- Attackers love to target companies that think that
- Downtime costs money
- 71% of attacks are on small businesses
- https://www.techtimes.com/articles/245791/20191022/71-of-ransomware-attacks-target-small-businesses-are-you-ready.htm
- This should be a conference presentation

JUST BECAUSE YOU'RE PARANOID DOESN'T MEAN THEY'RE NOT OUT TO GET YOU

Insurance

Insurance

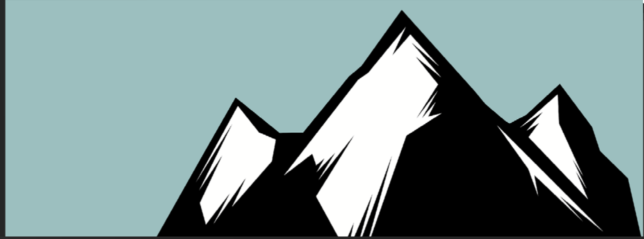
- Need for “Due Diligence”
- Different requirements for different industries and insurance companies
- Can no longer just have cyber insurance in lieu of having a security program
- Basics come into play here

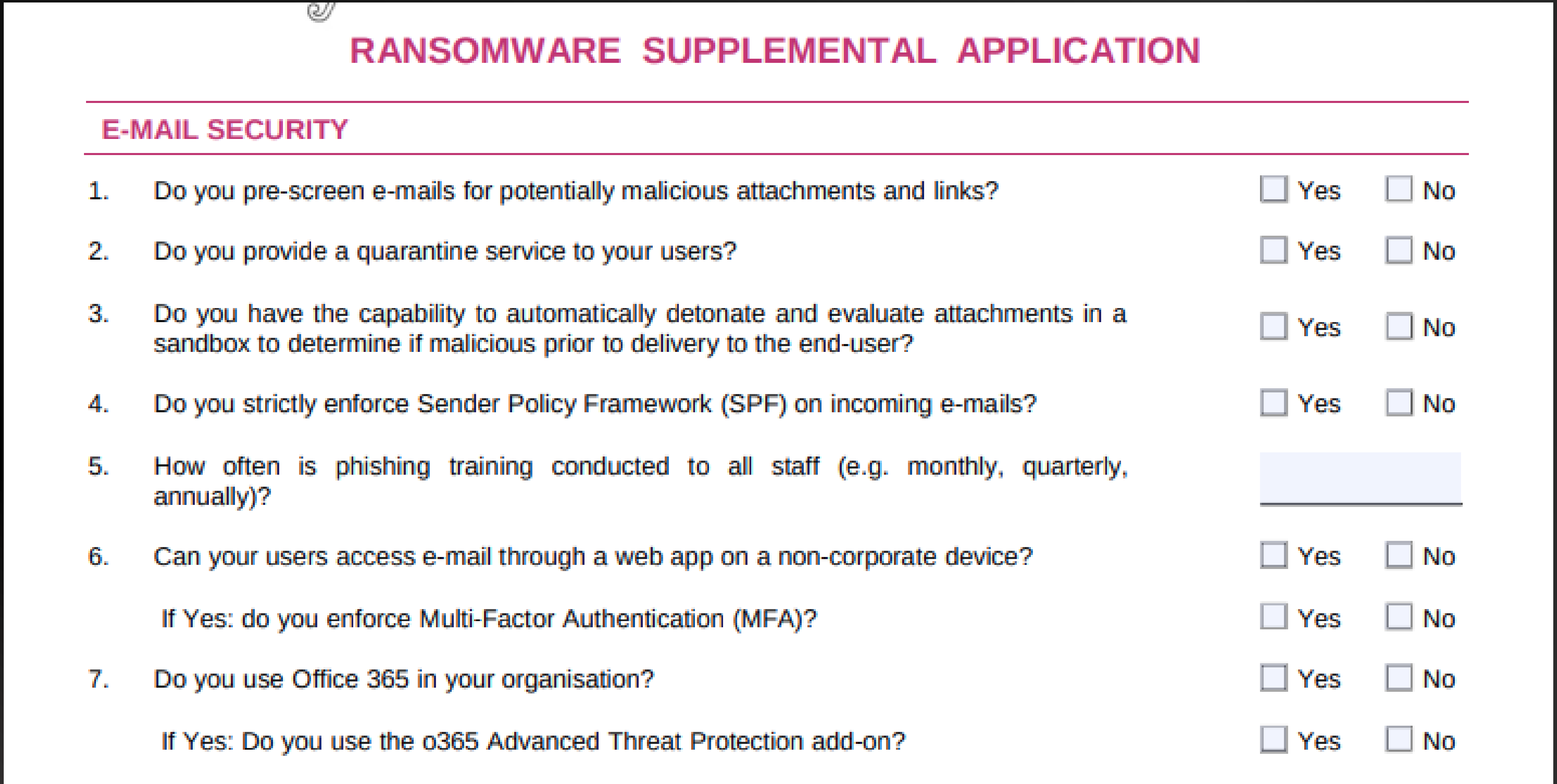
Insurance and IR

- Let's talk through a ransomware IR example
- Your customer may not get to choose the firm
- You will be essential to keep costs down
- What the insurance IR firm says "goes"
- The insurance IR firm is not your advocate

Master! Master! Master of Insurance is pulling your strings!!!!

Insurance and IR





RANSOMWARE SUPPLEMENTAL APPLICATION

E-MAIL SECURITY

1. Do you pre-screen e-mails for potentially malicious attachments and links? □ Yes □ No

2. Do you provide a quarantine service to your users? □ Yes □ No

3. Do you have the capability to automatically detonate and evaluate attachments in a sandbox to determine if malicious prior to delivery to the end-user? □ Yes □ No

4. Do you strictly enforce Sender Policy Framework (SPF) on incoming e-mails? □ Yes □ No

5. How often is phishing training conducted to all staff (e.g. monthly, quarterly, annually)? ______

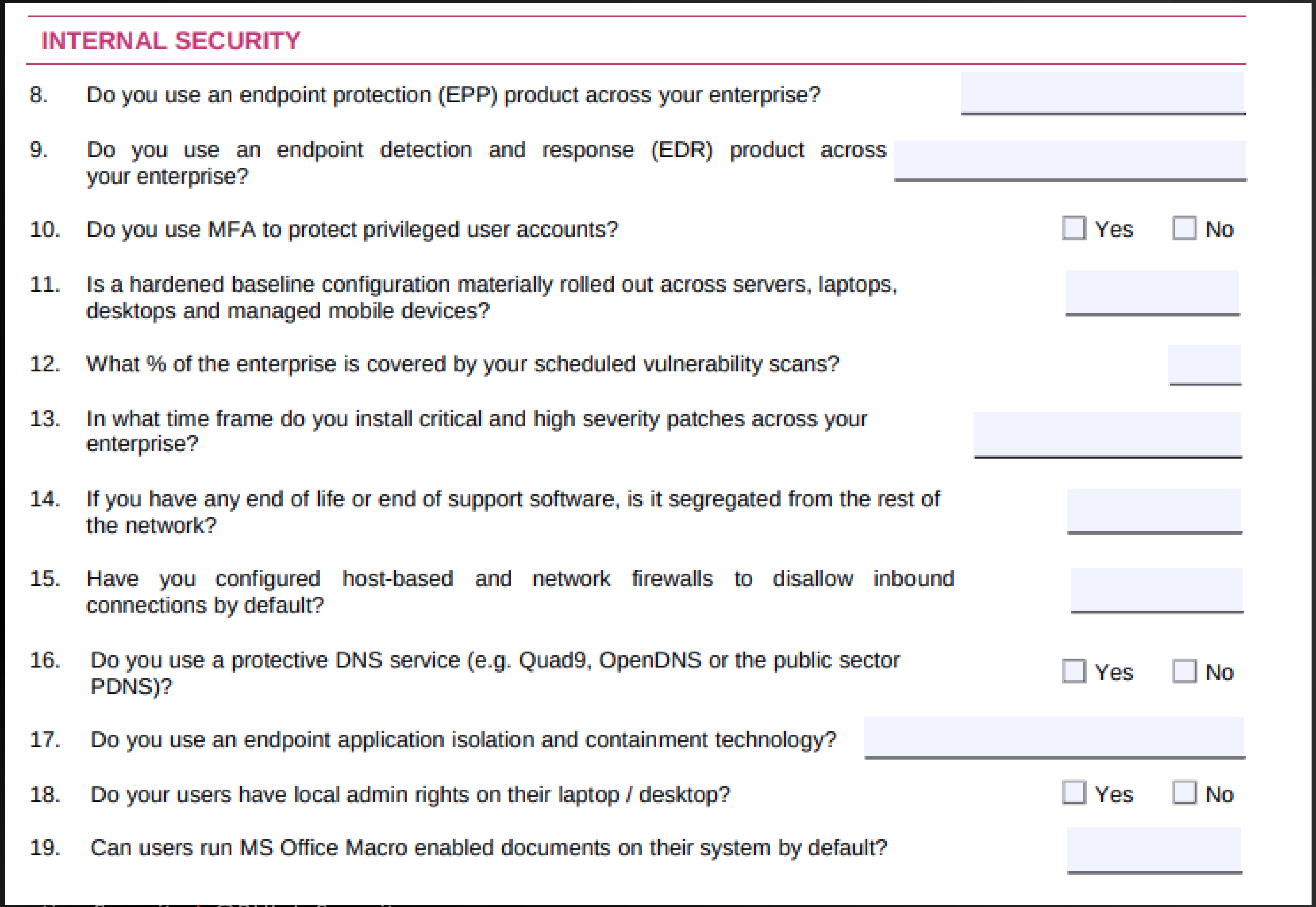
6. Can your users access e-mail through a web app on a non-corporate device? □ Yes □ No

   If Yes: do you enforce Multi-Factor Authentication (MFA)? □ Yes □ No

7. Do you use Office 365 in your organisation? □ Yes □ No

   If Yes: Do you use the o365 Advanced Threat Protection add-on? □ Yes □ No

Insurance and IR



INTERNAL SECURITY

8. Do you use an endpoint protection (EPP) product across your enterprise?

9. Do you use an endpoint detection and response (EDR) product across your enterprise?

10. Do you use MFA to protect privileged user accounts? □ Yes □ No

11. Is a hardened baseline configuration materially rolled out across servers, laptops, desktops and managed mobile devices?

12. What % of the enterprise is covered by your scheduled vulnerability scans?

13. In what time frame do you install critical and high severity patches across your enterprise?

14. If you have any end of life or end of support software, is it segregated from the rest of the network?

15. Have you configured host-based and network firewalls to disallow inbound connections by default?

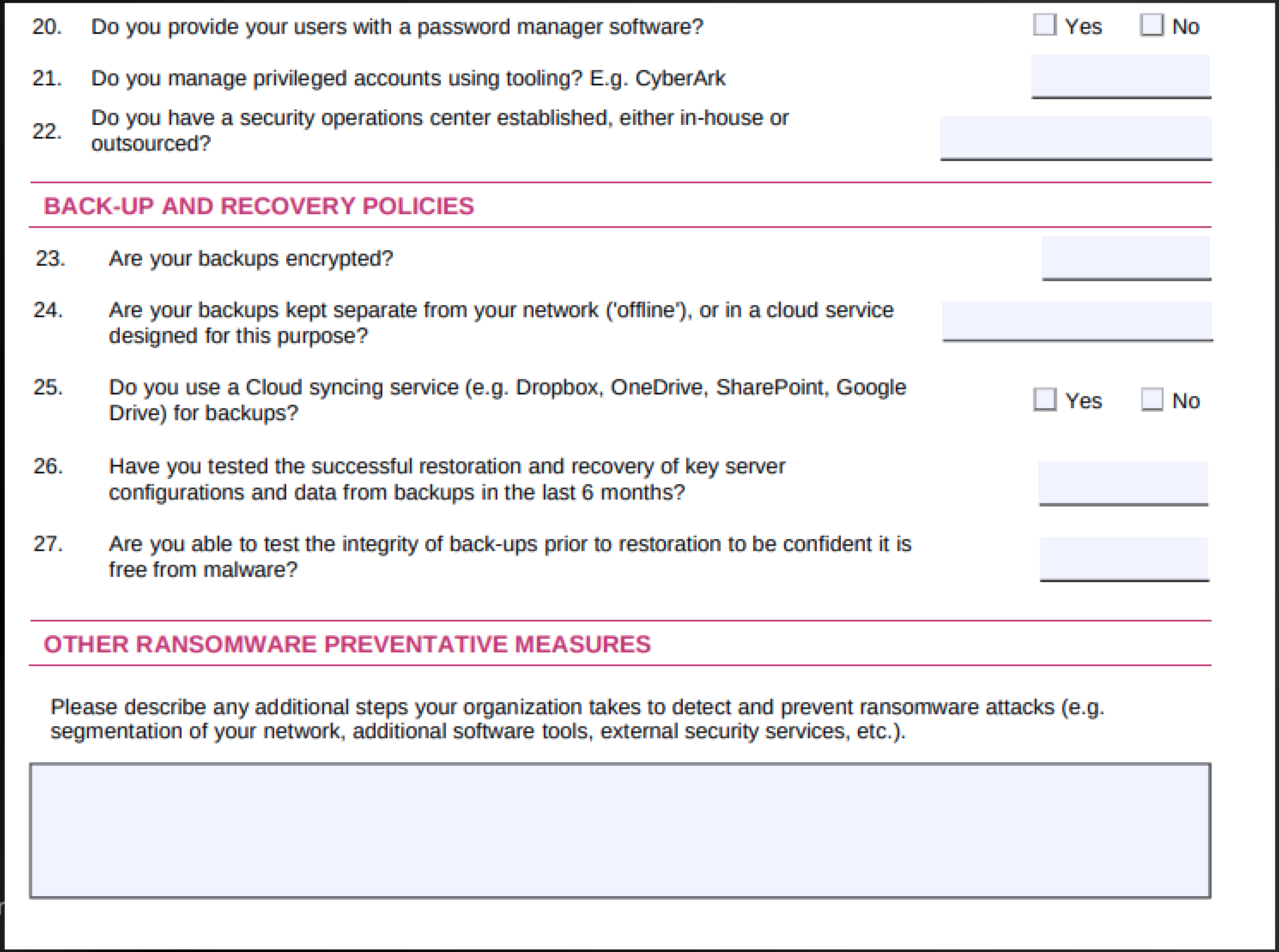
16. Do you use a protective DNS service (e.g. Quad9, OpenDNS or the public sector PDNS)? □ Yes □ No

17. Do you use an endpoint application isolation and containment technology?

18. Do your users have local admin rights on their laptop / desktop? □ Yes □ No

19. Can users run MS Office Macro enabled documents on their system by default?

Insurance and IR



20. Do you provide your users with a password manager software? ☐ Yes ☐ No

21. Do you manage privileged accounts using tooling? E.g. CyberArk

22. Do you have a security operations center established, either in-house or outsourced?

BACK-UP AND RECOVERY POLICIES

23. Are your backups encrypted?

24. Are your backups kept separate from your network ('offline'), or in a cloud service designed for this purpose?

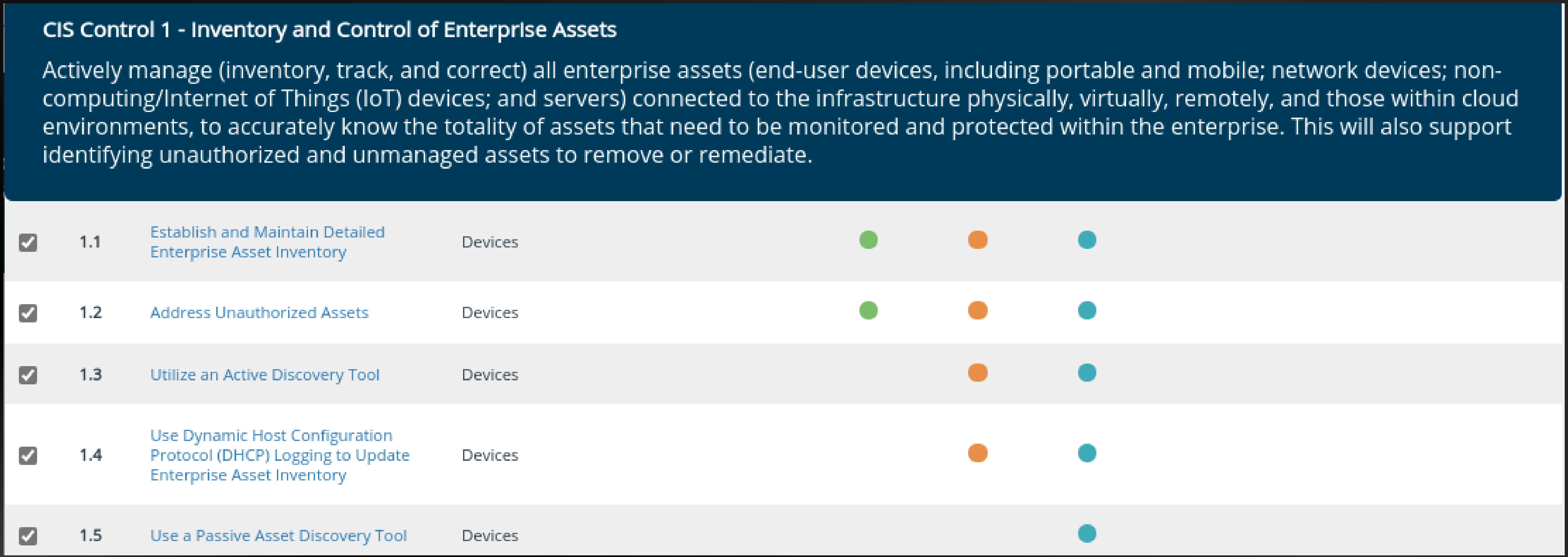
25. Do you use a Cloud syncing service (e.g. Dropbox, OneDrive, SharePoint, Google Drive) for backups? ☐ Yes ☐ No

26. Have you tested the successful restoration and recovery of key server configurations and data from backups in the last 6 months?

27. Are you able to test the integrity of back-ups prior to restoration to be confident it is free from malware?

OTHER RANSOMWARE PREVENTATIVE MEASURES

Please describe any additional steps your organization takes to detect and prevent ransomware attacks (e.g. segmentation of your network, additional software tools, external security services, etc.).



CIS Control 1 - Inventory and Control of Enterprise Assets

Actively manage (inventory, track, and correct) all enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/Internet of Things (IoT) devices; and servers) connected to the infrastructure physically, virtually, remotely, and those within cloud environments, to accurately know the totality of assets that need to be monitored and protected within the enterprise. This will also support identifying unauthorized and unmanaged assets to remove or remediate.

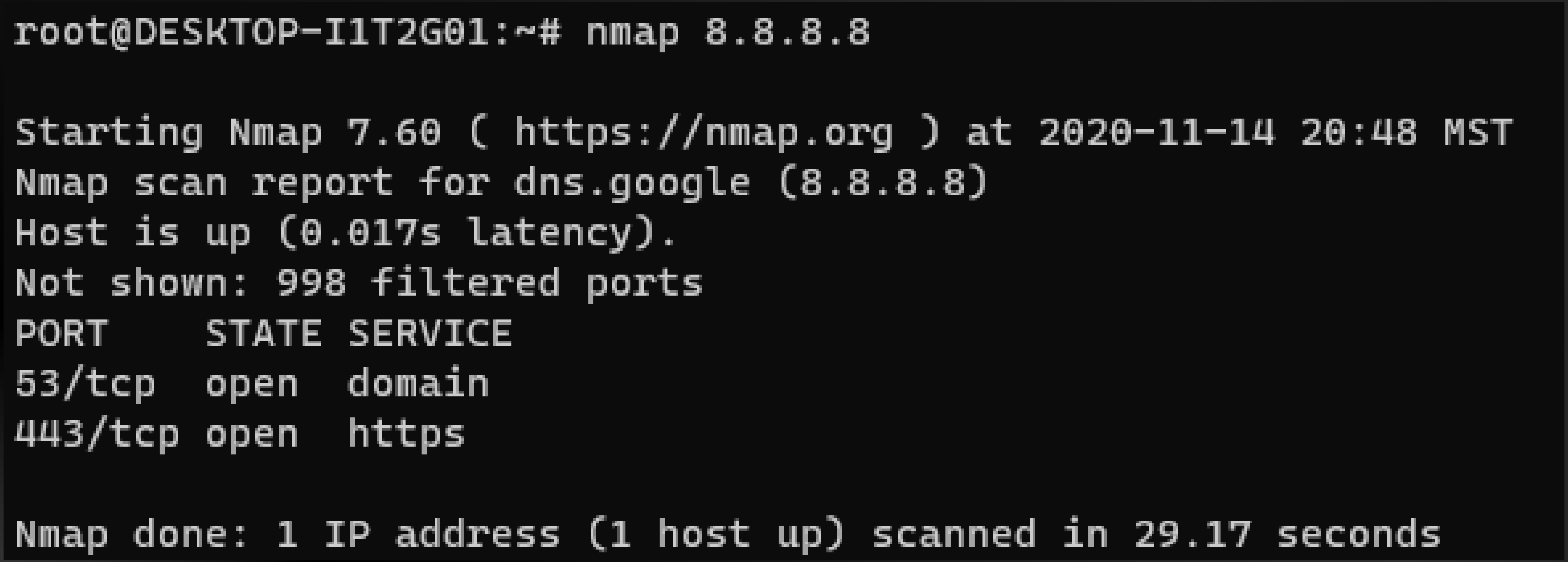
☑	1.1	Establish and Maintain Detailed Enterprise Asset Inventory	Devices	●	●	●
☑	1.2	Address Unauthorized Assets	Devices	●	●	●
☑	1.3	Utilize an Active Discovery Tool	Devices		●	●
☑	1.4	Use Dynamic Host Configuration Protocol (DHCP) Logging to Update Enterprise Asset Inventory	Devices		●	●
☑	1.5	Use a Passive Asset Discovery Tool	Devices			●

Active Device Discovery

Need For Scanning

- Going to need to scan
- Number of free tools
- But use Nmap
  - Used Everywhere
  - Gold standard
  - Great output options
  - Every tool can import results
- https://nmap.org/

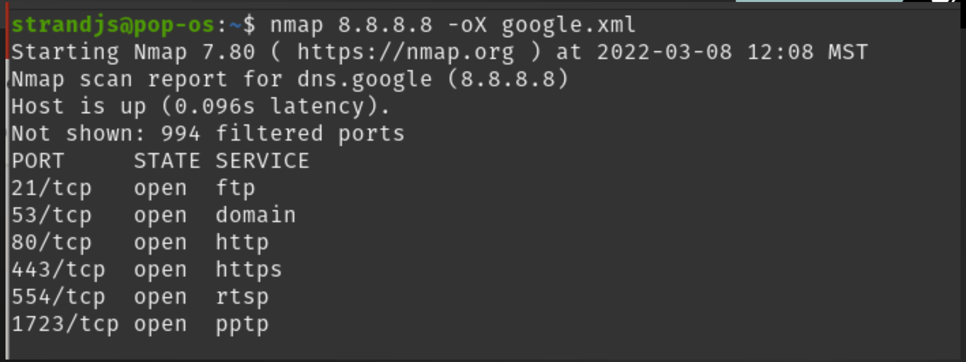
Open Remote Ports With Nmap



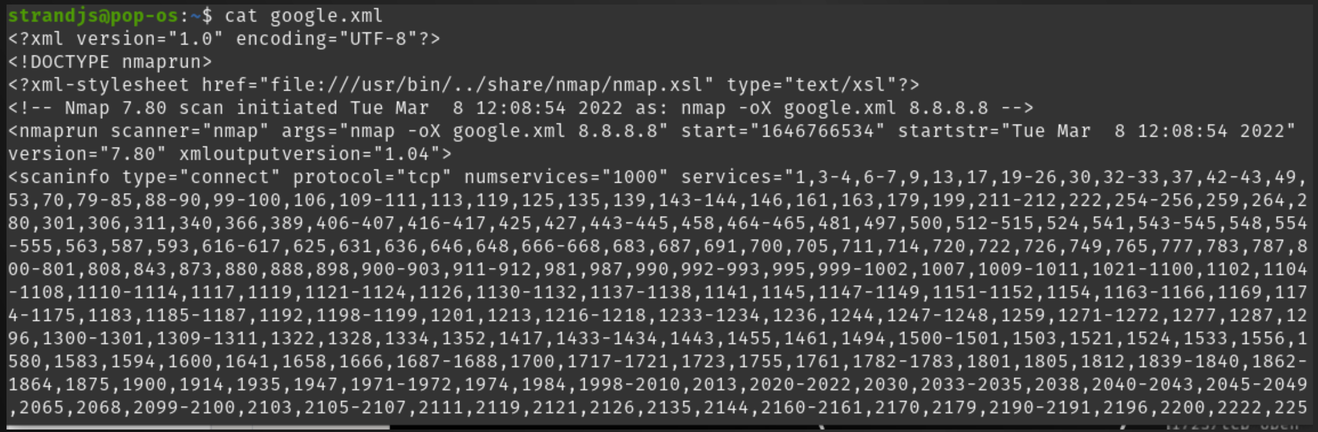
```
root@DESKTOP-I1T2G01:~# nmap 8.8.8.8

Starting Nmap 7.60 ( https://nmap.org ) at 2020-11-14 20:48 MST
Nmap scan report for dns.google (8.8.8.8)
Host is up (0.017s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE
53/tcp  open  domain
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 29.17 seconds
```

Nmap Output

- -oN = Normal
- -oX = XML (Use this one!)
- -oS = "ScRipT KIdd|3 oUTpuT"
- -oG = Greppable



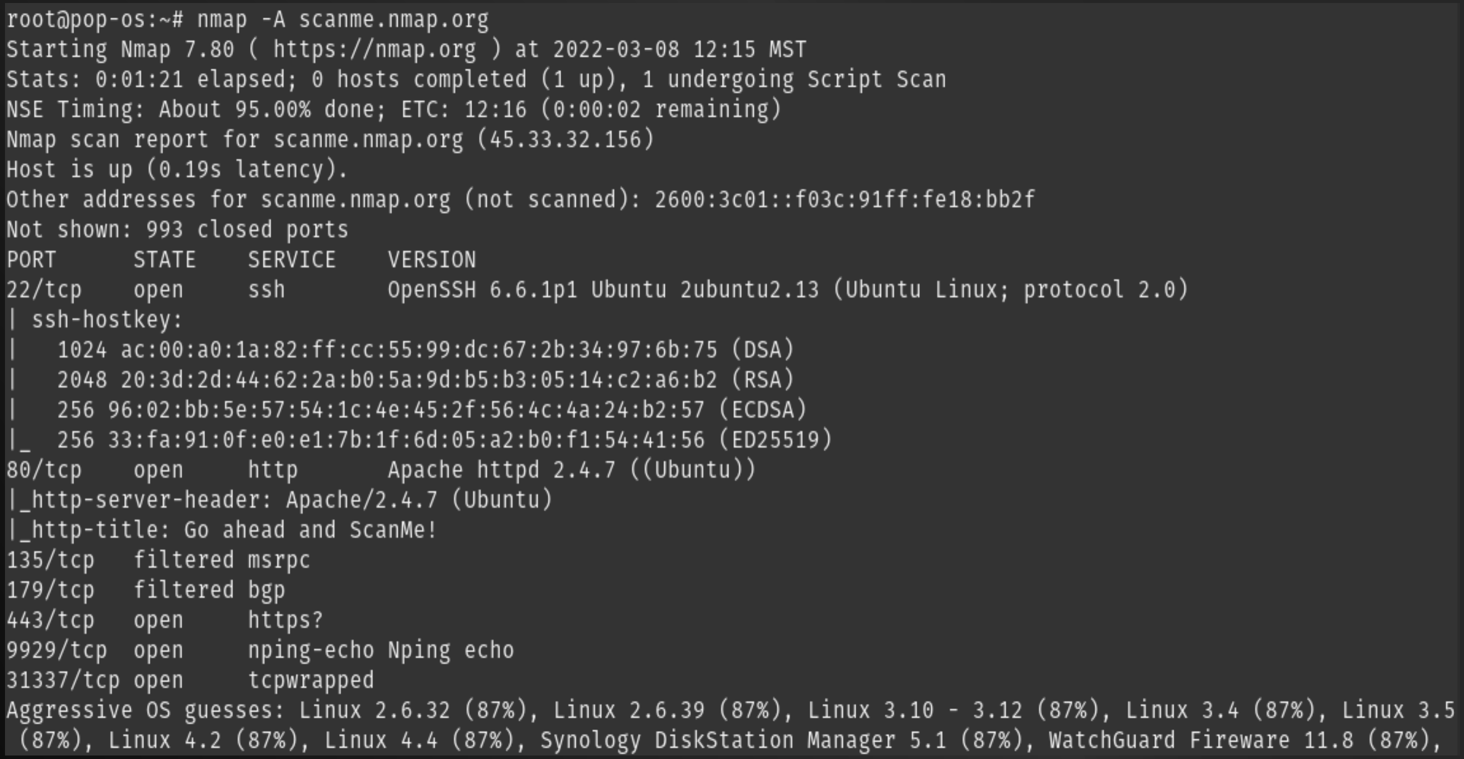
```
strandjs@pop-os:~$ nmap 8.8.8.8 -oX google.xml
Starting Nmap 7.80 ( https://nmap.org ) at 2022-03-08 12:08 MST
Nmap scan report for dns.google (8.8.8.8)
Host is up (0.096s latency).
Not shown: 994 filtered ports
PORT     STATE SERVICE
21/tcp   open  ftp
53/tcp   open  domain
80/tcp   open  http
443/tcp  open  https
554/tcp  open  rtsp
1723/tcp open  pptp
```



```
strandjs@pop-os:~$ cat google.xml
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE nmaprun>
<?xml-stylesheet href="file:///usr/bin/../share/nmap/nmap.xsl" type="text/xsl"?>
<!-- Nmap 7.80 scan initiated Tue Mar  8 12:08:54 2022 as: nmap -oX google.xml 8.8.8.8 -->
<nmaprun scanner="nmap" args="nmap -oX google.xml 8.8.8.8" start="1646766534" startstr="Tue Mar  8 12:08:54 2022"
version="7.80" xmloutputversion="1.04">
<scaninfo type="connect" protocol="tcp" numservices="1000" services="1,3-4,6-7,9,13,17,19-26,30,32-33,37,42-43,49,
53,70,79-85,88-90,99-100,106,109-111,113,119,125,135,139,143-144,146,161,163,179,199,211-212,222,254-256,259,264,2
80,301,306,311,340,366,389,406-407,416-417,425,427,443-445,458,464-465,481,497,500,512-515,524,541,543-545,548,554
-555,563,587,593,616-617,625,631,636,646,648,666-668,683,687,691,700,705,711,714,720,722,726,749,765,777,783,787,8
00-801,808,843,873,880,888,898,900-903,911-912,981,987,990,992-993,995,999-1002,1007,1009-1011,1021-1100,1102,1104
-1108,1110-1114,1117,1119,1121-1124,1126,1130-1132,1137-1138,1141,1145,1147-1149,1151-1152,1154,1163-1166,1169,117
4-1175,1183,1185-1187,1192,1198-1199,1201,1213,1216-1218,1233-1234,1236,1244,1247-1248,1259,1271-1272,1277,1287,12
96,1300-1301,1309-1311,1322,1328,1334,1352,1417,1433-1434,1443,1455,1461,1494,1500-1501,1503,1521,1524,1533,1556,1
580,1583,1594,1600,1641,1658,1666,1687-1688,1700,1717-1721,1723,1755,1761,1782-1783,1801,1805,1812,1839-1840,1862-
1864,1875,1900,1914,1935,1947,1971-1972,1974,1984,1998-2010,2013,2020-2022,2030,2033-2035,2038,2040-2043,2045-2049
,2065,2068,2099-2100,2103,2105-2107,2111,2119,2121,2126,2135,2144,2160-2161,2170,2179,2190-2191,2196,2200,2222,225
```

Nmap Service Identification

- -A Everything Fyodor wants, or Aggressive
- OS, Service, Version and Traceroute
- Great for inventorying systems and services



```
root@pop-os:~# nmap -A scanme.nmap.org
Starting Nmap 7.80 ( https://nmap.org ) at 2022-03-08 12:15 MST
Stats: 0:01:21 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 95.00% done; ETC: 12:16 (0:00:02 remaining)
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.19s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 993 closed ports
PORT      STATE    SERVICE    VERSION
22/tcp    open     ssh        OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 ac:00:a0:1a:82:ff:cc:55:99:dc:67:2b:34:97:6b:75 (DSA)
|   2048 20:3d:2d:44:62:2a:b0:5a:9d:b5:b3:05:14:c2:a6:b2 (RSA)
|   256 96:02:bb:5e:57:54:1c:4e:45:2f:56:4c:4a:24:b2:57 (ECDSA)
|_  256 33:fa:91:0f:e0:e1:7b:1f:6d:05:a2:b0:f1:54:41:56 (ED25519)
80/tcp    open     http       Apache httpd 2.4.7 ((Ubuntu))
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Go ahead and ScanMe!
135/tcp   filtered msrpc
179/tcp   filtered bgp
443/tcp   open     https?
9929/tcp  open     nping-echo Nping echo
31337/tcp open     tcpwrapped
Aggressive OS guesses: Linux 2.6.32 (87%), Linux 2.6.39 (87%), Linux 3.10 - 3.12 (87%), Linux 3.4 (87%), Linux 3.5
 (87%), Linux 4.2 (87%), Linux 4.4 (87%), Synology DiskStation Manager 5.1 (87%), WatchGuard Fireware 11.8 (87%),
```

Why Active Device Discovery?

- Rogue Assets
  - Wireless access points
  - Personal PCs and Phones
  - Wi-Fi Pineapple
- Old Assets
  - That Windows 2000 server in the closet
- Incident Response!!!
  - Answering what and where

Active "Device" Discovery and the Cloud

- Very hard
- Back to Vuln Scanning
- Transient and ephemeral assets
- What is the "cloud"?
  - Azure/AWS/GCP easier
  - Third-party services are much harder
  - Think Salesforce, Calendly, Grammarly, etc.

Fine, this is fine

Passive Device and Software Discovery

Passive Device Discovery

- Number of ways to do this
- Dynamic Host Configuration Protocol
- Data in switch CAM table
- Mostly just IP and MAC address
- Need for tools like Zeek

Passive Device DiscoveryAD

- For Windows systems
- Active Directory is good
- Microsoft Endpoint Configuration Manager is better
- RMM tools have great data

Microsoft

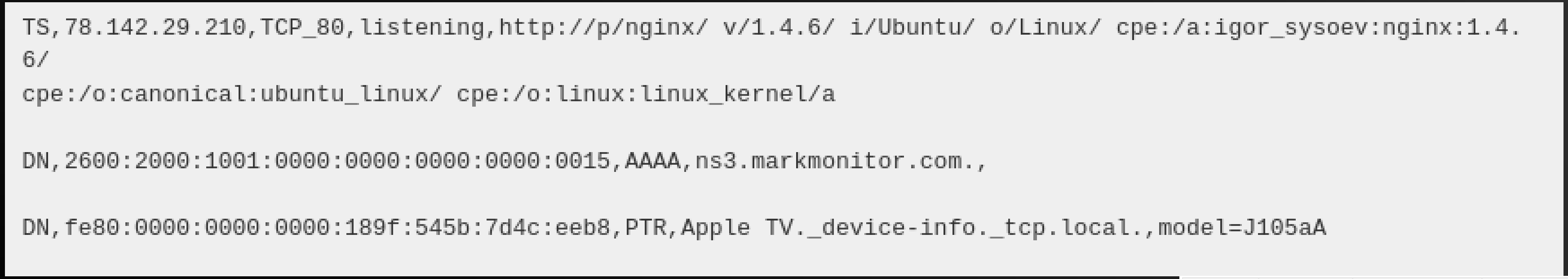
Microsoft Endpoint Configuration Manager

Passive Device Discovery - Zeek

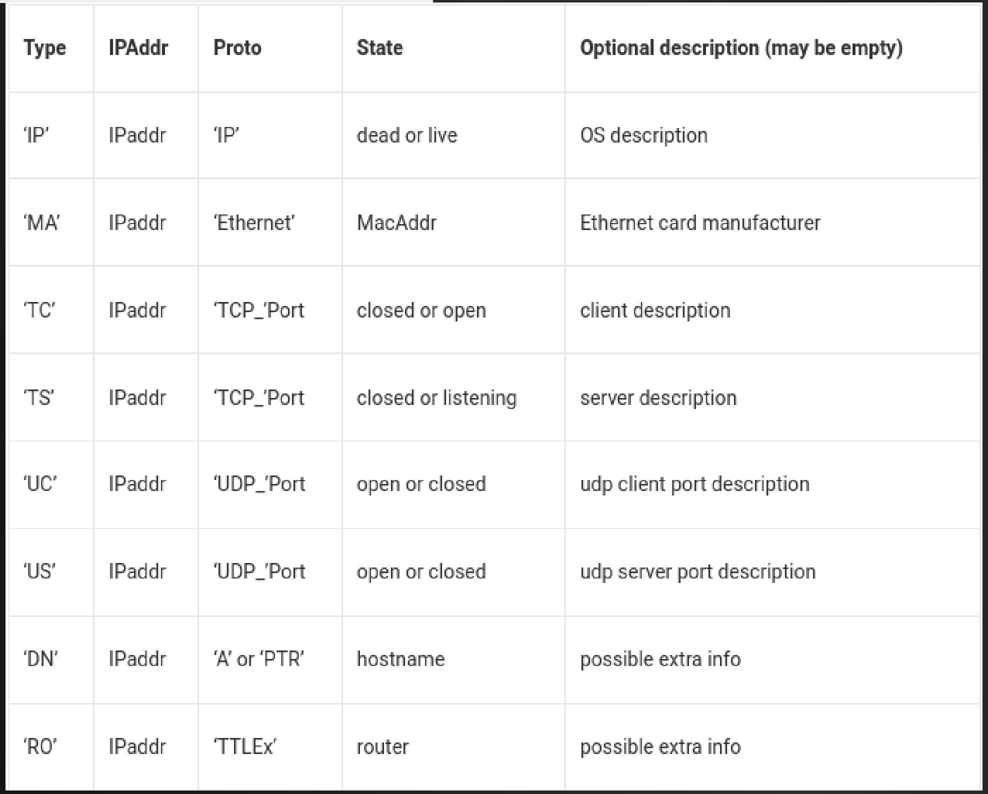
- Place on egress
- Pre NAT
- Can help identify systems based on multiple points (i.e. User Agent Strings)
- Can be coupled with tools like Passer

The Zeek Network Security Monitor

Passive Device Discovery - Passer

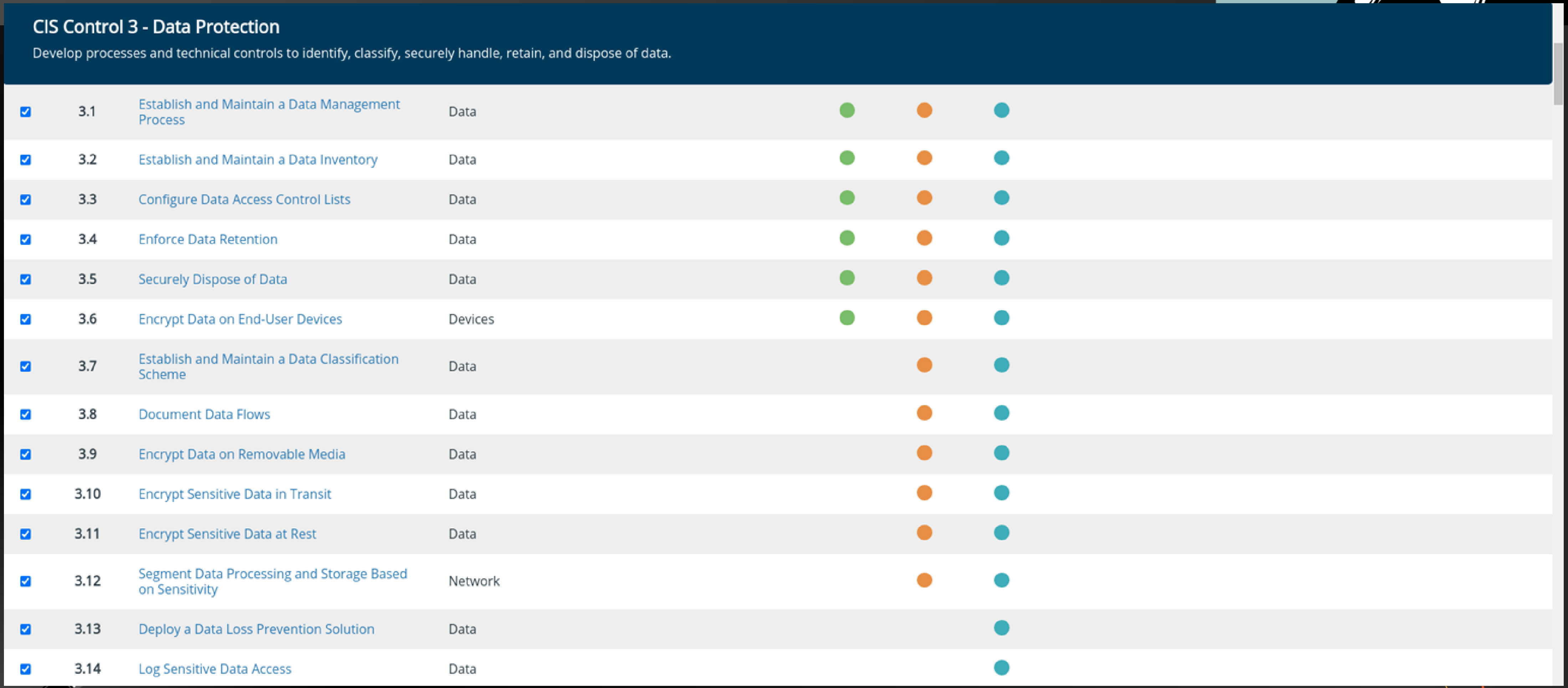


```
TS,78.142.29.210,TCP_80,listening,http://p/nginx/ v/1.4.6/ i/Ubuntu/ o/Linux/ cpe:/a:igor_sysoev:nginx:1.4.
6/
cpe:/o:canonical:ubuntu_linux/ cpe:/o:linux:linux_kernel/a

DN,2600:2000:1001:0000:0000:0000:0000:0015,AAAA,ns3.markmonitor.com.,

DN,fe80:0000:0000:0000:189f:545b:7d4c:eeb8,PTR,Apple TV._device-info._tcp.local.,model=J105aA
```



Type	IPAddr	Proto	State	Optional description (may be empty)
‘IP’	IPaddr	‘IP’	dead or live	OS description
‘MA’	IPaddr	‘Ethernet’	MacAddr	Ethernet card manufacturer
‘TC’	IPaddr	‘TCP_’Port	closed or open	client description
‘TS’	IPaddr	‘TCP_’Port	closed or listening	server description
‘UC’	IPaddr	‘UDP_’Port	open or closed	udp client port description
‘US’	IPaddr	‘UDP_’Port	open or closed	udp server port description
‘DN’	IPaddr	‘A’ or ‘PTR’	hostname	possible extra info
‘RO’	IPaddr	‘TTLEx’	router	possible extra info

Data Inventory/Classification



CIS Control 3 - Data Protection

Develop processes and technical controls to identify, classify, securely handle, retain, and dispose of data.

☑	3.1	Establish and Maintain a Data Management Process	Data	●	●	●
☑	3.2	Establish and Maintain a Data Inventory	Data	●	●	●
☑	3.3	Configure Data Access Control Lists	Data	●	●	●
☑	3.4	Enforce Data Retention	Data	●	●	●
☑	3.5	Securely Dispose of Data	Data	●	●	●
☑	3.6	Encrypt Data on End-User Devices	Devices	●	●	●
☑	3.7	Establish and Maintain a Data Classification Scheme	Data		●	●
☑	3.8	Document Data Flows	Data		●	●
☑	3.9	Encrypt Data on Removable Media	Data		●	●
☑	3.10	Encrypt Sensitive Data in Transit	Data		●	●
☑	3.11	Encrypt Sensitive Data at Rest	Data		●	●
☑	3.12	Segment Data Processing and Storage Based on Sensitivity	Network		●	●
☑	3.13	Deploy a Data Loss Prevention Solution	Data			●
☑	3.14	Log Sensitive Data Access	Data			●

Data Protection

- Every standard has recommended procedures for:
    - Retention, disposal, classification, flows, Access Controls, etc.
- Need to focus on a few key things
- Let's focus on actual attacks more than each nitnoid standard
- Simply having a policy that outlines the above is enough for most customers

Data Protection – Real Attacks

- Real attacks leverage data being where it should not be
- File servers
- .xls files with passwords
- Under protected shares
- You can classify all you want... But if a user loads sensitive data on a open share, it does not matter at all

Data Protection – Auditing

- What are the permissions on your shares?
- Run tools like FileFinder
- Audit access to sensitive files.... Also, honey shares and files

Data Protection – Classification

- Does little to stop attacks
- Builds awareness
- Honest people honest
- Forces an org to know what they are dealing with
- Brings compliance to the forefront
- Dirty word search and filtering