Continuous Monitoring on a Budget

OpenWRT, Python, Documented Analytic Tradecraft, and the Cloud

Ryan Wilson
@SpotlightCybsec

Spotlight Cybersecurity

BSides Atlanta 2019

spotlightcybersecurity.com

Need Enterprise Experience…

… on a beer budget

Saving Money Takes Time!

… because the Bad Guy only needs one way in

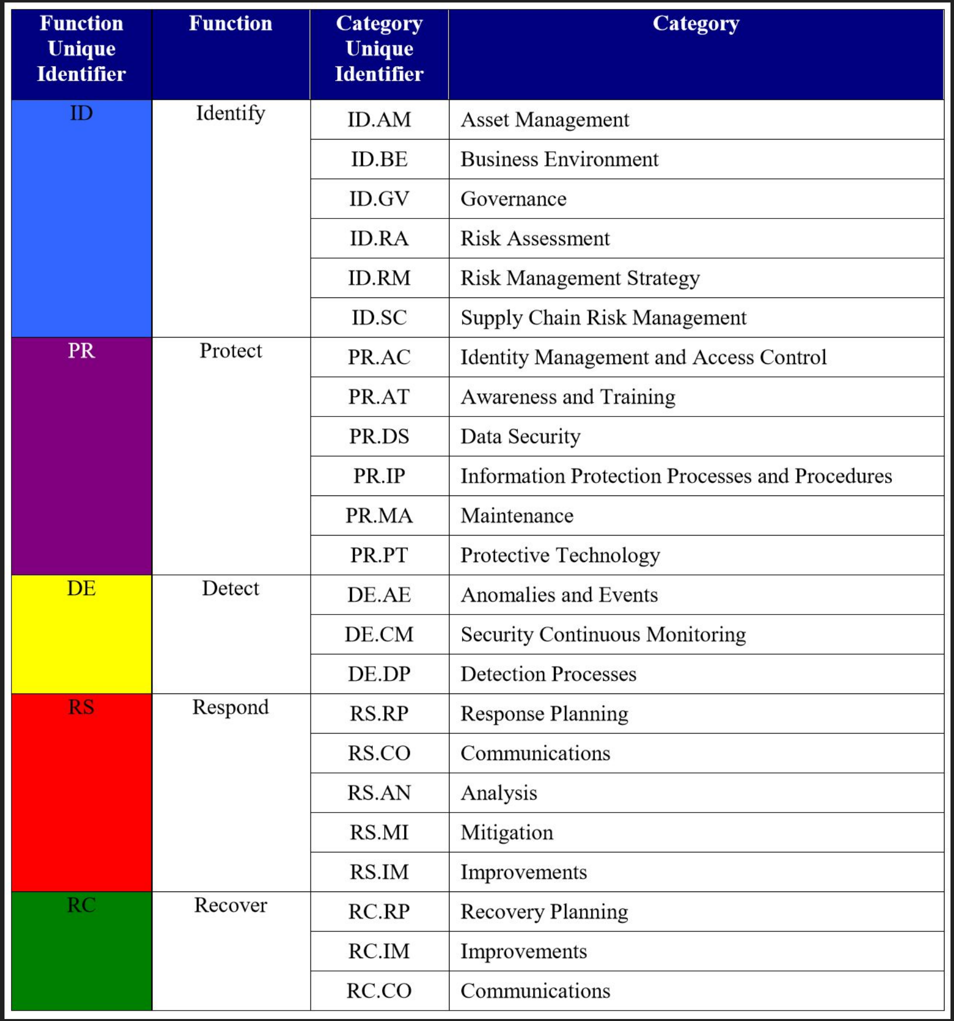
Continuous Monitoring vs. Continuous Assurance

feeling confident about the state of your business operations and data

Where to Start

What should I do to protect my [home/business]?

- Frameworks Prioritized by Threats:
  - NIST Cybersecurity Framework (v1.1)
  - CIS Controls (v7.1)
- Identify What’s Important to Protect
  - CIS Controls: “You must still understand what is critical to your business, data, systems, networks, and infrastructures, and you must consider the adversarial actions that could impact your ability to be successful in the business or operation.”
  - Any regulations that apply? PCI, HIPAA, OSHA?



Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Components of a Continuous Monitoring System

- Documentation
  - What are we protecting
  - Client Policies - descriptions of what the system should look like and how the system (and the users!) should behave
- Data
  - Hardware Sensors/TAPs - gather network data
  - Software Agents - gather system data
- Data Storage - securely store data
- Data Transport - securely get data from the client’s systems back to yours
- Analysis Servers - out-of-band place to run analytics on the data
- Analytics - what to look for in the data

Components of a Continuous Monitoring System

- Documentation
  - What are we protecting
  - Client Policies - descriptions of what the system should look like and how the system (and the users!) should behave
- Data
  - Hardware Sensors/TAPs - gat rk data
  - Software Agents - gather system da
- Data Storage - securely
- Data Transport - securely get urs
- Analysis Servers - out-of-band plac
- Analytics - what to look for in the data

The Fun Technical Stuff

Components of a Continuous Monitoring System

- Documentation
  - What are we protecting
  - Client Policies - descriptions o ystem. users!) should behav
- Data
  - Hardware Sensors/TAPs - gat rk data
  - Software Agents - gather system da
- Data Storage - securely
- Data Transport - securely get urs
- Analysis Servers - out-of-band plac
- Analytics - what to look for in the data

The Boring but Important Written Details

The Fun Technical Stuff

Components of a Continuous Monitoring System

- Documentation
  - What are we protecting
  - Client Policies - descriptions o system.
    users!) should behav
- Data
  - Hardware
  - Software A
- Data Storag
- Data Transp
- Analysis Ser
- Analytics - w

The Boring but Important
Written Details

Best Practices Require Documentation! Some examples:

- NIST CSF -
  - ID.AM - Inventory of hardware, software, external systems, data flows
  - PR.PT - Locations of audit logs are documented and reviewed
  - DE.DP - Detection processes are documented
  - RS.RP - Incident response plan documented
  - RC.RP - Recovery plan documented
- CIS Control 5.1 “Establish Secure Configurations - Maintain documented security configuration standards for all authorized operating systems and software.”

Work-in-Progress!

Goals

Regulatory Compliance (mostly HIPAA):

Documentation! Two clients have nothing for the technical rule!

One client cares especially about current Windows Updates and Anti-Virus

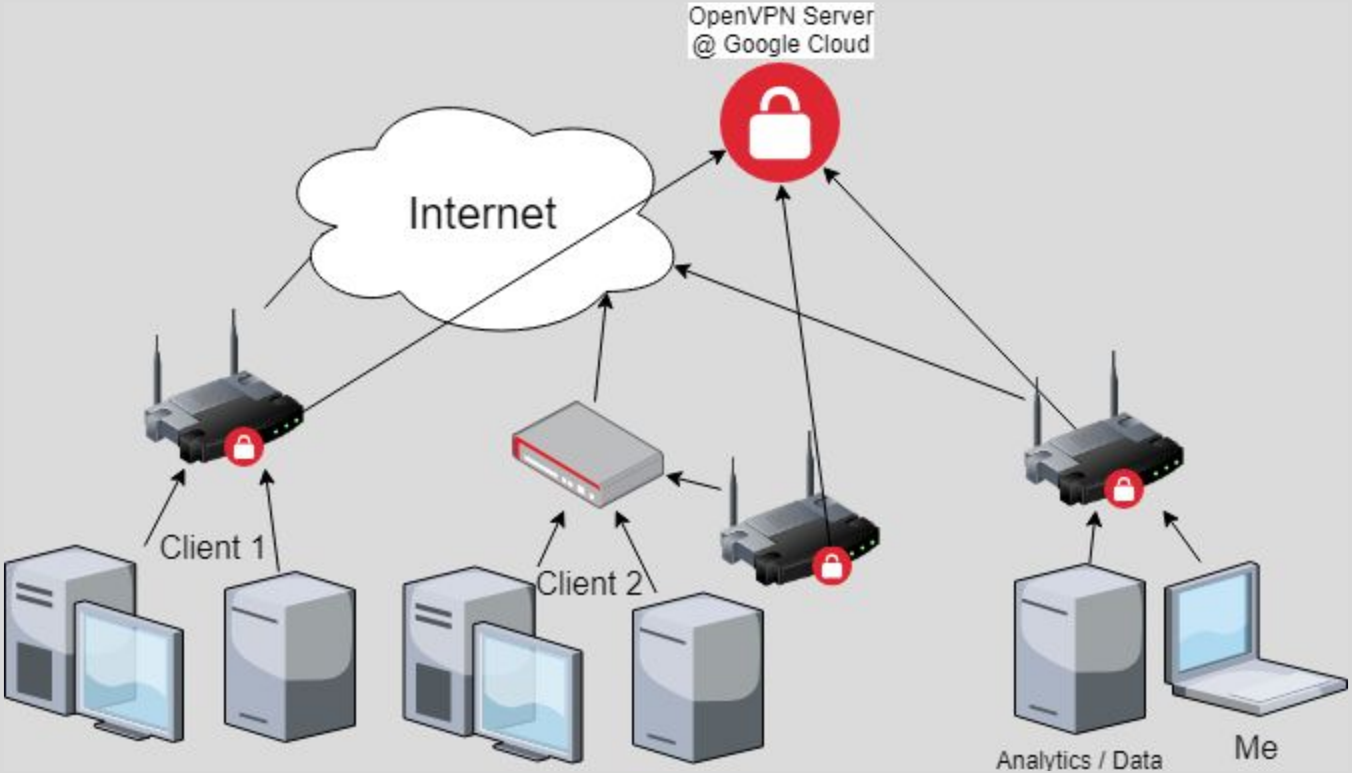
CIS Control 1 - Inventory & Control of Hardware Assets

CIS Control 2 - Inventory & Control of Software Assets

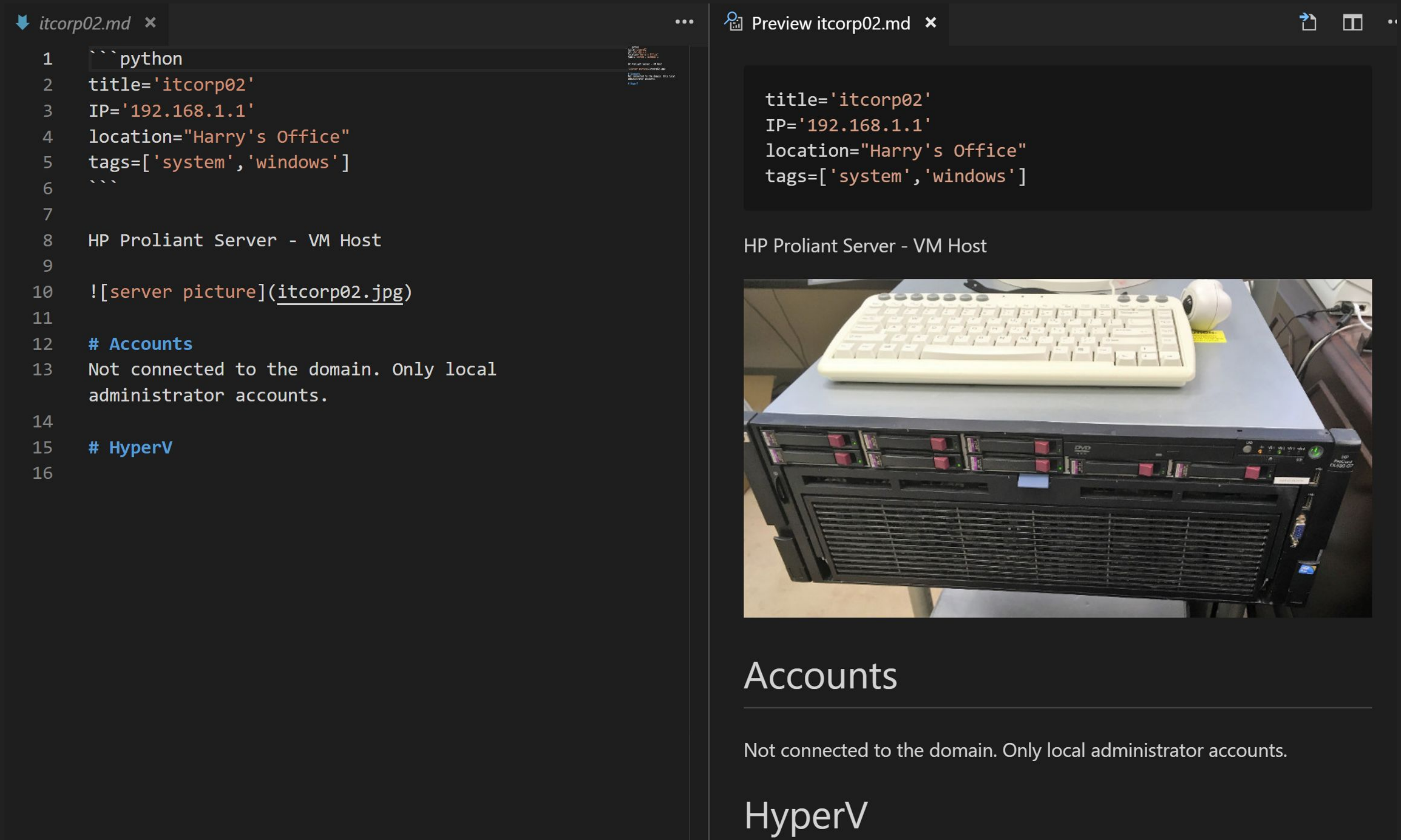
CIS Control 3 - Continuous Vulnerability Management

RMM - Are the systems up? What IPs are they at?

The Architecture



Documentation - Surety



~~~
```python
title='itcorp02'
IP='192.168.1.1'
location="Harry's Office"
tags=['system','windows']
```

HP Proliant Server - VM Host

![server picture](itcorp02.jpg)

# Accounts
Not connected to the domain. Only local administrator accounts.

# HyperV
~~~

```
title='itcorp02'
IP='192.168.1.1'
location="Harry's Office"
tags=['system','windows']
```

HP Proliant Server - VM Host

Accounts

Not connected to the domain. Only local administrator accounts.

HyperV

Written in Markdown
Rendered as HTML

Spotlight
Cybersecurity

Surety ≡ Tested & Rendered on 2019-05-03 21:33

Dashboard

Anti-Virus

compliance ›

systems ›

User Accounts

Windows Software

Windows Updates

itcorp02

python

```python
title='itcorp02'
IP='192.168.1.1'
location="Harry's Office"
tags=['system','windows']
```

HP Proliant Server - VM Host

Accounts

Not connected to the domain. Only local administrator accounts.

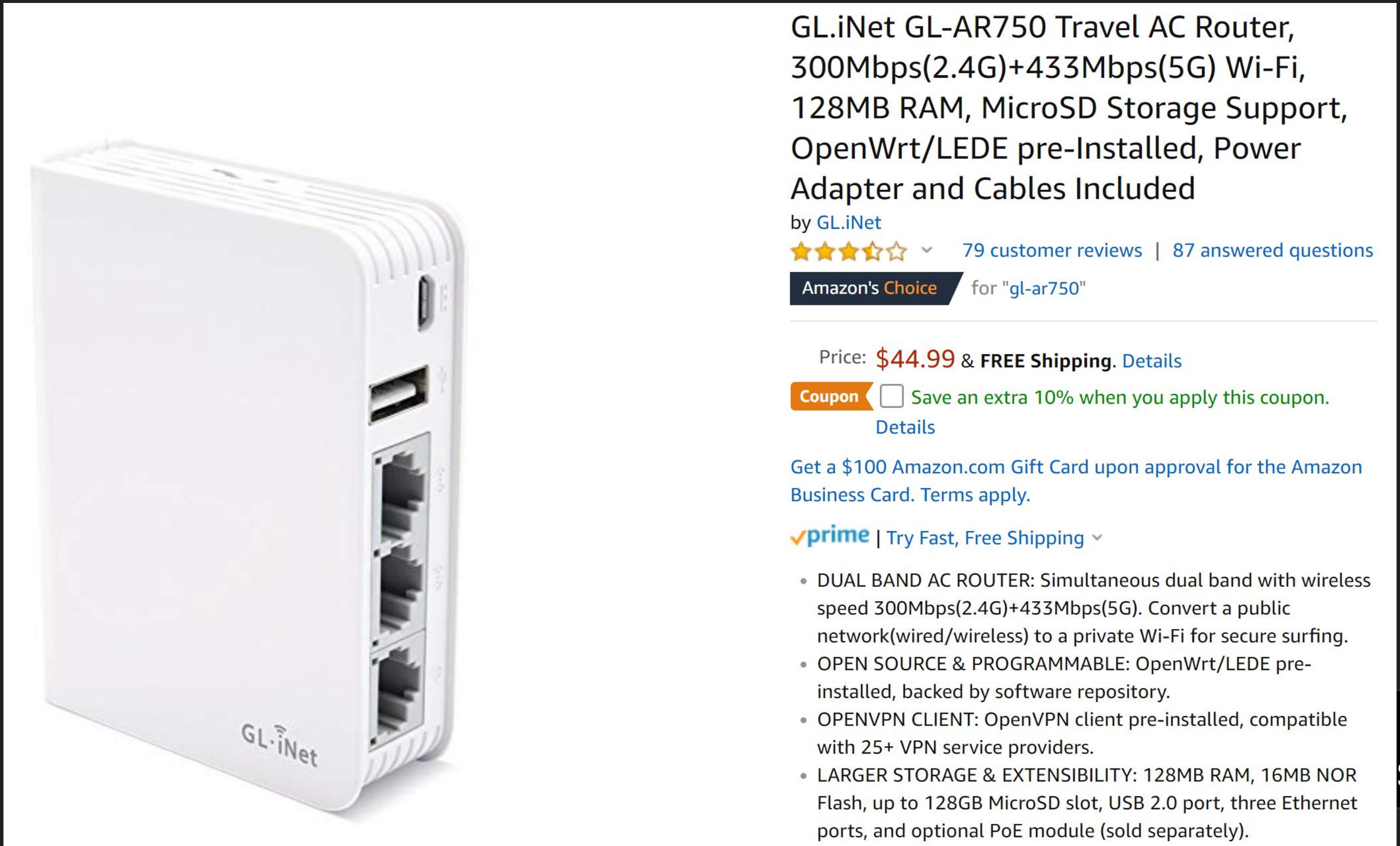
OpenWRT as a Hardware Sensor, Router, VPN

@ BSides Augusta 2018
http://bit.ly/2DBB1O4

OpenWrt
Wireless Freedom

Spotlight
Cybersecurity

OpenWRT - GL.iNet GL-AR750 Travel Router



GL.iNet GL-AR750 Travel AC Router, 300Mbps(2.4G)+433Mbps(5G) Wi-Fi, 128MB RAM, MicroSD Storage Support, OpenWrt/LEDE pre-Installed, Power Adapter and Cables Included

by GL.iNet

★★★⯪☆ 79 customer reviews | 87 answered questions

Amazon's Choice for "gl-ar750"

Price: $44.99 & **FREE Shipping**. Details

Coupon □ Save an extra 10% when you apply this coupon. Details

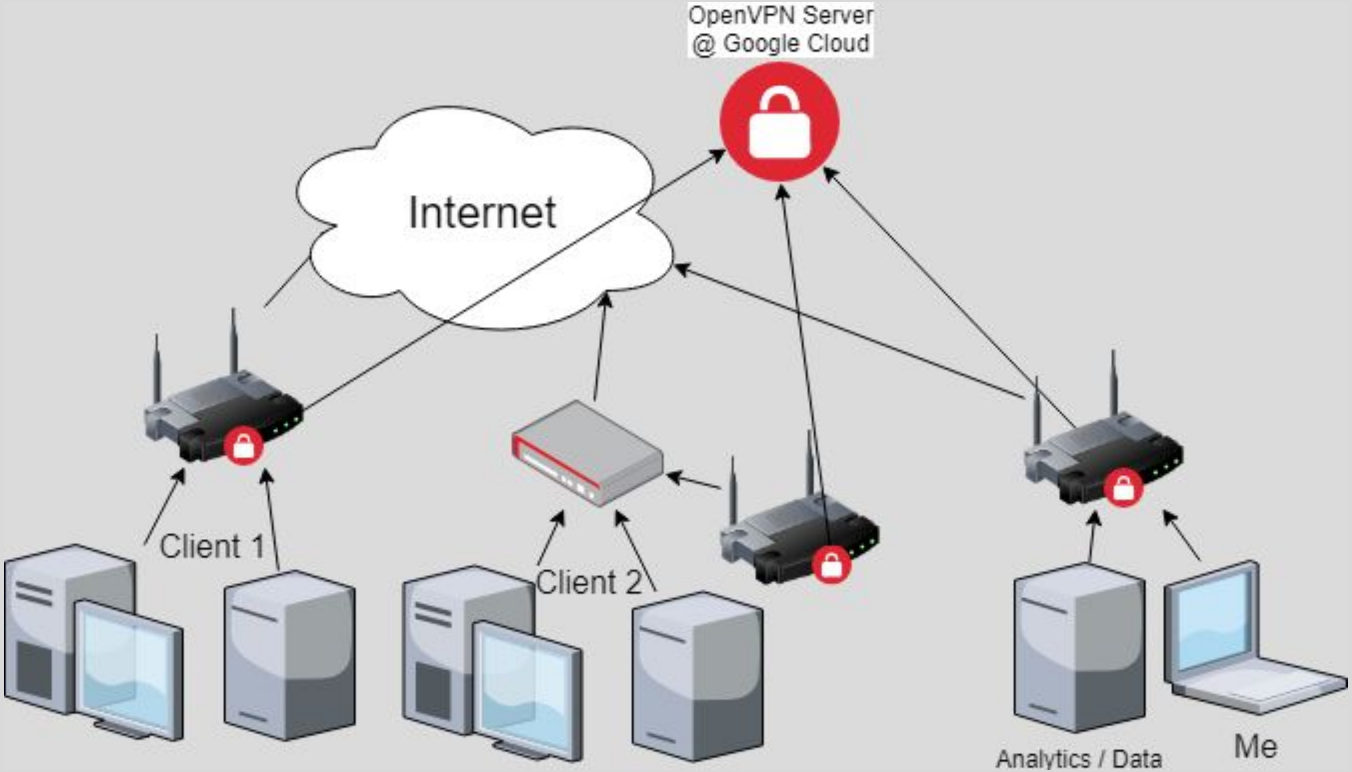
Get a $100 Amazon.com Gift Card upon approval for the Amazon Business Card. Terms apply.

✓prime | Try Fast, Free Shipping

- DUAL BAND AC ROUTER: Simultaneous dual band with wireless speed 300Mbps(2.4G)+433Mbps(5G). Convert a public network(wired/wireless) to a private Wi-Fi for secure surfing.
- OPEN SOURCE & PROGRAMMABLE: OpenWrt/LEDE pre-installed, backed by software repository.
- OPENVPN CLIENT: OpenVPN client pre-installed, compatible with 25+ VPN service providers.
- LARGER STORAGE & EXTENSIBILITY: 128MB RAM, 16MB NOR Flash, up to 128GB MicroSD slot, USB 2.0 port, three Ethernet ports, and optional PoE module (sold separately).

ight
security

The Architecture



Data Collection at the Device

Data Collected:

- Netflow (using softflowd)
- DNS queries
- Full PCAP (using daemonlogger)
- Syslog (DHCP, Wireless)
- ARP (IPs/MACs)

Planned Collection:

- Wireless Surveys, Rogue AP Detection

Sample Data Collection - ARP, DHCP Leases

```
#!/bin/sh

TMPDIR="/data/log"
DESTDIR="/data/pickup"

if [[ -f /proc/net/arp ]]; then
FNPREFIX="arp"
BASEFN="${FNPREFIX}_`date +%Y%m%d_%H%M%S`.log"
cat /proc/net/arp > "$TMPDIR/$BASEFN"
mv "$TMPDIR/$BASEFN" "$DESTDIR/$BASEFN"
fi

if [[ -f /tmp/dhcp.leases ]]; then
FNPREFIX="dnsmasqdhcp"
BASEFN="${FNPREFIX}_`date +%Y%m%d_%H%M%S`.log"
cat /tmp/dhcp.leases > "$TMPDIR/$BASEFN"
mv "$TMPDIR/$BASEFN" "$DESTDIR/$BASEFN"
fi
```

VPN Server

Hosted on Google Compute Engine

Google Cloud Platform

Google’s Container-Optimized OS -

semi-immutable Linux image optimized for running Docker containers

A Quick Intro to Google Cloud Platform

Rent storage and computer and pay for only what you use. All hardware maintenance is abstracted away. Some software maintenance is too.

AWS and Azure both have similar options and similar “freebies”

Free Trial (with credit card) - 12 Months - $300 free credit

Some “Always Free” services:

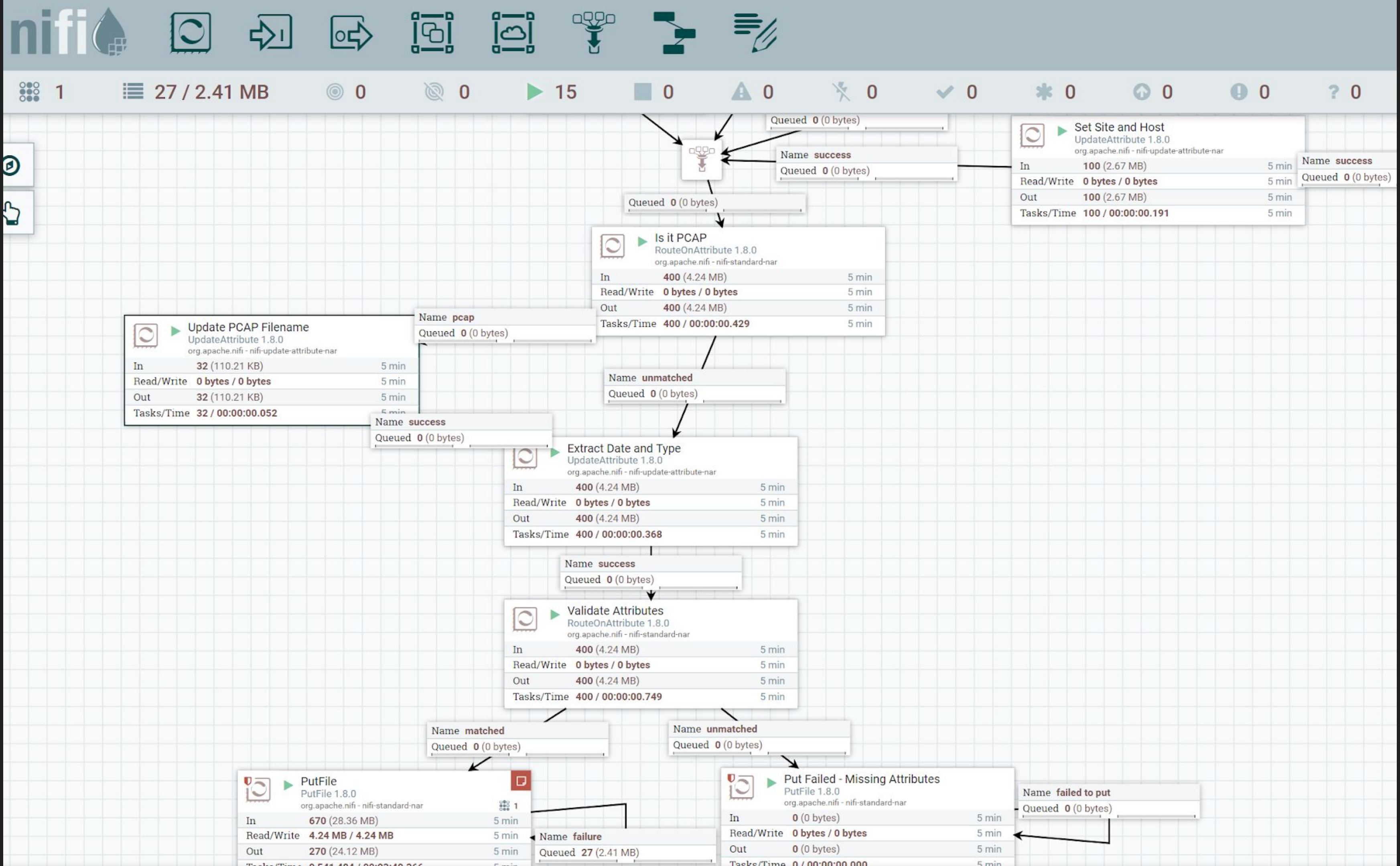
- Google Compute Engine: 1 micro instance with 30 GB HDD
- Google Cloud Storage: 5GB
- Google Cloud Source Repositories: private git repos for <=5 users & <50GB

Data Transport to Analytic Server

2 Methods:

1) Pull (via ssh to endpoint)
   Using Apache NiFi in
   a Docker container

2) Push/pull using Surety



Queued 0 (0 bytes)

Name success
Queued 0 (0 bytes)

Set Site and Host
UpdateAttribute 1.8.0
org.apache.nifi - nifi-update-attribute-nar

In	100 (2.67 MB)	5 min
Read/Write	0 bytes / 0 bytes	5 min
Out	100 (2.67 MB)	5 min
Tasks/Time	100 / 00:00:00.191	5 min

Name success
Queued 0 (0 bytes)

Queued 0 (0 bytes)

Is it PCAP
RouteOnAttribute 1.8.0
org.apache.nifi - nifi-standard-nar

In	400 (4.24 MB)	5 min
Read/Write	0 bytes / 0 bytes	5 min
Out	400 (4.24 MB)	5 min
Tasks/Time	400 / 00:00:00.429	5 min

Update PCAP Filename
UpdateAttribute 1.8.0
org.apache.nifi - nifi-update-attribute-nar

In	32 (110.21 KB)	5 min
Read/Write	0 bytes / 0 bytes	5 min
Out	32 (110.21 KB)	5 min
Tasks/Time	32 / 00:00:00.052	5 min

Name pcap
Queued 0 (0 bytes)

Name unmatched
Queued 0 (0 bytes)

Name success
Queued 0 (0 bytes)

Extract Date and Type
UpdateAttribute 1.8.0
org.apache.nifi - nifi-update-attribute-nar

In	400 (4.24 MB)	5 min
Read/Write	0 bytes / 0 bytes	5 min
Out	400 (4.24 MB)	5 min
Tasks/Time	400 / 00:00:00.368	5 min

Name success
Queued 0 (0 bytes)

Validate Attributes
RouteOnAttribute 1.8.0
org.apache.nifi - nifi-standard-nar

In	400 (4.24 MB)	5 min
Read/Write	0 bytes / 0 bytes	5 min
Out	400 (4.24 MB)	5 min
Tasks/Time	400 / 00:00:00.749	5 min

Name matched
Queued 0 (0 bytes)

Name unmatched
Queued 0 (0 bytes)

PutFile
PutFile 1.8.0
org.apache.nifi - nifi-standard-nar
1

In	670 (28.36 MB)	5 min
Read/Write	4.24 MB / 4.24 MB	5 min
Out	270 (24.12 MB)	5 min

Name failure
Queued 27 (2.41 MB)

Put Failed - Missing Attributes
PutFile 1.8.0
org.apache.nifi - nifi-standard-nar

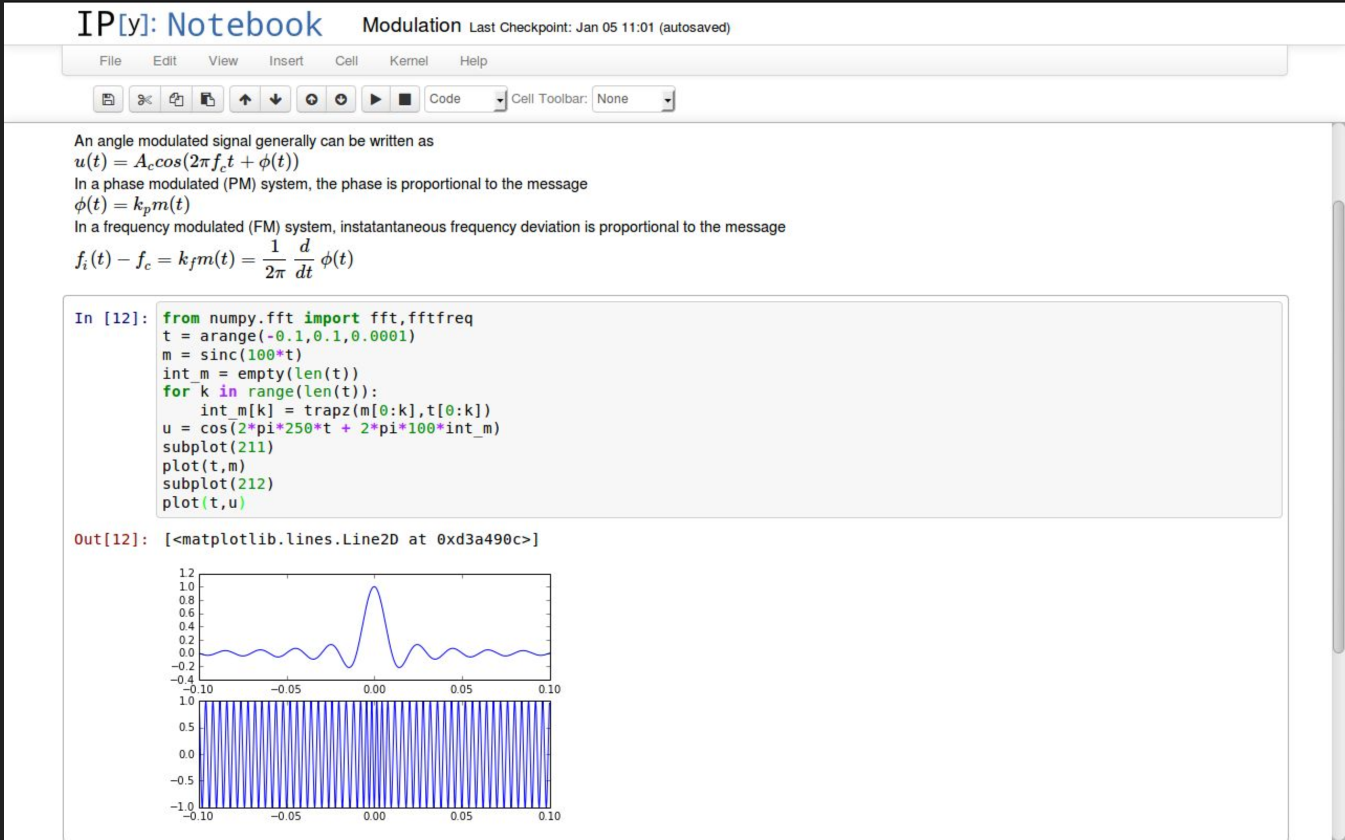
In	0 (0 bytes)	5 min
Read/Write	0 bytes / 0 bytes	5 min
Out	0 (0 bytes)	5 min

Name failed to put
Queued 0 (0 bytes)

Analytics - Surety

What if the documentation and analytics could live together?

Jupyter Notebook does something like this for data exploration & the data science community



An angle modulated signal generally can be written as

$u(t) = A_c cos(2\pi f_c t + \phi(t))$

In a phase modulated (PM) system, the phase is proportional to the message

$\phi(t) = k_p m(t)$

In a frequency modulated (FM) system, instatantaneous frequency deviation is proportional to the message

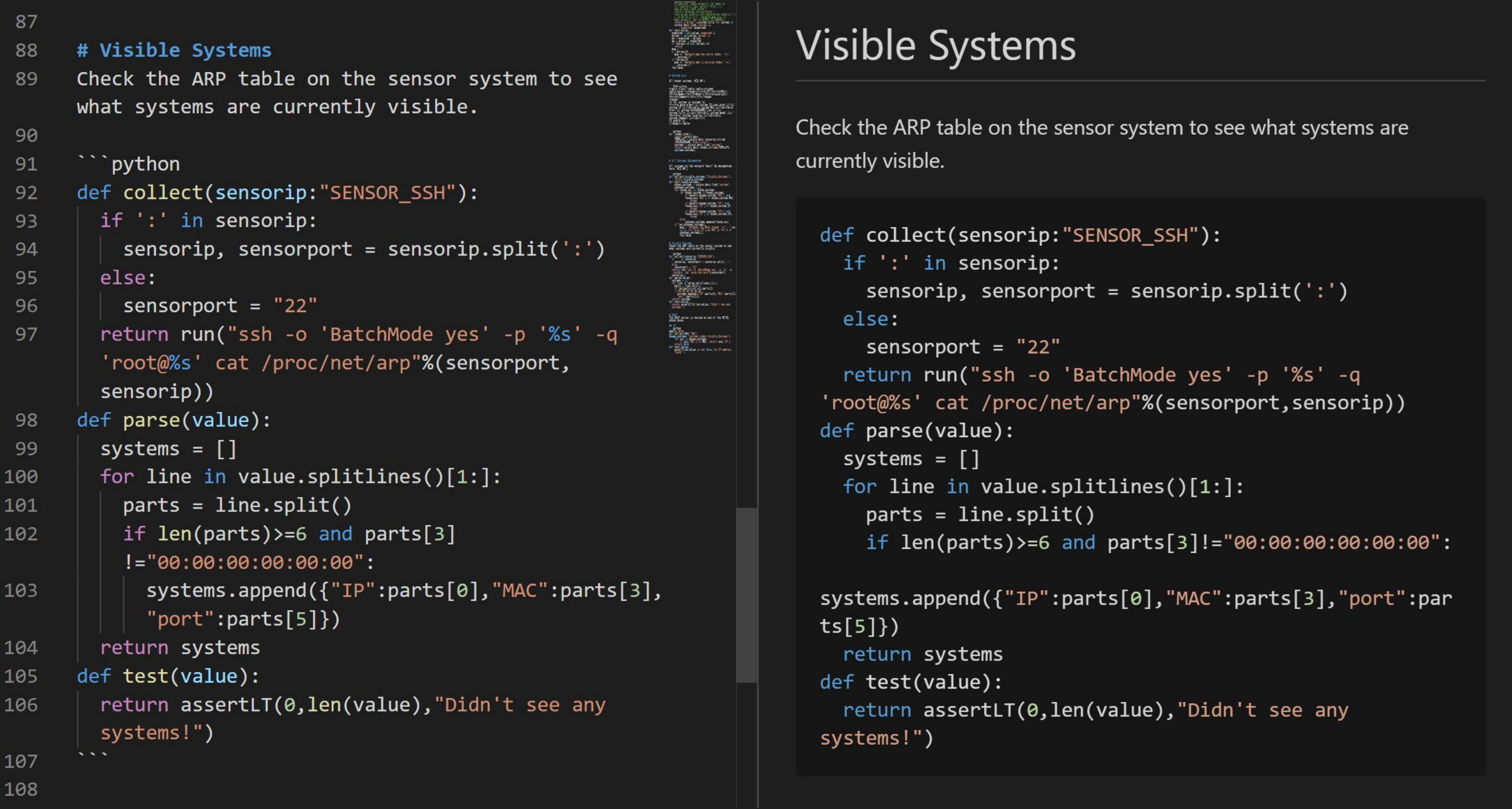
$$f_i(t) - f_c = k_f m(t) = \frac{1}{2\pi} \frac{d}{dt} \phi(t)$$

In [12]:

```
from numpy.fft import fft,fftfreq
t = arange(-0.1,0.1,0.0001)
m = sinc(100*t)
int_m = empty(len(t))
for k in range(len(t)):
    int_m[k] = trapz(m[0:k],t[0:k])
u = cos(2*pi*250*t + 2*pi*100*int_m)
subplot(211)
plot(t,m)
subplot(212)
plot(t,u)
```

Out[12]:

```
[<matplotlib.lines.Line2D at 0xd3a490c>]
```



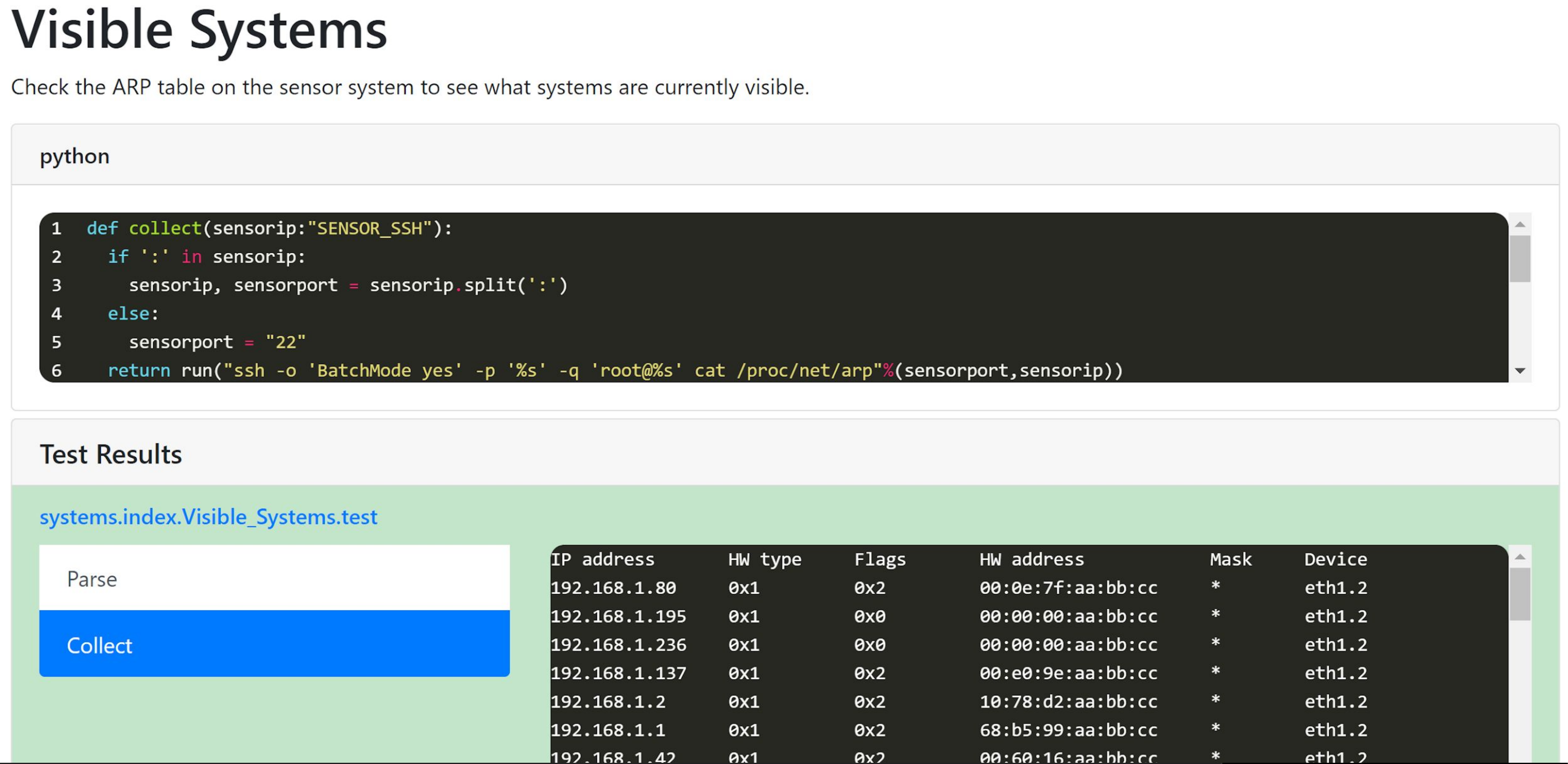
~~~
# Visible Systems
Check the ARP table on the sensor system to see what systems are currently visible.

```python
def collect(sensorip:"SENSOR_SSH"):
  if ':' in sensorip:
    sensorip, sensorport = sensorip.split(':')
  else:
    sensorport = "22"
  return run("ssh -o 'BatchMode yes' -p '%s' -q 'root@%s' cat /proc/net/arp"%(sensorport,sensorip))
def parse(value):
  systems = []
  for line in value.splitlines()[1:]:
    parts = line.split()
    if len(parts)>=6 and parts[3]!="00:00:00:00:00:00":
      systems.append({"IP":parts[0],"MAC":parts[3],"port":parts[5]})
  return systems
def test(value):
  return assertLT(0,len(value),"Didn't see any systems!")
```
~~~

Visible Systems

Check the ARP table on the sensor system to see what systems are currently visible.

```
def collect(sensorip:"SENSOR_SSH"):
  if ':' in sensorip:
    sensorip, sensorport = sensorip.split(':')
  else:
    sensorport = "22"
  return run("ssh -o 'BatchMode yes' -p '%s' -q 'root@%s' cat /proc/net/arp"%(sensorport,sensorip))
def parse(value):
  systems = []
  for line in value.splitlines()[1:]:
    parts = line.split()
    if len(parts)>=6 and parts[3]!="00:00:00:00:00:00":
      systems.append({"IP":parts[0],"MAC":parts[3],"port":parts[5]})
  return systems
def test(value):
  return assertLT(0,len(value),"Didn't see any systems!")
```



Visible Systems

Check the ARP table on the sensor system to see what systems are currently visible.

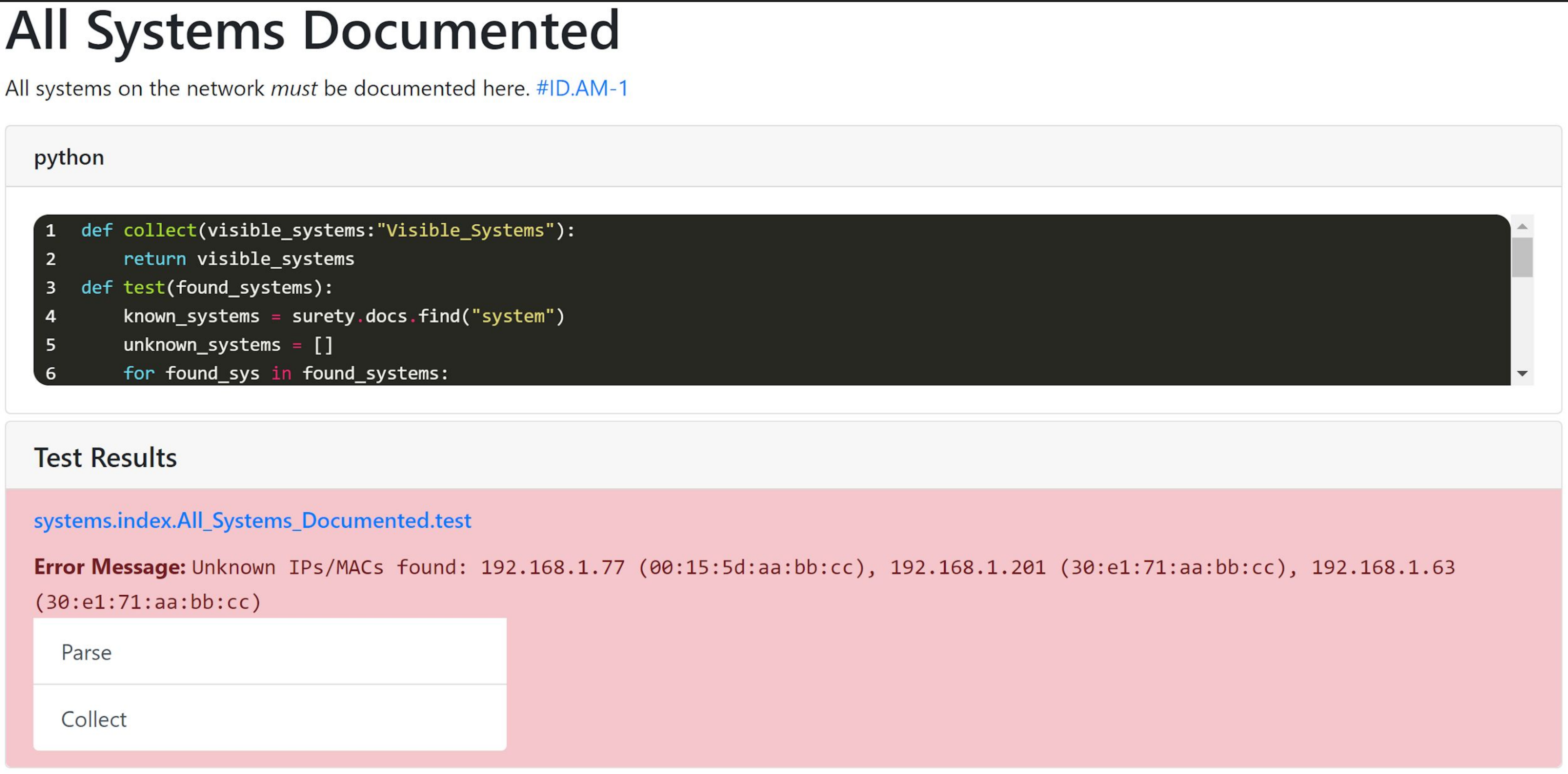
python

```python
def collect(sensorip:"SENSOR_SSH"):
  if ':' in sensorip:
    sensorip, sensorport = sensorip.split(':')
  else:
    sensorport = "22"
  return run("ssh -o 'BatchMode yes' -p '%s' -q 'root@%s' cat /proc/net/arp"%(sensorport,sensorip))
```

Test Results

systems.index.Visible_Systems.test

```
IP address       HW type     Flags       HW address            Mask     Device
192.168.1.80     0x1         0x2         00:0e:7f:aa:bb:cc     *        eth1.2
192.168.1.195    0x1         0x0         00:00:00:aa:bb:cc     *        eth1.2
192.168.1.236    0x1         0x0         00:00:00:aa:bb:cc     *        eth1.2
192.168.1.137    0x1         0x2         00:e0:9e:aa:bb:cc     *        eth1.2
192.168.1.2      0x1         0x2         10:78:d2:aa:bb:cc     *        eth1.2
192.168.1.1      0x1         0x2         68:b5:99:aa:bb:cc     *        eth1.2
192.168.1.42     0x1         0x2         00:60:16:aa:bb:cc     *        eth1.2
```



All Systems Documented

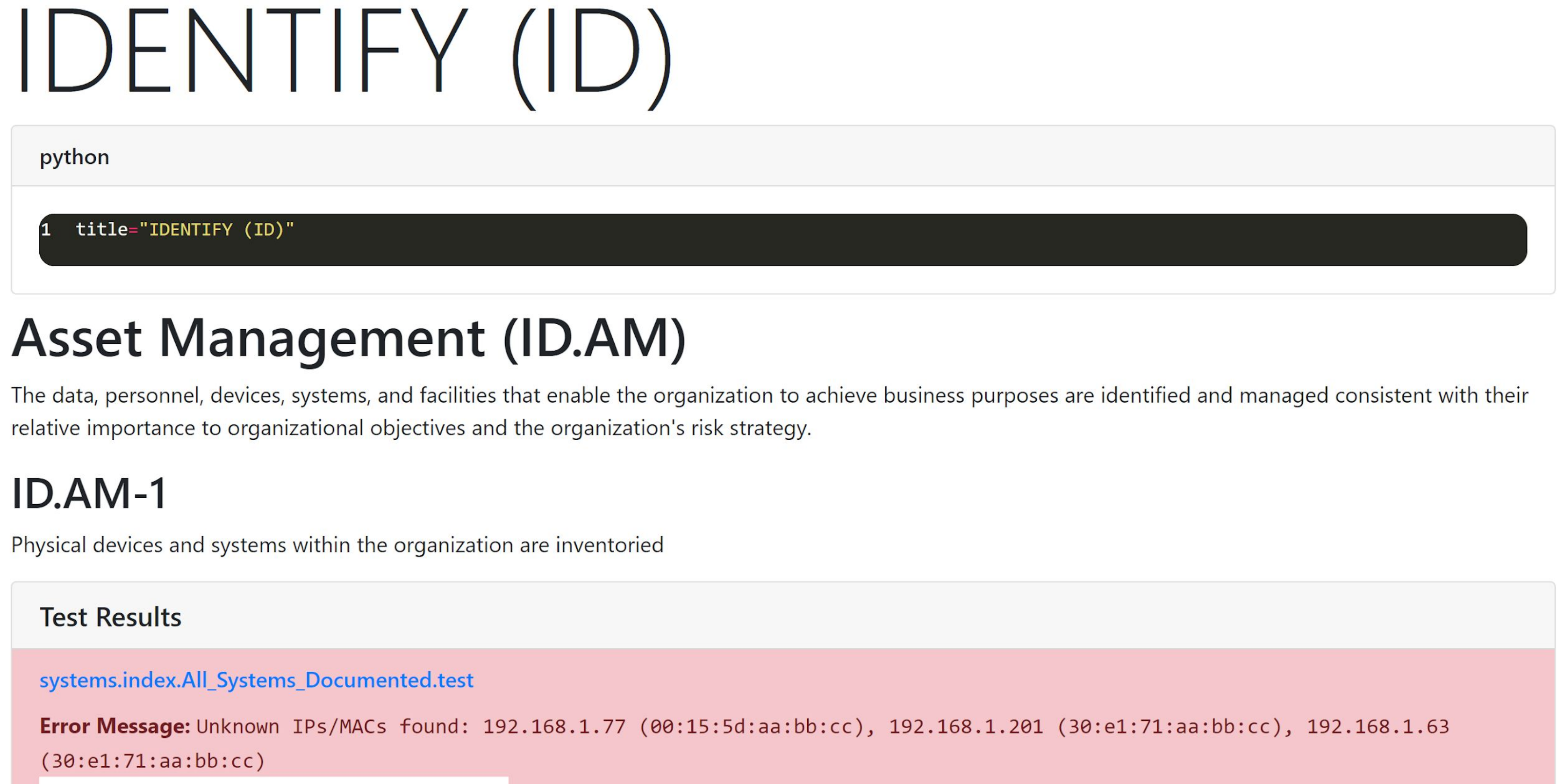
All systems on the network *must* be documented here. #ID.AM-1

```python
def collect(visible_systems:"Visible_Systems"):
    return visible_systems
def test(found_systems):
    known_systems = surety.docs.find("system")
    unknown_systems = []
    for found_sys in found_systems:
```

Test Results

systems.index.All_Systems_Documented.test

Error Message: `Unknown IPs/MACs found: 192.168.1.77 (00:15:5d:aa:bb:cc), 192.168.1.201 (30:e1:71:aa:bb:cc), 192.168.1.63 (30:e1:71:aa:bb:cc)`



IDENTIFY (ID)

python

```python
title="IDENTIFY (ID)"
```

Asset Management (ID.AM)

The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.

ID.AM-1

Physical devices and systems within the organization are inventoried

Test Results

systems.index.All_Systems_Documented.test

Error Message: `Unknown IPs/MACs found: 192.168.1.77 (00:15:5d:aa:bb:cc), 192.168.1.201 (30:e1:71:aa:bb:cc), 192.168.1.63 (30:e1:71:aa:bb:cc)`

Authorized Software

Verify that each Windows system ONLY has authorized software packages installed. #ID.AM-2

powershell

```
# pull from the "official" source (which seems to be missing a bunch)
$a = (get-ciminstance win32_product | select-object Name,Version,Vendor)
# now check the 64 and 32 bit registry locations for more options
$b = (get-itemproperty HKLM:\software\microsoft\Windows\CurrentVersion\Uninstall\* | select-object @{N="Name";E={$_.DisplayName}}, @{N="V
$c = (get-itemproperty HKLM:\software\wow6432node\microsoft\Windows\CurrentVersion\Uninstall\* | select-object @{N="Name";E={$_.DisplayNa
```

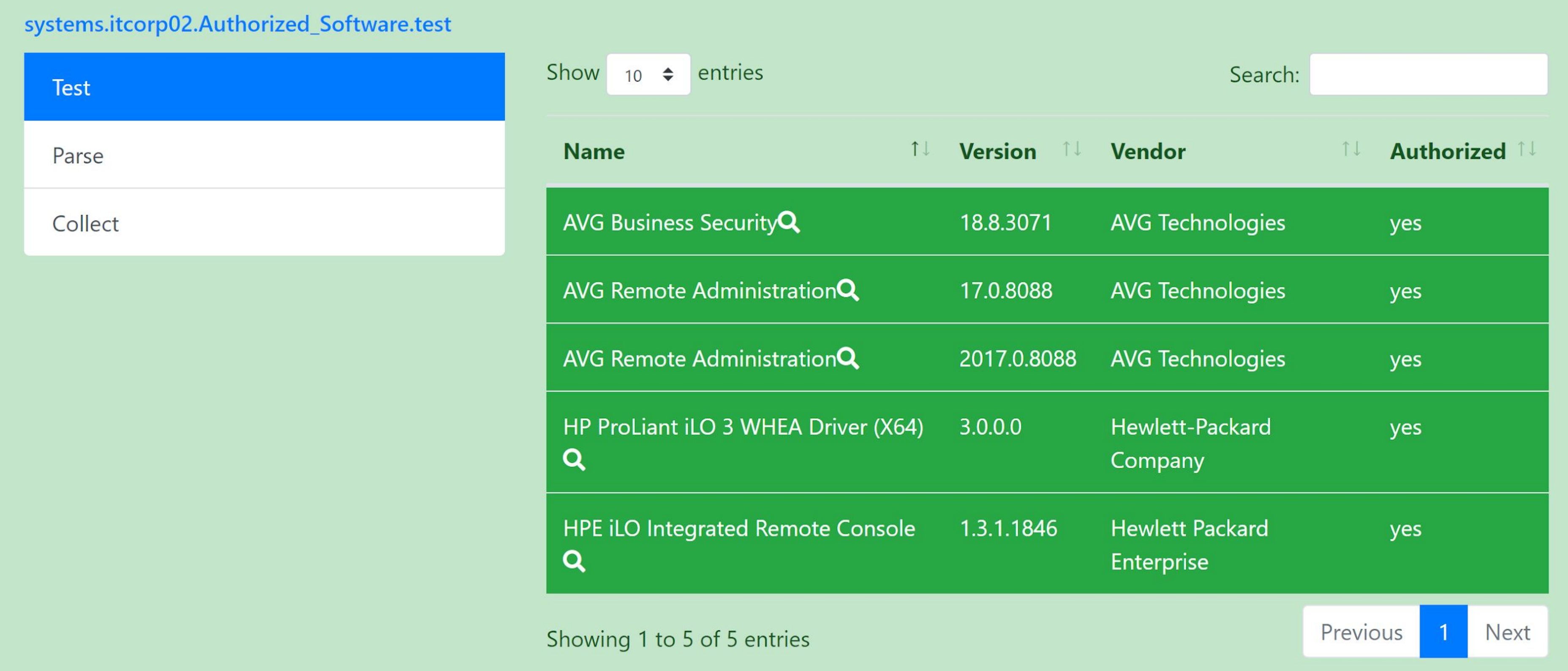
python

```
    for software in value:
        if not  _isAuthorized(software):
            # we didn't match anything authorized...
            unauthorized.append(software)
    assertEqual(0, len(unauthorized))
```

s

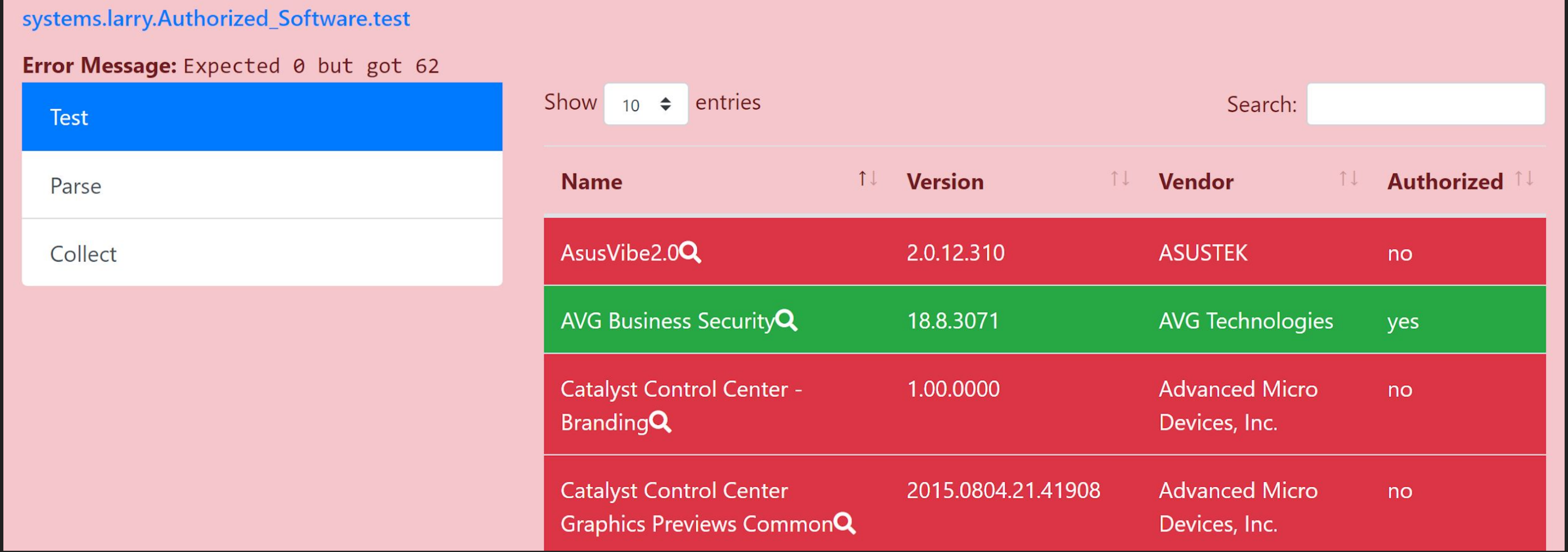
html+jinja

```
<table class="table"><thead><tr><th>Name</th><th>Version</th><th>Vendor</th><th>Authorized</th></thead><tbody>
{% for s in software %}
```



Name	Version	Vendor	Authorized
AVG Business Security🔍	18.8.3071	AVG Technologies	yes
AVG Remote Administration🔍	17.0.8088	AVG Technologies	yes
AVG Remote Administration🔍	2017.0.8088	AVG Technologies	yes
HP ProLiant iLO 3 WHEA Driver (X64) 🔍	3.0.0.0	Hewlett-Packard Company	yes
HPE iLO Integrated Remote Console 🔍	1.3.1.1846	Hewlett Packard Enterprise	yes

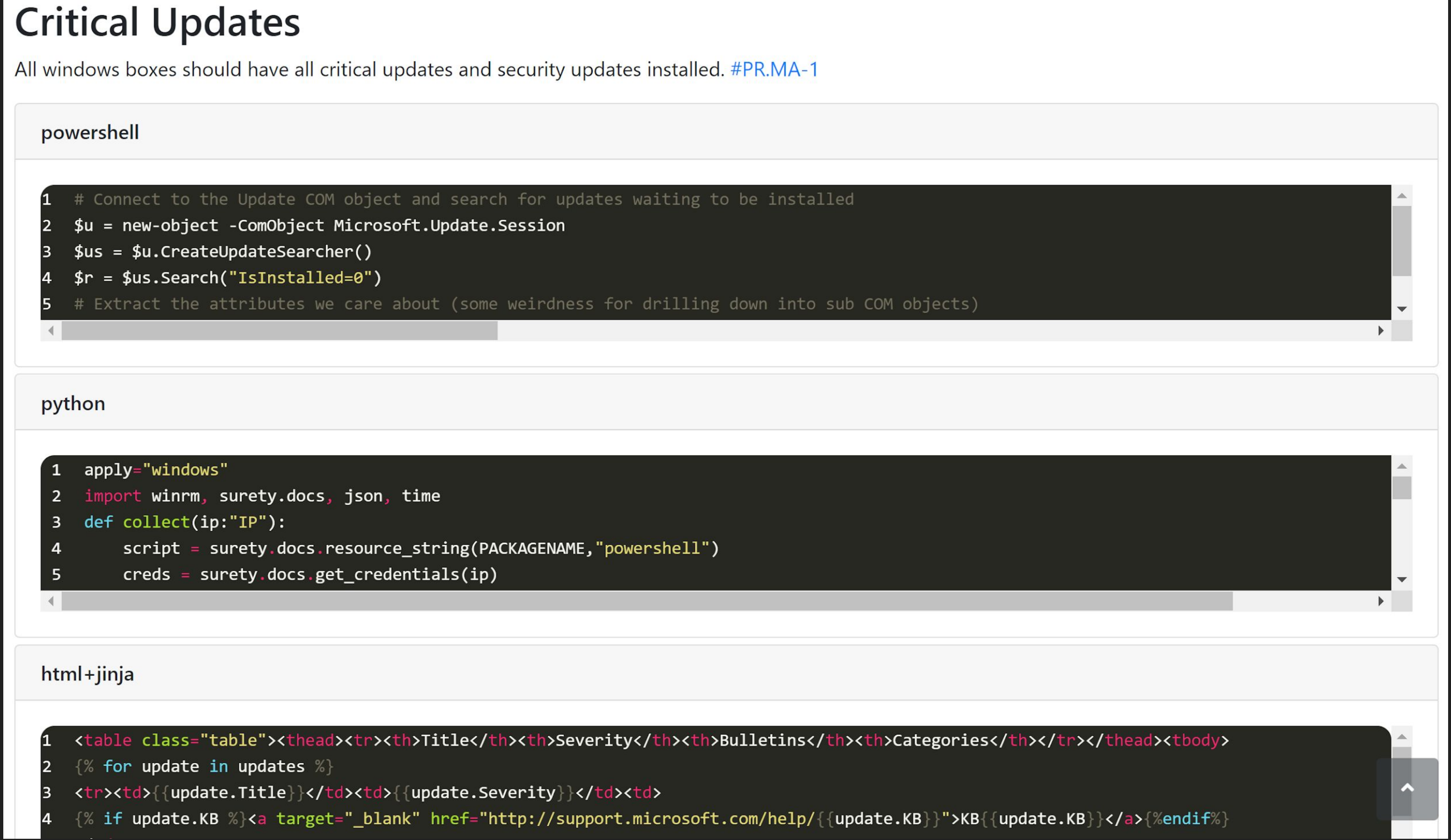
Showing 1 to 5 of 5 entries



systems.larry.Authorized_Software.test

Error Message: `Expected 0 but got 62`

Name	Version	Vendor	Authorized
AsusVibe2.0🔍	2.0.12.310	ASUSTEK	no
AVG Business Security🔍	18.8.3071	AVG Technologies	yes
Catalyst Control Center - Branding🔍	1.00.0000	Advanced Micro Devices, Inc.	no
Catalyst Control Center Graphics Previews Common🔍	2015.0804.21.41908	Advanced Micro Devices, Inc.	no



Critical Updates

All windows boxes should have all critical updates and security updates installed. #PR.MA-1

powershell

```
# Connect to the Update COM object and search for updates waiting to be installed
$u = new-object -ComObject Microsoft.Update.Session
$us = $u.CreateUpdateSearcher()
$r = $us.Search("IsInstalled=0")
# Extract the attributes we care about (some weirdness for drilling down into sub COM objects)
```

python

```
apply="windows"
import winrm, surety.docs, json, time
def collect(ip:"IP"):
    script = surety.docs.resource_string(PACKAGENAME,"powershell")
    creds = surety.docs.get_credentials(ip)
```

html+jinja

```
<table class="table"><thead><tr><th>Title</th><th>Severity</th><th>Bulletins</th><th>Categories</th></tr></thead><tbody>
{% for update in updates %}
<tr><td>{{update.Title}}</td><td>{{update.Severity}}</td><td>
{% if update.KB %}<a target="_blank" href="http://support.microsoft.com/help/{{update.KB}}">KB{{update.KB}}</a>{%endif%}
```

What’s next?

- Surety Improvements
  - Surety as online web app
  - Small, python-based endpoint agent to pull code, run it, push result back to server
  - History - look back at previously stored values
- Move all NiFi-pulled data to Surety (then all data collected will be documented and stored in same place!)

Components of a Continuous Monitoring System

- Documentation
  - What are we protecting
  - Client Policies - descriptions of what the system should look like and how the system (and the users!) should behave
- Data
  - Hardware Sensors/TAPs - gather network data
  - Software Agents - gather system data
- Data Storage - securely store data
- Data Transport - securely get data from the client's systems back to yours
- Analysis Servers - out-of-band place to run analytics on the data
- Analytics - what to look for in the data

Like what you saw? Want to join me?
Contact me!

@SpotlightCybsec

Spotlight
Cybersecurity