ars TECHNICA

BIZ & IT TECH SCIENCE POLICY CARS GAMING &

GEEK SQUAD —

Inmates built computers hidden ceiling, connected them to prison network

A Rogue Raspberry Pi Found on NASA's JPL Network

By Ryan Whitwam on June 20, 2019 at 12:26 pm | Comment

ClearFocus TECHNOLOGIES

Craig Bowser

GCDA, GSEC, GCED

555 Mentor

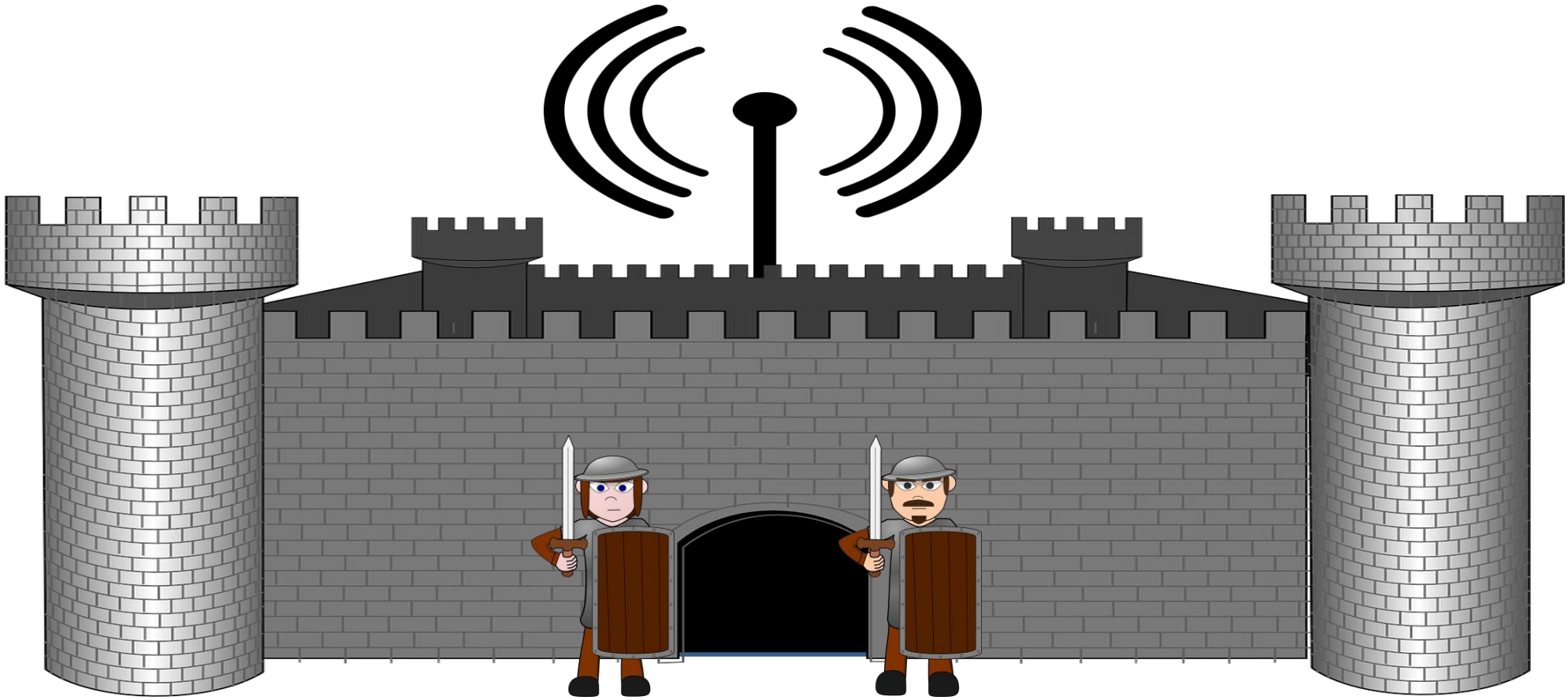
Rapid Recognition and Response to Rogues

ClearFocus TECHNOLOGIES

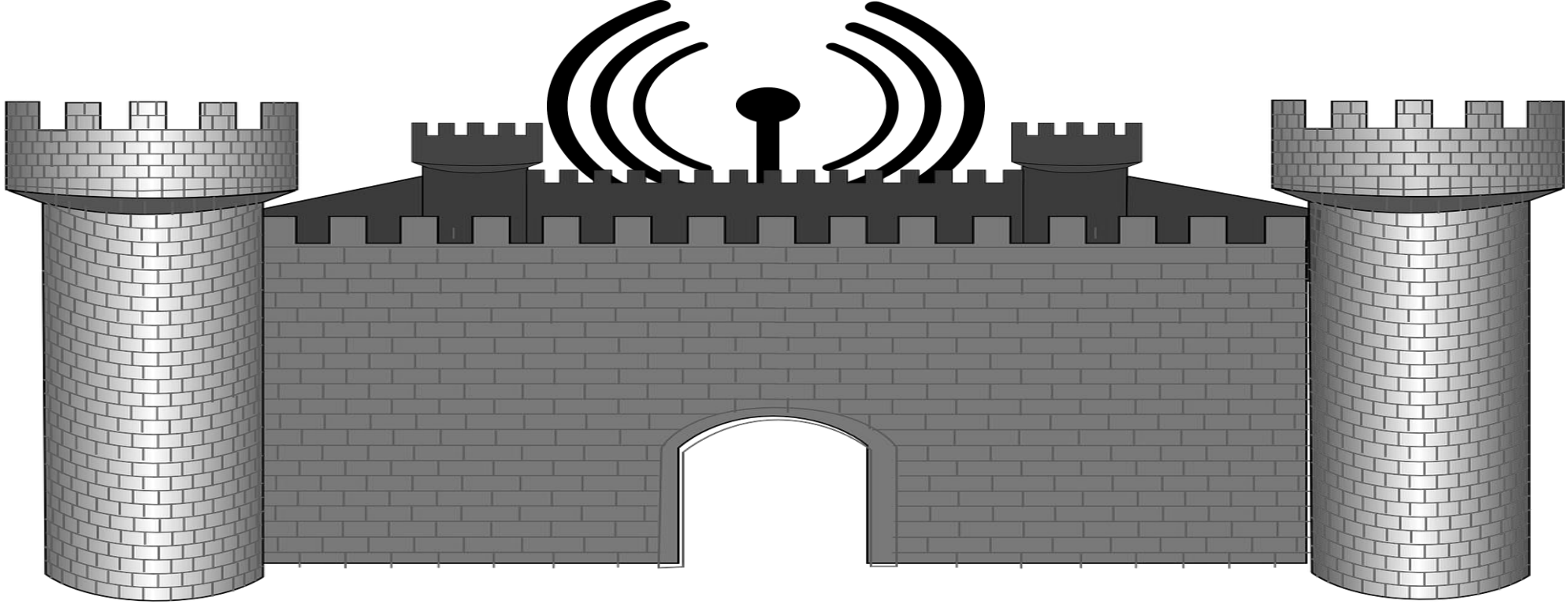
ClearFocus
TECHNOLOGIES

o by NASA on Unsplash

ClearFocus TECHNOLOGIES



ClearFocus TECHNOLOGIES



Back door

Man in the middle

Etc.

Private business

Malware Server

Sniffer

ClearFocus TECHNOLOGIES

ClearFocus TECHNOLOGIES

- Network Scans – Scan regularly and perform diffs on each scan
- Tools – Install and deploy
- Custom tools – Build, deploy and install

ClearFocus TECHNOLOGIES

Authorized Devices – Known, Approved (attributable), up to Date

Known, but outdated – Approved device, but does not have all required agents/proper configs.

Unauthorized – Know what it is and what it does, but it does not have permission to be on the network.

Unknown – Know IP, maybe know OS, ports, but not much else.

ClearFocus TECHNOLOGIES

IP & MAC & Hostname

……Maybe OS

……Maybe open ports

……Signal information… some

ClearFocus TECHNOLOGIES

1.1.1.1

OS

Open ports (w/ service guess)

MAC

Hostname

AD Membership

Possible Vendor

Results from Vulnerability Scan

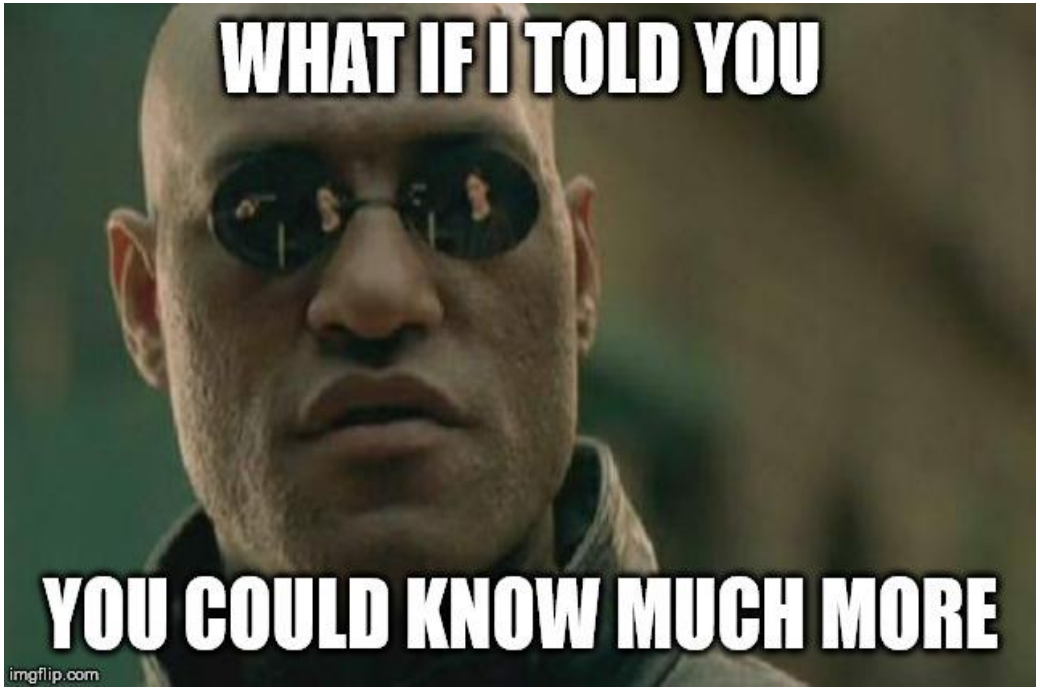
Installed Agents

Network location

Provider

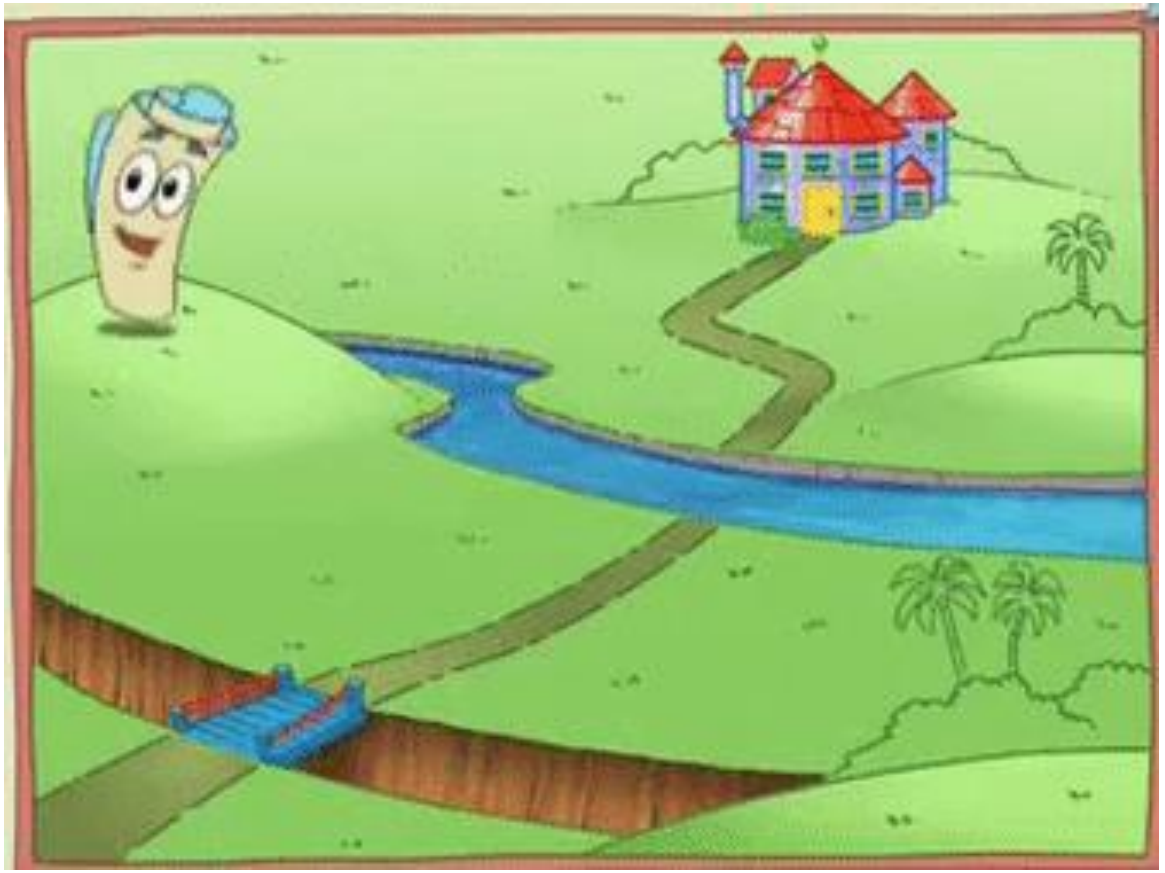
Physical location

Link to SIEM to pull up all related events related to that



ClearFocus TECHNOLOGIES

ClearFocus TECHNOLOGIES



ClearFocus TECHNOLOGIES

IP, MAC and Hostname:

DHCP, IPAM, SCCM

AD Membership:

WMI or PS query to AD

Possible vendor:

Query against MAC OUI file

Vulnerability Scan:

Query scanner API or results in SIEM

ClearFocus TECHNOLOGIES

Installed Agents:

Query tool API or compare to lookup table

Network location:

Query tool API, SNMP, or CAM tables

Provider:

Often comes with WIDS information

Physical location:

CAM tables, tool API, or approx location from WIDS

ClearFocus TECHNOLOGIES

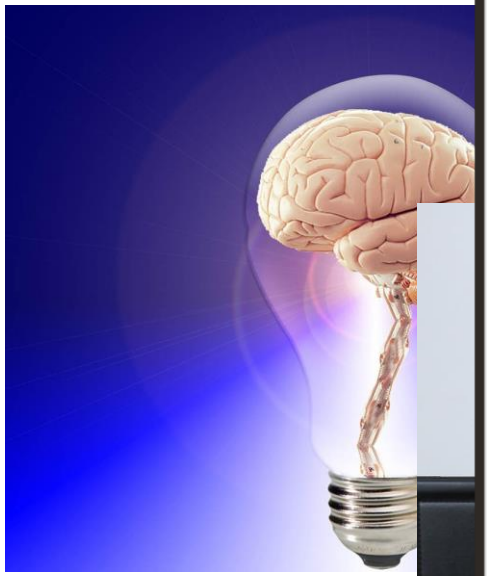
	DHCP-MAC	Date Found	DHCP-HOST	Sco	IP	Lease	VENDOR	Ping
1	00-0C-29-E4-48-10	5/26/2019	GIANTS.SCOUTS.LOCAL	Wor	192.168.1.101	####	VMWare	N
2	40-A8-F0-3E-E8-7E	5/26/2019		Wor	192.168.1.105	####	Hewlard Packard	Y
3	6C-01-A8-C0	5/26/2019	BAD_ADDRESS	Wor	192.168.1.108	####	INVALID OUI	Y
4	00-0C-29-3A-F2-60	5/26/2019	UBUNTU.SCOUTS.LOCAL	Wor	192.168.1.110	####	VMWare	Y

	P4445	C$	SAV	EPO	P80	DH	Link
1						192	http://192.168.1.106:8000/en-US/app/search/search?earliest=-7d&lat
2						192	http://192.168.1.106:8000/en-US/app/search/search?earliest=-7d&lat
3		Y				192	http://192.168.1.106:8000/en-US/app/search/search?earliest=-7d&lat
4					Y	192	http://192.168.1.106:8000/en-US/app/search/search?earliest=-7d&lat

https://github.com/ericmccullough/r2d2

ClearFocus TECHNOLOGIES

ClearFocus TECHNOLOGIES



ClearFocus TECHNOLOGIES

ClearFocus TECHNOLOGIES

Rogue Inquisitor

https://github.com/reswob10/RogueInquisitor

< logo here TBD>

ClearFocus TECHNOLOGIES

```
source2:
  name: DHCP
  filename: c:/tools/files/dhcp.csv
  MAC_Column: 1
  IP_Column:  0
  Host_Column: 2
  color: grey
  weight: 1
  enabled: 1
```

```
ports:
  - appname: Tanium
    port: 5123
    weight: 2
```

Rogue_Score: -5

Good_Score: 3

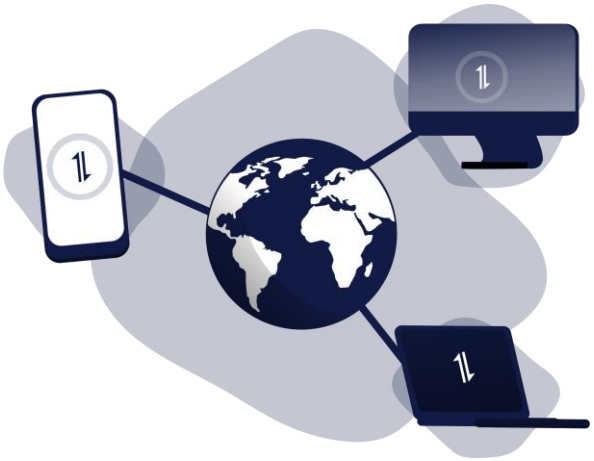
ClearFocus TECHNOLOGIES

Splunk Demo

ClearFocus TECHNOLOGIES

How do we protect our networks?

ClearFocus TECHNOLOGIES



Protections

Inventory of Known Devices
NAC/Port Security
802.1x
Physical Security
Zero Trust Model
User Education

ClearFocus TECHNOLOGIES

- Large number of possible rogues?
- Devices that have limited information?
- Can legit users/devices self remediate?

ClearFocus TECHNOLOGIES

- Tool Improvement
  - Add APIs
  - Add output options

Bryan Goff@bryangoffphoto

ClearFocus TECHNOLOGIES