

Cybersecurity Critical Path

How to Fast Track your Security Operations



About

- Matt Morton, CISM, CGEIT, CISSP
- Consultant, Vantage Technology Consulting Group
- CISO and experienced IT leader



Current State

- Survey Microsoft/Marsh
- NASCIO - #1 IT Issue 2015-2019
- CIO Magazine - #1 Issue for CIO's 2019, 2018
 - Also top investment priority in same time period
- EDUCAUSE – Cybersecurity #1 IT Issue 2019-2016, 2008
- Society of Information Management Professionals (SIM) 2018 - Cyber at the top of survey results

Declining Confidence in Results

Microsoft/Marsh 2019

- 79% of respondents ranked cyber risk as a top five concern for their organization, up from 62% in 2017.
- **Those saying they had “no confidence” increased:**
- **From 9% to 18% for understanding and assessing cyber risks.**
- **From 12% to 19% for preventing cyber threats.**
- **From 15% to 22% for responding to and recovering from cyber events.**

Rising Incidents

- Two-thirds of cyberattacks affect businesses with fewer than 1000 employees
 - *2018 Verizon Data Breach Report*
- The average cost of these cyber incidents is 1.43 million
 - *Ponemon Institute 2018 State of Cybersecurity in SMBs 2018*
- Only 17% of these businesses have a cybersecurity incident response plan
 - *Better Business Bureau "State of Cybersecurity" Report 2017*

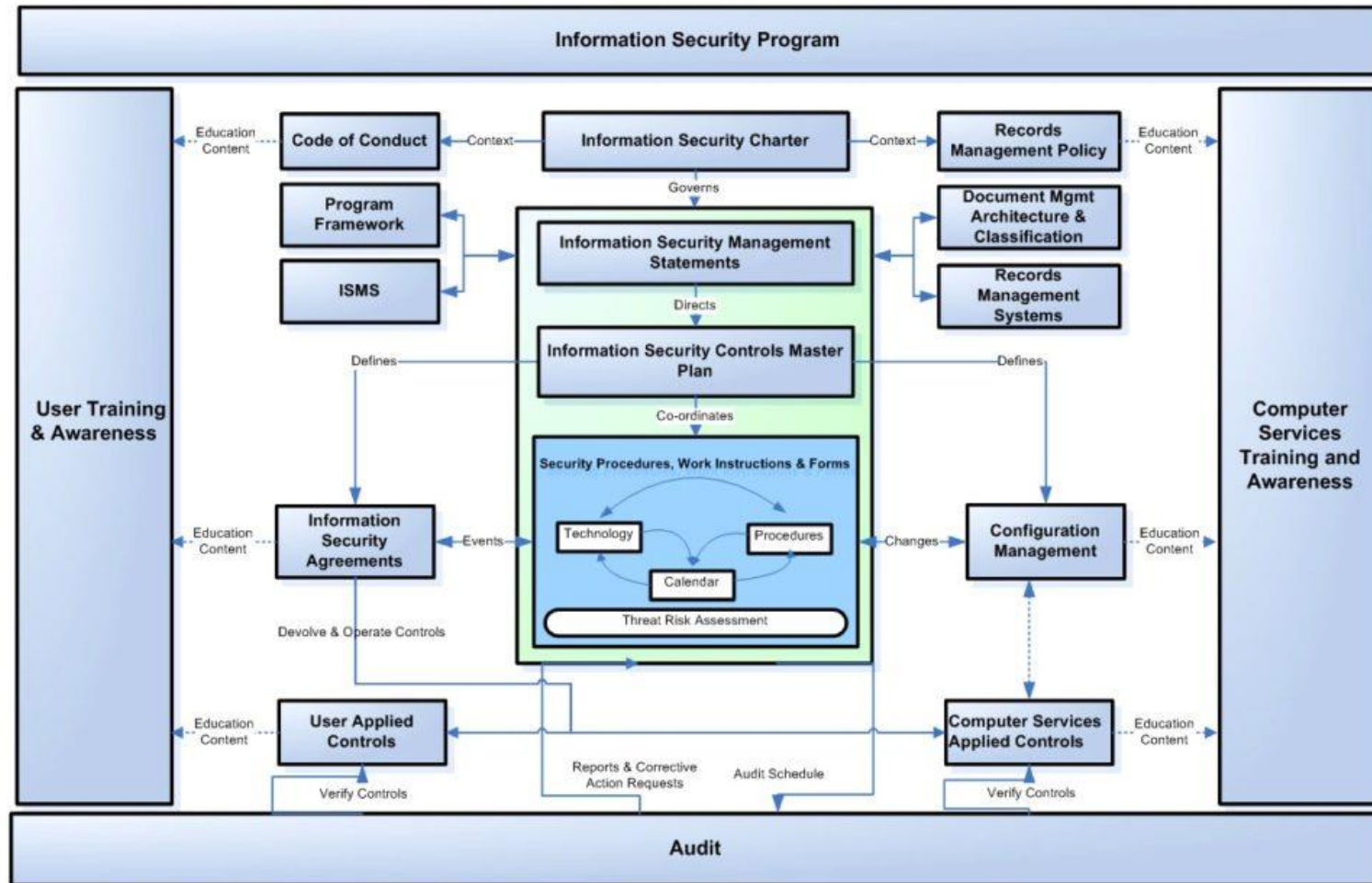
Annual Spend

Market Segment	2017	2018	2019
Application Security	2,434	2,742	3,003
Cloud Security	185	304	459
Data Security	2,563	3,063	3,524
Identity Access Management	8,823	9,768	10,578
Infrastructure Protection	12,583	14,106	15,337
Integrated Risk Management	3,949	4,347	4,712
Network Security Equipment	10,911	12,427	13,321
Other Information Security Software	1,832	2,079	2,285
Security Services	52,315	58,920	64,237
Consumer Security Software	5,948	6,395	6,661
Total	101,544	114,152	124,116
		5.8%	4.1%

In millions \$USD

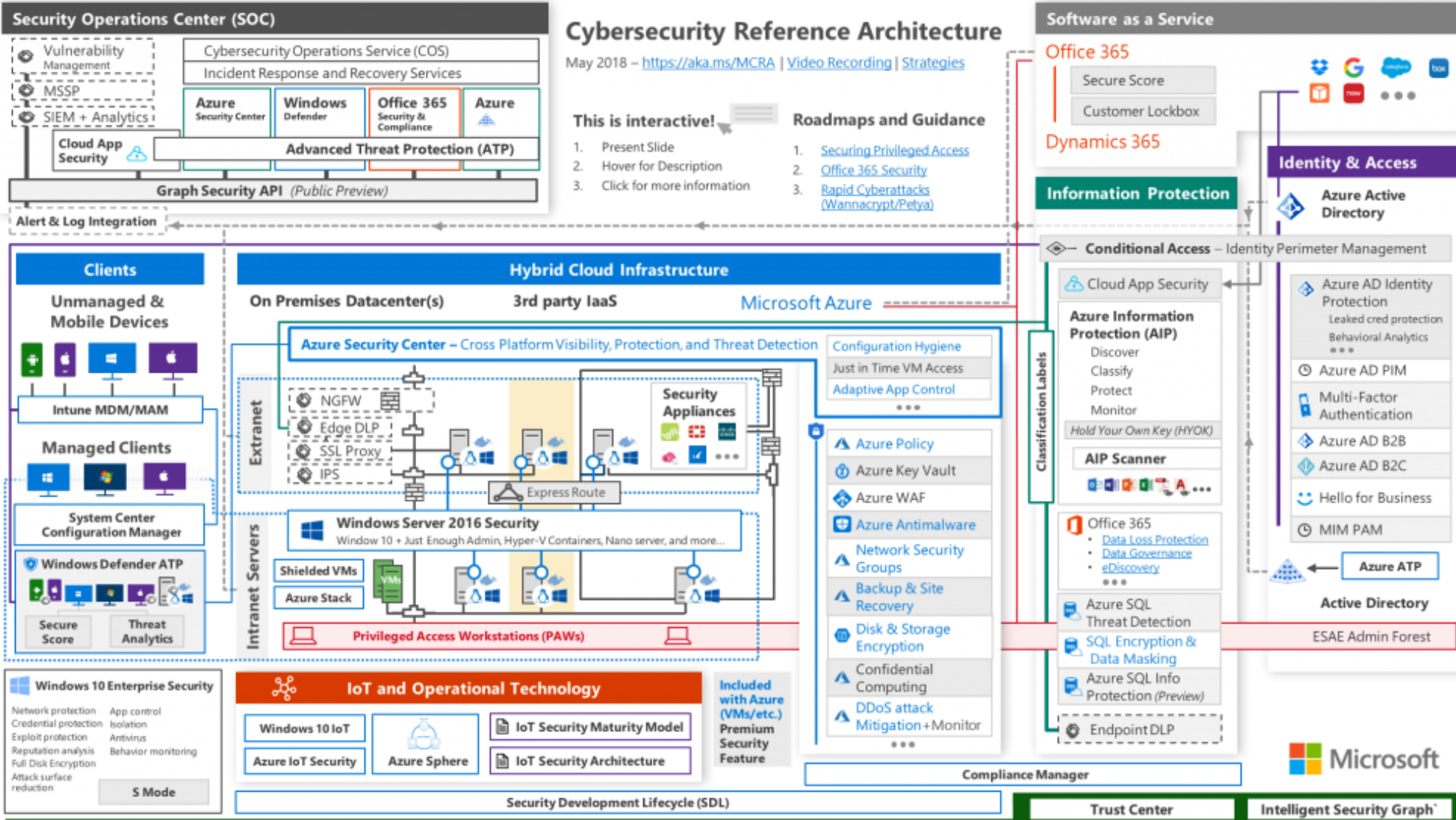
Source: Gartner (August 2018)

Security Program



Source: Information Systems Group Pty Limited. Reprinted with permission.

Security Program Technical Architecture



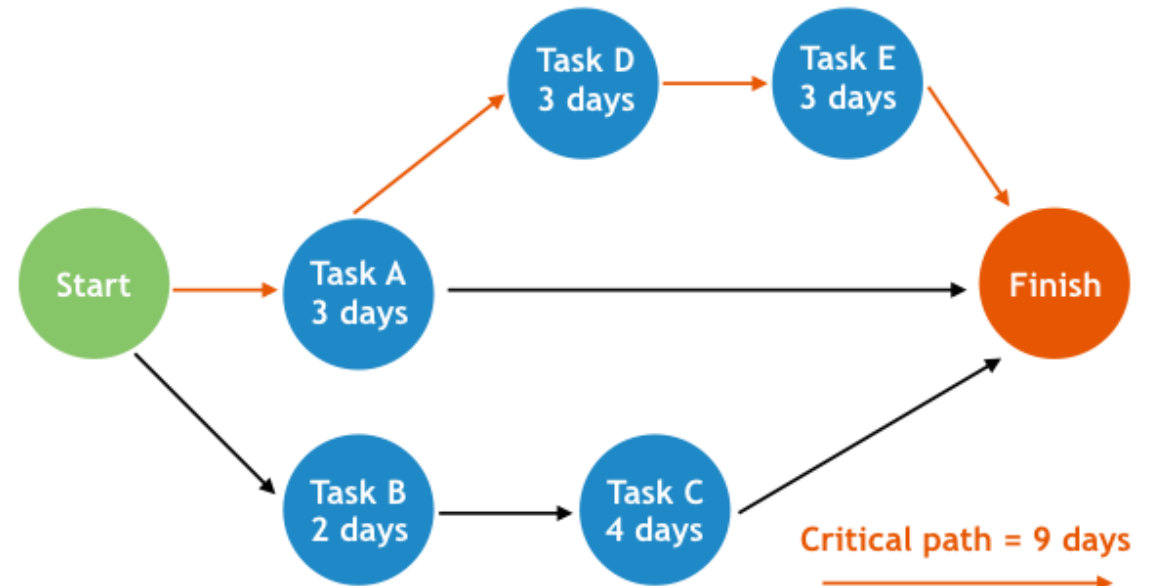
Simpler Way?

- Less complex
- More cost effective
- Easier to manage
- Easier to communicate
- Overall better results



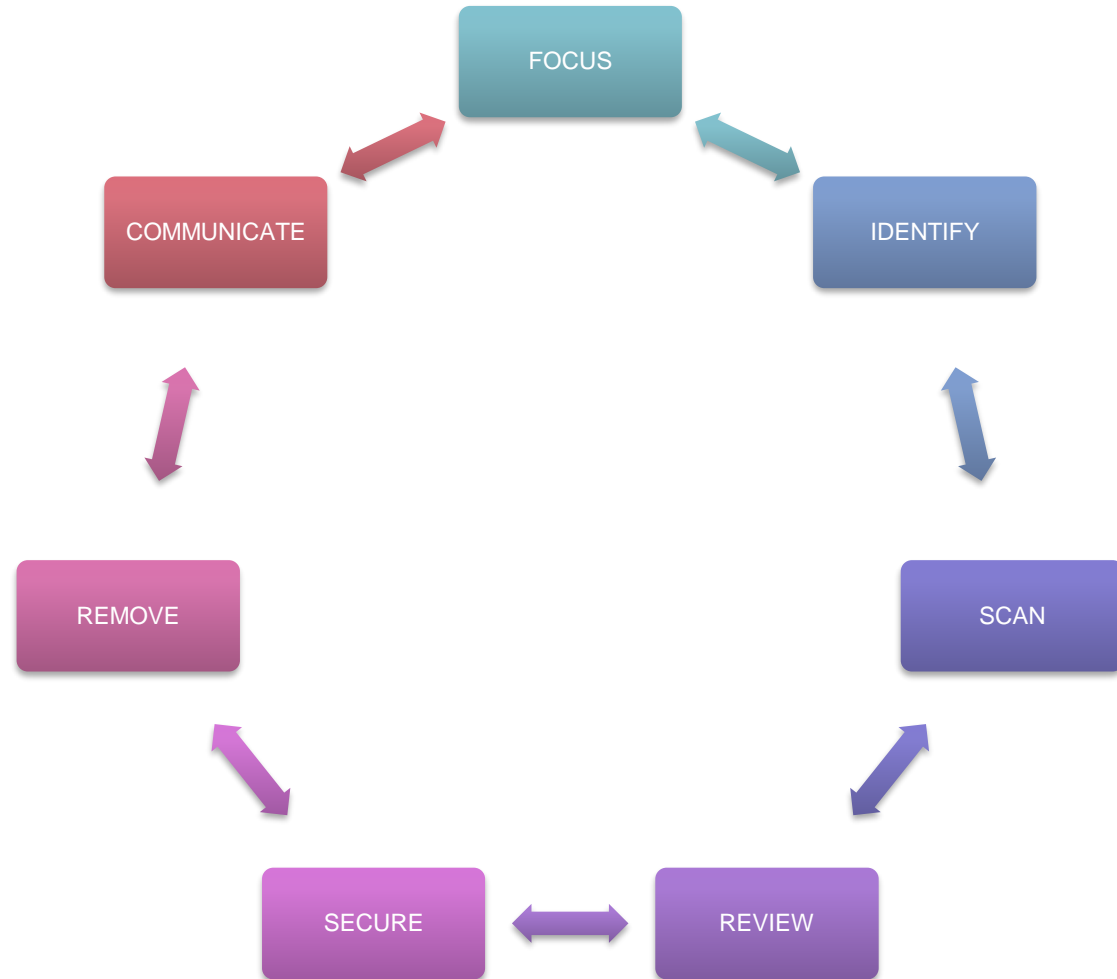
Critical Path

- What is it?
 - *The sequence of stages determining the minimum time needed for an operation, especially when analyzed on a computer for a large organization.*
- Why is it useful?
 - Focuses efforts on important tasks in getting to desired results



Critical Path for Security

- Focus
 - What you own
- Identify
 - Assets
- Scan
 - Assets
- Review
 - Logs
 - Results
 - Accounts
- Secure
- Remove
 - Assets
 - Accounts
- Communicate



Focus

- Plan teams
- Review tools
- Setup 'sprint' standups
- Setup shared storage areas
- Setup time capture tools (spreadsheet)
- Identify and acknowledge areas that will not be perfect
- Identify the scope
 - Clearly identify what you will NOT be doing!
- Set goals
 - # of assets, % scanned, % of accounts removed



Identify

- Review sources of asset information
 - Scans
 - Network scans
 - Purchase requisitions
 - Logs
- Compile asset list
- Classify assets
 - Criticality versus data stored/transmitted
- Start with those that have high criticality and high risk data

Scan

Scan . . .

- For vulnerabilities
- For high risk data (PII, etc.)
- With AV and Malware tools
- The network for activity
- Accounts
 - how are they used
- For shared credentials? (same login two IP's maybe?)

Review

- Review all the results of scanning
- Spot check review logs of highest risk assets
- Spot check accounts with access to the highest risk assets

Secure

- Identify your border(s)
- Network IP ranges
- Cloud IP ranges
- If you have no firewall then plan for installation
- Review data in next sprint
- Verify firewall is protecting highest risk assets
 - Check rules
 - Test rules

Remove

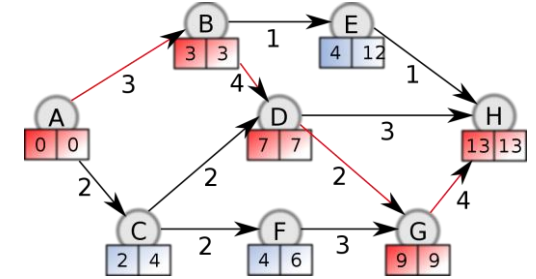
- Assets/systems/endpoints not being used
- Question everything
 - “wait, what?”
- Remove data not being used
- Remove all access not being used
- Remove shared credentials
- Remove all deprecated accounts

Communicate

- What level of effort was expended?
 - In hours days or weeks
- What was accomplished?
- Use visuals if possible, to communicate outcomes
- Try to report progress weekly - simply

Critical Path Core Controls

- Asset Management
- Vulnerability Management
- Data Management
- Malware Management
- Secure Communications
- Access Control
- Log Monitoring



Asset Management

- Inventory Assets
 - Endpoints
 - Servers
 - Applications (future)
 - Cloud Services (future)
- Data
 - Classify Assets
 - Sources of data
 - Scanning tools
 - Purchase history



Vulnerability Management

- Consistent Scanning of all servers
 - Focus on exploitable vulnerabilities
 - Servers and desktops/laptops
- Automatic patching
 - Tuesday Updates
 - Turned on by default

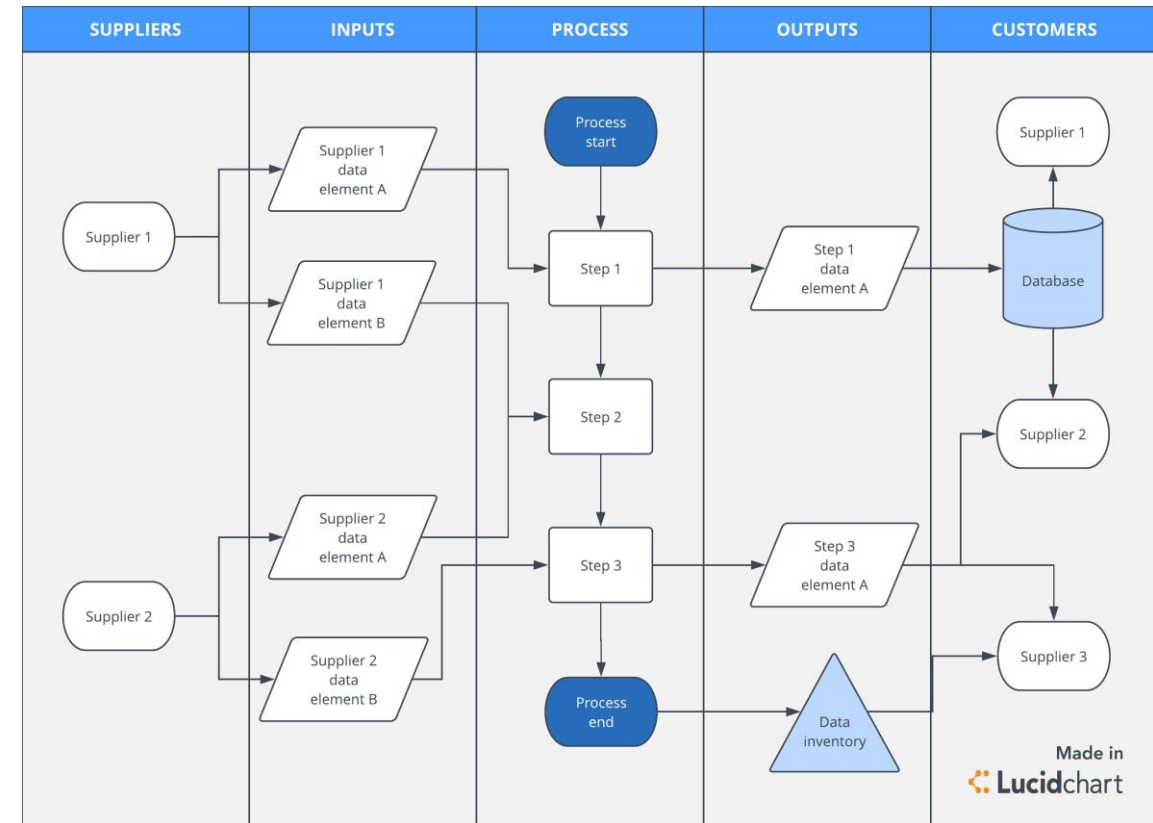
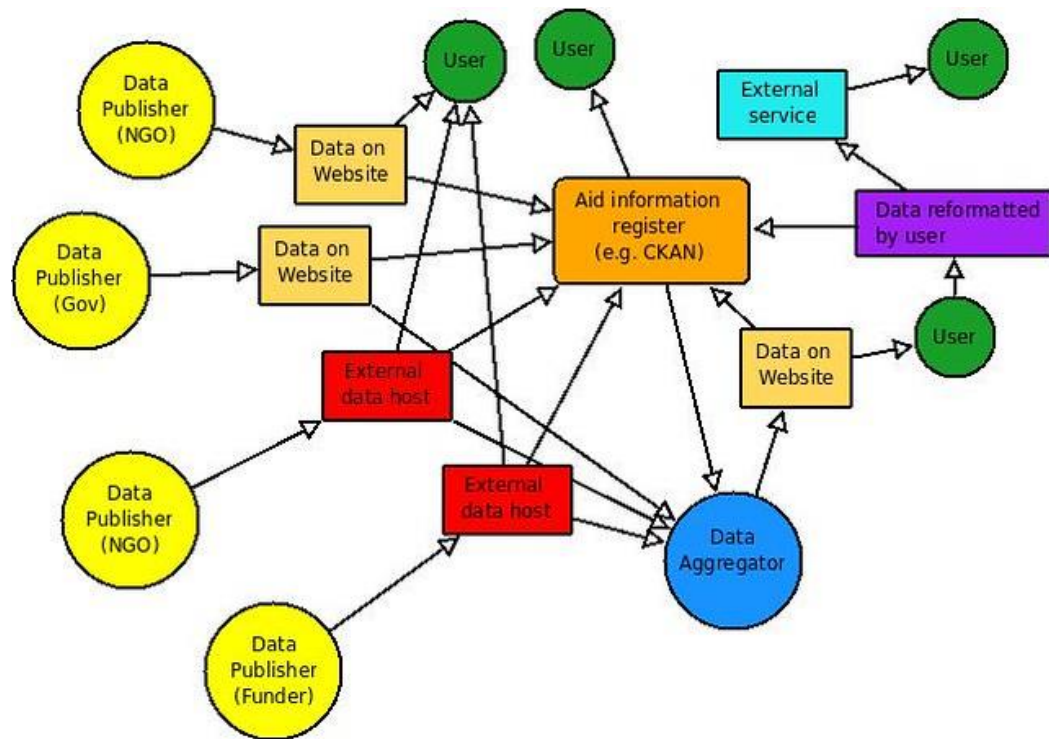


Data Management

- Inventory data locations/flows
- Classify data by risk
 - High
 - Medium
 - Low
 - Public (maybe)
 - 3-4 levels
- Map data flows
 - Applications
- Discover “hidden” data
 - Scan for PII
- Backups
 - Test assumptions



Data Flow Mapping Example



Malware Management

- Antivirus
 - Collect and review logs
 - How many infections are you getting?
 - How quickly is it being blocked/remediated?
- Malware Protection
 - Is there ransomware on your network?
 - Do you classify/analyze malware?



Secure Communications

- Protect the border
 - Border Firewalls
 - Firewall/IDS on endpoints
 - Auto block
 - Review network communications from endpoints
- Email security
 - SPAM protection
 - Phishing Protection
 - Commercial works the best
 - DMARC



Access Management & Control

- Simplify Access
 - One Directory
- Protect high risk accounts
- Multi-factor
- Remove/Delete unused accounts



Log Review

- Consistent log review
- Start with something
 - 0% reviewed of 0 logs is still 0
- Identify key assets from inventory and begin with them
 - Is logging on?
 - Are the right fields being logged?
 - Can they be aggregated and reviewed?

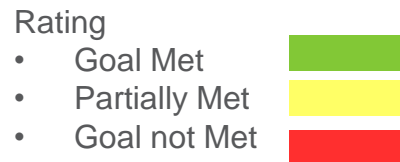
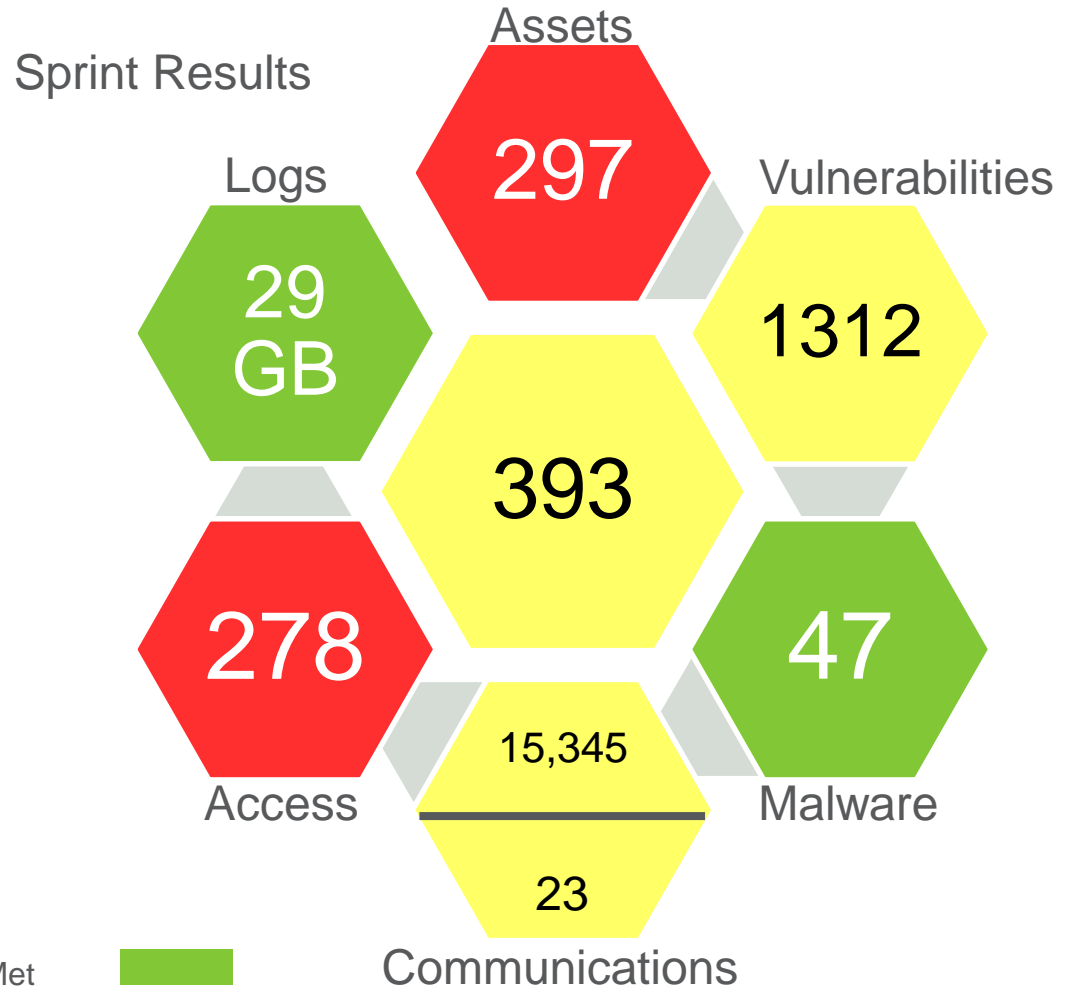
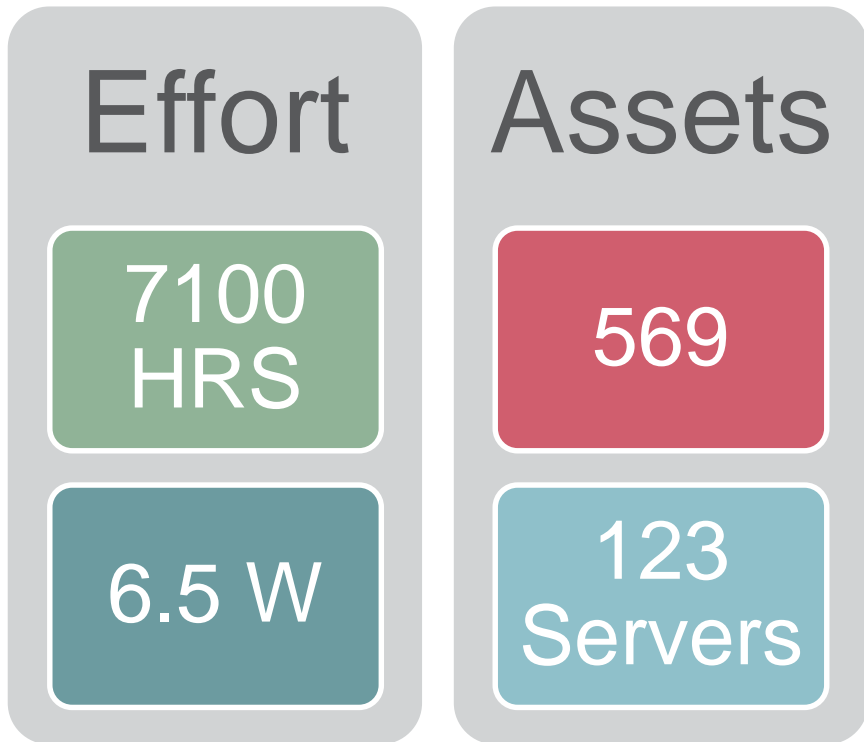


Secret Sauce

- Agile project based
 - Rinse and repeat
 - Complete focus for 6 week sprints
 - Daily or weekly standups
- Identify knowns and unknowns upfront
- Identify measures to gauge progress
- Communicate the plan
- Have a party (with food)



Communicate



Next Up

- Compliance (PCI, HIPAA etc.)
- BCP
- Wireless
- Mobile
- Application Security
- Cloud Security
- Risk Management
- Physical Security
- Data Governance
- Operational System Security
- IoT



The Ohio State University
WEXNER MEDICAL CENTER

The Ohio State University
Medical Center



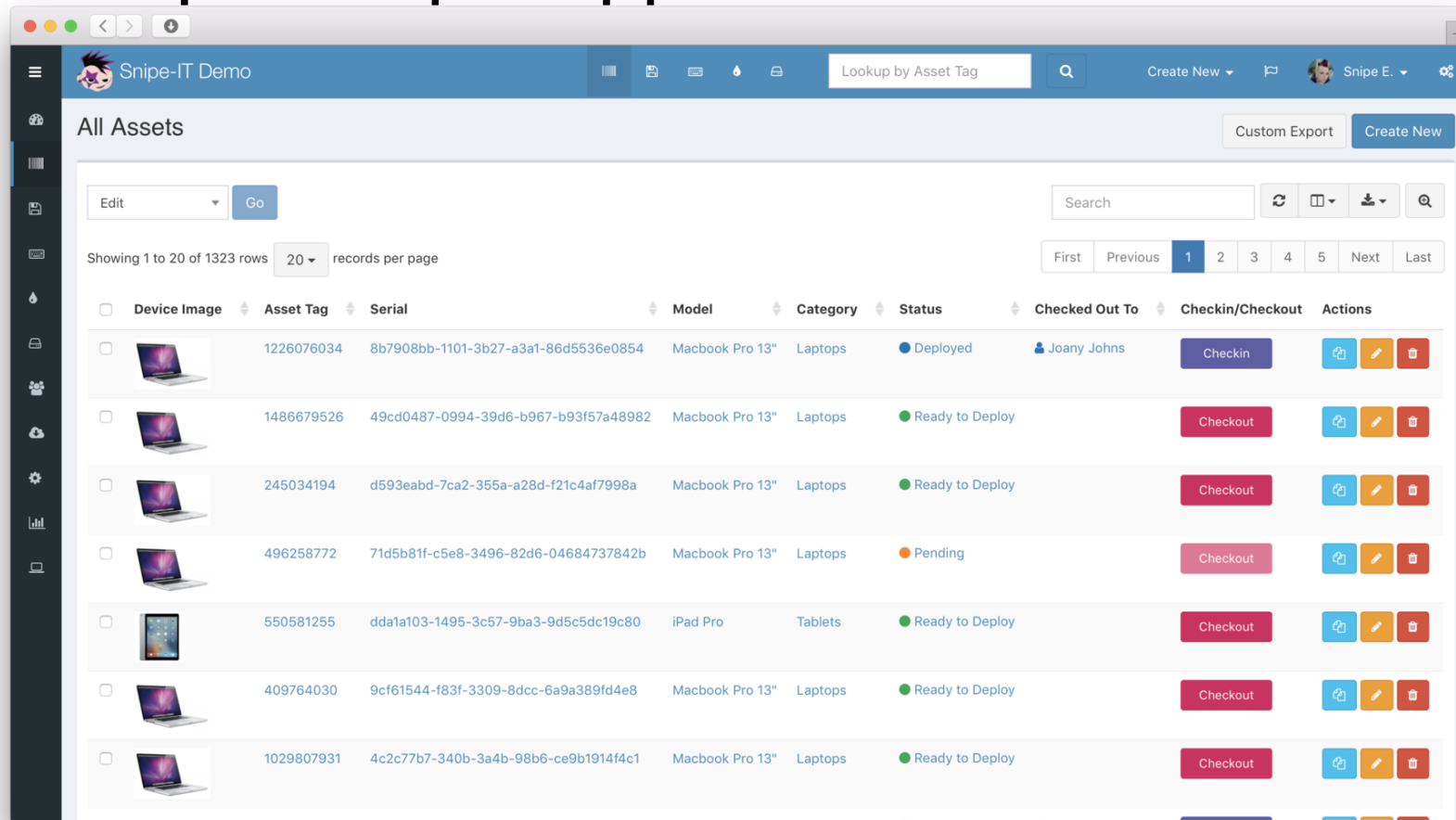
Questions?

Tools































Asset Management Tool Example

- <https://snipeitapp.com/demo>



The screenshot displays the Snipe-IT Demo interface. At the top, there is a navigation bar with the title "Snipe-IT Demo", a search bar labeled "Lookup by Asset Tag", and user information "Snipe E.". Below the navigation bar, the main content area is titled "All Assets". It includes a search bar, a "Custom Export" button, and a "Create New" button. The table below shows a list of assets with columns for Device Image, Asset Tag, Serial, Model, Category, Status, Checked Out To, Checkin/Checkout, and Actions. The table is currently showing 7 rows of data.

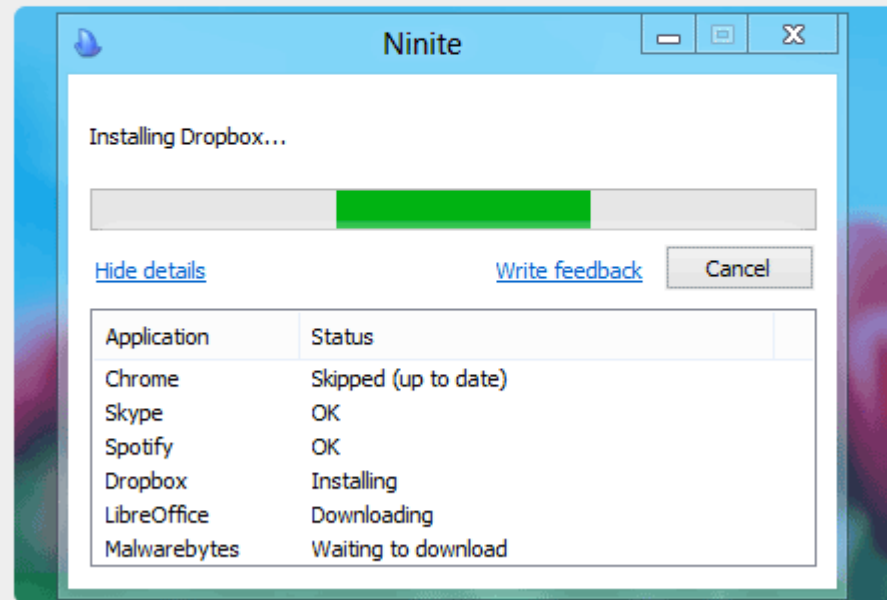
Device Image	Asset Tag	Serial	Model	Category	Status	Checked Out To	Checkin/Checkout	Actions
	122676034	8b7908bb-1101-3b27-a3a1-86d5536e0854	Macbook Pro 13"	Laptops	Deployed	Joany Johns	Checkin	  
	1486679526	49cd0487-0994-39d6-b967-b93f57a48982	Macbook Pro 13"	Laptops	Ready to Deploy		Checkout	  
	245034194	d593eabd-7ca2-355a-a28d-f21c4af7998a	Macbook Pro 13"	Laptops	Ready to Deploy		Checkout	  
	496258772	71d5b81f-c5e8-3496-82d6-04684737842b	Macbook Pro 13"	Laptops	Pending		Checkout	  
	550581255	dda1a103-1495-3c57-9ba3-9d5c5dc19c80	iPad Pro	Tablets	Ready to Deploy		Checkout	  
	409764030	9cf61544-f83f-3309-8dcc-6a9a389fd4e8	Macbook Pro 13"	Laptops	Ready to Deploy		Checkout	  
	1029807931	4c2c77b7-340b-3a4b-98b6-ce9b1914f4c1	Macbook Pro 13"	Laptops	Ready to Deploy		Checkout	  

Patching



Install and Update All Your Programs at Once

No toolbars. No clicking next. Just pick your apps and go.



Vulnerability Management Example

Open VAS

<http://openvas.org/>



Data Discovery

Open Source

- SENF - <https://github.com/utiso/senf>
- ccsrch - <https://sourceforge.net/projects/ccsrch/>
- Open DLP - <https://code.google.com/archive/p/opendlp/>
- Powershell script - <https://superwidgets.wordpress.com/2014/08/23/using-powershell-to-report-on-files-containing-pii-personally-identifiable-information/>
- Gliffy
- LibreDraw

Commercial

- Spirion
- Symantec
- SolarWinds

AV & Malware Tools

- MS Windows Defender
- Clam AV (Clam WIN) - <https://www.clamav.net/>
- Immundet (CISCO Amp) - <https://www.immunet.com/index>
- AVG*
- Panda*
- Bitdefender*
- Research test results - <https://www.av-comparatives.org/>

* Free is not free – your data is the product

Cuckoo Sandbox

The screenshot displays the Cuckoo Sandbox web interface. At the top, there is a navigation bar with the Cuckoo logo, a search bar, and menu items for Dashboard, Recent, and Pending. On the right of the navigation bar are buttons for Submit, Import, and a refresh icon.

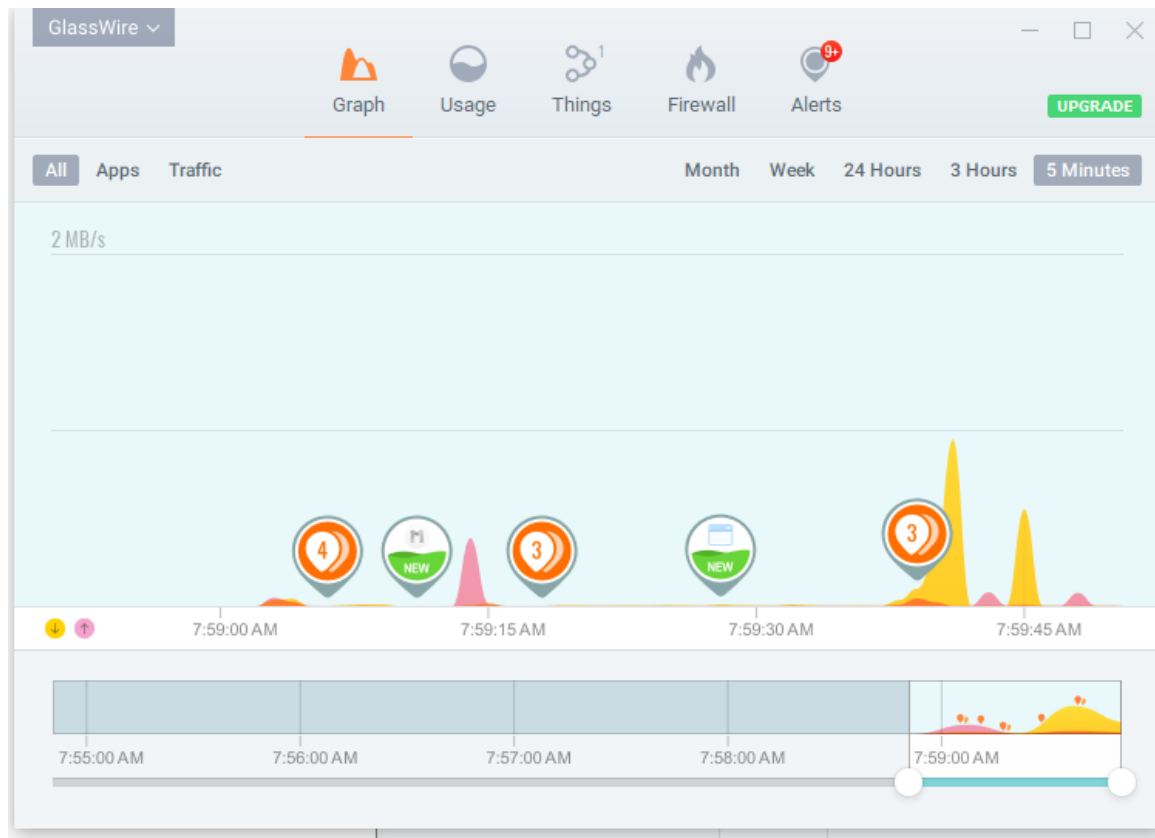
The main content area is divided into several sections:

- Insights:** Contains two tables. The first, "Cuckoo Installation", shows the version as 2.0.4. The second, "Usage statistics", shows counts for reported (68), completed (0), total (68), running (0), and pending (0) analyses.
- Cuckoo:** Features a "SUBMIT A FILE FOR ANALYSIS" section with an upload icon and a "SUBMIT URLS/HASHES" section with a text input field and a Submit button. A note below states: "Drag your file into the left field or click the icon to select a file."
- System info:** Displays system metrics using donut charts. It includes tabs for "free", "used", and "total". The "FREE DISK SPACE" chart shows 296.3 GB free and 931.5 GB total. The "CPU LOAD" chart shows 17% load on 8 cores. The "MEMORY USAGE" section indicates "NO DATA AVAILABLE".
- Recent analyses:** A table listing recent analysis results. The table has columns for #, Date, File, Package, and Score. One entry is visible: #107, Date 08/02/2018, File new.bin, and Score 2.4 / 10.

Secure Communciations

- Glasswire (\$) - <https://www.glasswire.com/>
- pfSense - <https://www.pfsense.org/>
- ClearOS - <https://www.clearos.com/>
- Smoothwall - <http://www.smoothwall.org/>
- VyOS - <https://vyos.io/>
- DMARC
 - Fraudmarc CE - <https://www.fraudmarc.com/fraudmarc-ce-open-source-dmarc/>
 - DMARC.org
 - Trusted Domain Project - <http://www.trusteddomain.org/opendmarc/>

Glasswire



GlassWire v

Graph Usage Things Firewall Alerts **UPGRADE**

Firewall Profiles 200 MB

Firewall **OFF**

Click To Block

Apps	Hosts	VirusTotal	↓	↑
Microsoft PowerPoint	prod.ols.live.com...:443	+13 more		
Host Process for Windows Services	array602.prod.d...:443	+11 more	175 B/s	52 B/s
Search and Cortana application	www.tm.f.prd.a...:443	+8 more		
Dropbox	bolt-sjc.v.dropbo...:443	+5 more		
Microsoft Teams	52.114.76.37:443	+2 more		
Microsoft Office Click-to-Run (SxS)	prod.mrodevicem...:443	+2 more		
Microsoft Outlook	40.97.116.82:443	+1 more		
Box	api.box.com:443	+1 more	1 KB/s	481 B/s
Bitwarden	2606:4700:20::6...:443	+1 more		
NT Kernel & System	192.168.0.255:137			

pfSense

Status: Dashboard

System Information

Name	pfsense.local
Version	2.0-RC1 (i386) built on Sat Feb 26 16:00:14 EST 2011 You are on the latest version.
Platform	pfSense
CPU Type	Intel(R) Pentium(R) 4 CPU 2.40GHz
Uptime	5 days, 19:06
Current date/time	Wed Mar 30 10:32:06 CDT 2011
DNS server(s)	208.67.222.222 208.67.220.220
Last config change	Wed Mar 30 8:38:51 CDT 2011
State table size	1478/197000 Show states
Mbuf Usage	533 / 780
CPU usage	<div style="width: 0%; height: 10px; background-color: #ccc;"></div> (Updating in 10 seconds)
Memory usage	<div style="width: 11%; height: 10px; background-color: #ccc;"></div> 11%
SWAP usage	<div style="width: 0%; height: 10px; background-color: #ccc;"></div> 0%
Disk usage	<div style="width: 2%; height: 10px; background-color: #ccc;"></div> 2%

Interfaces

<input checked="" type="checkbox"/> LAN	↑ 192.168.10.254	1000baseT <full-duplex>
<input checked="" type="checkbox"/> WAN (DHCP)	↑ 173.197.16.57	1000baseT <full-duplex>

Traffic Graphs

Current LAN Traffic

In: 1.43 Mbps
Out: 25.18 Mbps

Current WAN Traffic

In: 12.88 Mbps
Out: 1 Mbps

Current OPT1 Traffic

In: 10.69 Mbps
Out: 305 Kbps

ClearOS

The screenshot shows a web browser window displaying the ClearOS Network Report for interface eth0. The browser address bar shows the URL: `https://themedev.clearos.com:1501/app/network_report/iface/index/eth0`. The page header includes the ClearOS logo and navigation links for DASHBOARD, MARKETPLACE, SUPPORT, and ROOT (with a notification badge). The main content area is titled "Network Report" and "Interface - eth0". A search bar is present on the left. A sidebar menu lists categories: Cloud, Gateway, Server, Network, System, and Reports. Under Reports, the "Network" section is expanded to show "Network Report". A descriptive box states: "The Network Report provides network throughput information on all your network interfaces." The main chart, titled "Interface - eth0", shows network throughput in kb/s over time (12/01 00:00 to 16:00). The Y-axis ranges from 0 to 600 kb/s. The chart displays two data series: "Received" (yellow line) and "Transmitted" (blue line). Both series show low activity until approximately 11:00, followed by a sharp spike in both directions, peaking at around 500 kb/s. Below the chart is a "Report Data" table with a "Show 50 Rows" dropdown. The table has columns for "Date", "Received", and "Transmitted".

Date	Received	Transmitted
2014-12-01 16:10	69	575

Smoothwall

SmoothWall Express 3.0
Control About Services Networking VPN Logs Tools Maintenance shutdown | help

status advanced traffic graphs bandwidth bars traffic monitor my smoothwall

Pertinent information about your Smoothie, current configuration and resource usage.

Memory:

	Total	Used	Free	Used %	Shared	Buffers	Cached
Mem:	256824	64712K	192112K	25%	OK	23440K	26560K
Swap:	257032	OK	257032K	0%			
Total:	513856	64712K	449144K	12%			

Disk usage:

Filesystem	Mount point	Size	Used	Available	Used %
/dev/hda4	/	5.1G	186M	4.7G	4%
/dev/hda1	/boot	20M	3.6M	16M	19%
/dev/hda3	/var/log	2.6G	33M	2.4G	2%

Inode usage:

Filesystem	Mount point	Inodes	Used	Free	Used %
/dev/hda4	/	675840	27507	648333	5%
/dev/hda1	/boot	2616	20	2596	1%
/dev/hda3	/var/log	338944	34	338910	1%

Uptime and users:
15:22:15, up 5:54, 0 users, load average: 0.00, 0.00, 0.00

User	TTY	Login time	Idle	JCPU	PCPU	What

Interfaces:

eth0 (Green)			
IP Address:	192.168.72.141	Broadcast	192.168.72.255
Netmask:	255.255.255.0	MTU	1500
MAC Address:	00:0C:29:F8:1B:F1	Status	UP
Send:	5104481 (4.9%)	Receive:	0 (0.0%)

SmoothWall Express 3.0
Control About Services Networking VPN Logs Tools Maintenance shutdown | help

system web proxy firewall ids instant messages email

Check logs for attempted access to your network from outside hosts. Connections listed here **have** been blocked.

Settings:
Month: July Day: 31 Update Export

Log:

Time	In » Out		Source	Src Port	Destination	Dst Port
12:27:36	eth0 » -	UDP	202.97.238.202	49987	82.69.176.148	1027
12:29:47	eth0 » -	TCP	82.9.212.160	3706	82.69.176.151	2967
12:29:50	eth0 » -	TCP	82.9.212.160	3706	82.69.176.151	2967
12:32:55	eth0 » -	UDP	221.208.208.90	36877	82.69.176.148	1026
12:32:55	eth0 » -	UDP	221.208.208.90	36877	82.69.176.148	1027
12:32:55	eth0 » -	UDP	221.208.208.90	36877	82.69.176.151	1026
12:32:55	eth0 » -	UDP	221.208.208.90	36877	82.69.176.151	1027
12:37:54	eth0 » -	UDP	212.23.6.163	53(DOMAIN)	82.69.176.148	32768
12:43:38	eth0 » -	UDP	164.210.120.191	30593	82.69.176.148	1026
12:43:38	eth0 » -	UDP	164.210.120.191	30596	82.69.176.151	1026
12:49:15	eth0 » -	TCP	82.246.144.203	2381	82.69.176.148	445(MICROSOFT-DS)
12:49:18	eth0 » -	TCP	82.246.144.203	2381	82.69.176.148	445(MICROSOFT-DS)
12:51:44	eth0 » -	TCP	82.240.62.74	2032	82.69.176.148	445(MICROSOFT-DS)
12:51:47	eth0 » -	TCP	82.240.62.74	2032	82.69.176.148	445(MICROSOFT-DS)
12:55:30	eth1 » eth0	UDP	192.168.72.16	137(NETBIOS-NS)	192.168.110.110	137(NETBIOS-NS)
12:55:36	eth1 » eth0	UDP	192.168.72.16	137(NETBIOS-NS)	192.168.110.110	137(NETBIOS-NS)
12:55:41	eth1 » eth0	UDP	192.168.72.16	137(NETBIOS-NS)	192.168.110.110	137(NETBIOS-NS)
12:55:46	eth1 » eth0	UDP	192.168.72.16	137(NETBIOS-NS)	192.168.110.110	137(NETBIOS-NS)

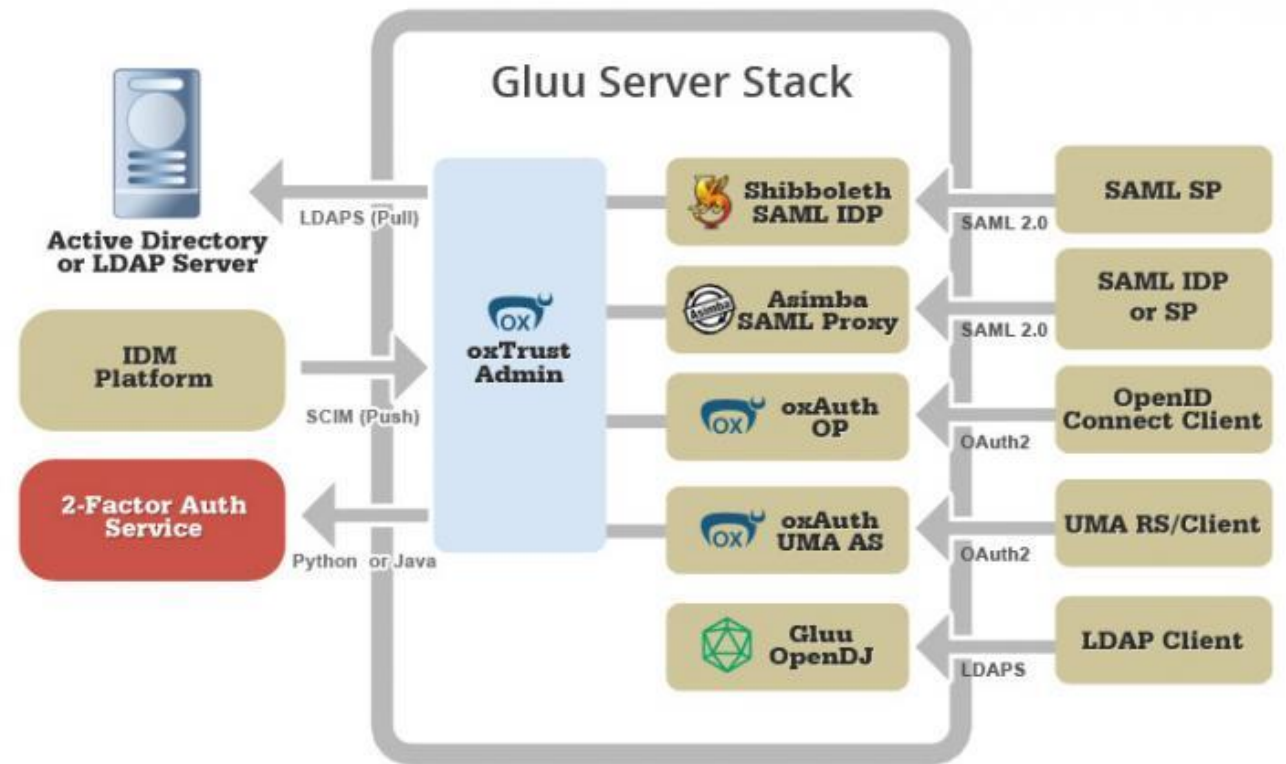
Lookup Add to IP block list

SmoothWall Express 3.0-polar-i386
SmoothWall™ is a trademark of SmoothWall Limited.

© 2000 - 2007 The SmoothWall Team
Credits - Portions © original authors

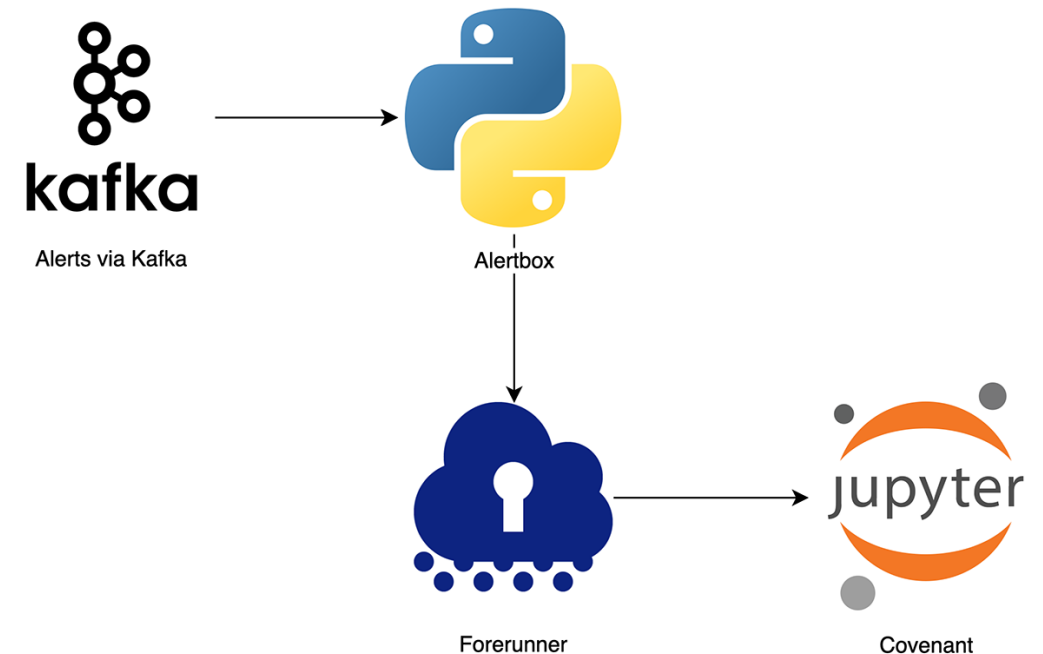
Access Management Tools (open)

- gluu Identity Server
- Oxpash (multifactor)
- Azure Active Directory



Log Tools

- Kafka - <https://kafka.apache.org/>
- Jupyter- <https://jupyter.org/>
- Graylog
- Elastic Stack (ELK)
- syslog



Jupyter

The image displays a collage of Jupyter Notebook interfaces. The top-left window shows a notebook titled "In Depth: Linear Regression" with introductory text and a code cell for plotting Lorenz attractor data. The top-right window shows the "Launcher" interface with options for Python 3, C++11, C++14, C++17, Julia 1.1.0, phylogenetics (Python 3.7), and R. The bottom row shows three separate notebook windows: "Julia" with a scatter plot of Iris species, "python notebook" with Lorenz system equations and code, and "R" with a ggplot of the Iris dataset and its output table.

```
File Edit View Run Kernel Tabs Settings Help
Python 3
```

In Depth: Linear Regression

Just as naive Bayes (discussed earlier in [In Depth: Naive Bayes Classification](#)) is a good starting point for classification tasks, linear regression models are a good starting point for regression tasks. Such models are popular because they can be fit very quickly, and are very interpretable. You are probably familiar with the simplest form of a linear regression model (i.e., fitting a straight line to data) but such models can be extended to model more complicated data behavior.

In this section we will start with a quick intuitive walk-through of the mathematics behind this well-known problem, before seeing how before moving on to see how linear models can be generalized to account for more complicated patterns in data.

We begin with

```
File Edit View Run Kernel Tabs Settings Help
```

```
[1]: %matplotlib inline
import matplotlib.pyplot as plt
import numpy as np
```

Simple

We will start with a simple example where z is a function of x and y .

```
[2]: rng = np.random.RandomState(1)
x = 10 * rng.rand(100)
y = 2 * x + rng.rand(100)
plt.scatter(x, y)
```

```
20
15
10
5
0
-5
-10
-15
```

We can use

```
[3]: from sklearn
```

```
File Edit View Run Kernel Tabs Settings Help
```

Launcher

Notebook

- Python 3
- C++11
- C++14
- C++17
- Julia 1.1.0
- phylogenetics (Python 3.7)
- R

Console

```
File Edit View Run Kernel Tabs Settings Help
```

Julia

```
[10]: using RDatasets, Gadfly
plot(dataset("datasets", "iris"), x="Sepal.Length", y="Species", size=:Sepal.Length)
```

```
[8]: eigen(x)
```

```
[8]: Eigen{Complex{Float64}, Complex{Float64}, Array{Complex{Float64}, 2}, Array{Complex{Float64}, 1}}
eigenvalues:
10-element Array{Complex{Float64}, 1}:
 4.7933881566545466 + 0.01im
-0.044538623333333333 - 0.01im
```

```
File Edit View Run Kernel Tabs Settings Help
```

python notebook

```
***
from IPython.display import Interactive, Fixed

We explore the Lorenz system of differential equations:

x-dot = sigma(y - x)
y-dot = rho*x - y - xz
z-dot = -beta*z + xy

Let's change (sigma, rho, beta) with ipywidgets and examine the trajectories.
```

```
[2]: from Lorenz import solve_lorenz

w = Interactive(solve_lorenz, sigma=(0.0, 50.0), rho=10.0, beta=2.6666666666666666)
```

```
File Edit View Run Kernel Tabs Settings Help
```

R

```
[3]: ggplot(data=iris, aes(x=Sepal.Length, y=Petal.Length)) + geom_point()
```

```
[1]: head(iris)
```

Sepal.Length	Sepal.Width	Petal.Length
5.1	3.5	1.4
4.9	3.0	1.4

Mode: Command Ln 1, Col 1 Lorenz.ipynb

elastic





- A seventeen year old Technology Consulting Firm with offices in New York, Boston, Los Angeles and San Francisco.
- We have a forward looking vision coupled with an attention to detail.
- We look for opportunities for integration between technologies, systems and applications.
- We avoid “technology for technology’s sake” by looking for value in the systems we design.
- We speak the language of our clients to match expectations with project deliverables.

VANTAGE TECHNOLOGY
CONSULTING GROUP

VANTAGE TECHNOLOGY SERVICES

