IT Forum

Security, UC Learning Center, Sophos, Cloud Storage, and Windows 10 Upgrade

June 27, 2017

Office of the
Chief Information Officer

Agenda

1. **CIO Welcome/Introduction – Matt Hall**
2. Security Briefing – Matt Hall & Kevin Schmidt
   a. Palo Alto Deployment
3. Review of Cloud File Storage Services – Google Drive – Steve Miley
4. Windows 10 Upgrade Discussion – Ben Price
5. Sophos Campus Deployment – Scott Nowell & Mershad Moghimi
6. UC Learning Center Upgrade – Doug Drury

Agenda

1. **CIO Welcome/Introduction**
2. Security Briefing – Matt Hall
   a. Palo Alto Deployment – Kevin Schmidt
3. Review of Cloud File Storage Services – Google Drive – Steve Miley
4. Windows 10 Upgrade Discussion – Ben Price
5. Sophos Campus Deployment – Scott Nowell & Mershad Moghimi
6. UC Learning Center Upgrade – Doug Drury

Security Briefing

Training

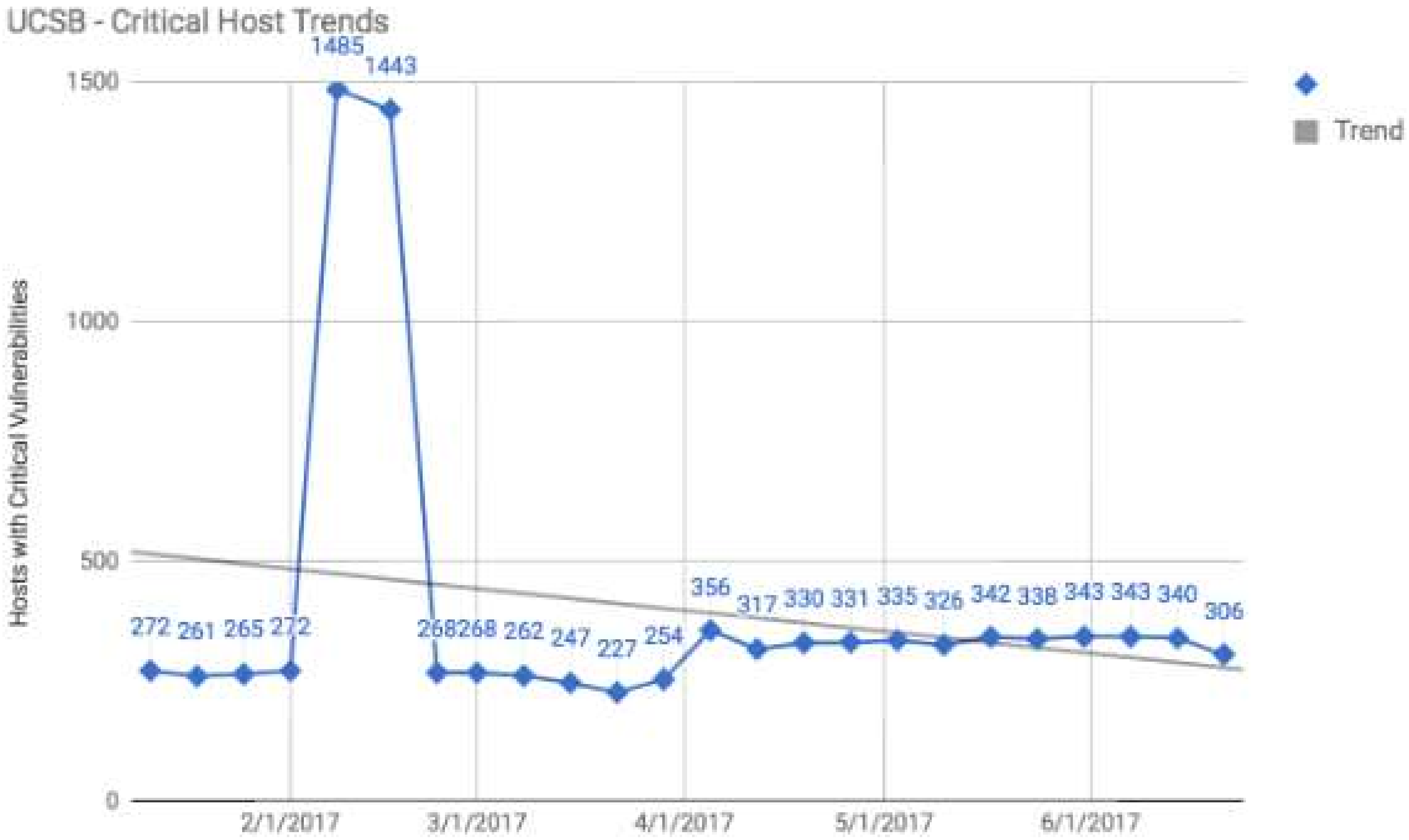
Only 79% of the employees completed the required Cyber Security Awareness Training have done so before the due date.

Of the 322 employees in a CNT job, 99% completed the required Cyber Security Awareness Training before the due date.

18 people completed advanced Security+ training and 11 more are scheduled for training. Ask your manager to contact Sam if you want to be on the list.

Online training on avoiding common vulnerabilities created through poor coding practices is available to web developers. If you develop code, Sam can hook you up.

Security Briefing



Security Briefing

Vulnerabilities

There are an average of 250 systems with critical vulnerabilities on the network each week.

These numbers are low because we are unable to detect vulnerabilities behind NAT or ACLs

Patching is important. WannaCry did not affect us, but there were more than 90 vulnerable systems when the attack broke out.

The patch for the WannaCry vulnerability was released in March; 2 months before the attack.

Incidents

537 UMail accounts were compromised this fiscal year. Most of these are the result of a phishing campaign last summer.

Please remind the users you work with to look out for phishing and coach them to recognize the signs of a fake message.

Security Briefing

NIST Framework

Identify

Protect

Detect

Respond

Recover

UC System-Wide

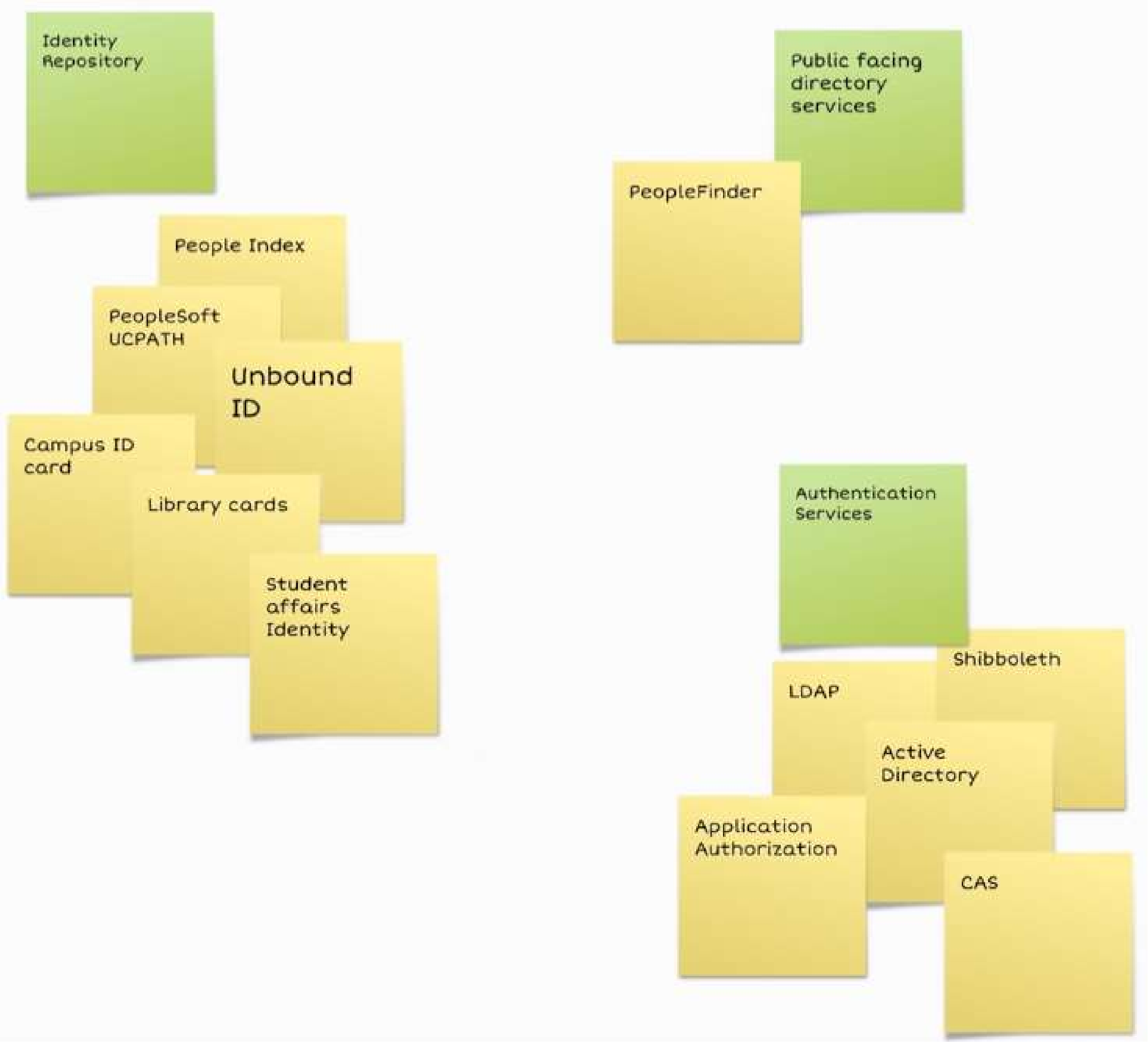
NIST Cybersecurity Framework

Aggregated Assessment

Security Briefing

Identify	Identity Architecture – Chair Jim Woods	Current state architecture complete
		Working on Greenfield description
	Network Architecture – Chair Ted Cabeen	Current state architecture complete (Google Drive)
		Working on Greenfield description including development of use cases, exploring technologies and developing proposals
	Cloud Architecture – Chair Steve Miley	Group membership still open
		Developing current state architecture for backup, complimentary/core servers
		Will develop Greenfield descriptions
Protect	Palo Alto	
Detect	Palo Alto	

Identity Architecture



Identity Repository

People Index

PeopleSoft UCPATH

Unbound ID

Campus ID card

Library cards

Student affairs Identity

Public facing directory services

PeopleFinder

Authentication Services

Shibboleth

LDAP

Active Directory

Application Authorization

CAS

Agenda

1. **CIO Welcome/Introduction – Matt Hall**
2. Security Briefing – Matt Hall
    a. Palo Alto Deployment – Kevin Schmidt
3. Review of Cloud File Storage Services – Google Drive – Steve Miley
4. Windows 10 Upgrade Discussion – Ben Price
5. Sophos Campus Deployment – Scott Nowell & Mershad Moghimi
6. UC Learning Center Upgrade – Doug Drury

Palo Alto Deployment Update

1. Palo Alto 7050 Unified Threat Management Status - It is here and being configured.

2. Critical vulnerability machine remediation.

Agenda

1. **CIO Welcome/Introduction – Matt Hall**
2. Security Briefing – Matt Hall & Kevin Schmidt
    a. Palo Alto Deployment
3. Review of Cloud File Storage Services – Google Drive – Steve Miley
4. Windows 10 Upgrade Discussion – Ben Price
5. Sophos Campus Deployment – Scott Nowell & Mershad Moghimi
6. UC Learning Center Upgrade – Doug Drury

Review of Cloud File Storage Services – Google Drive

Unlimited storage on Box and Google

- We spend lots of money and staff time on file servers and backups.
- What % of our storage is going to be in the cloud in 2020?

Where things are going?

- Goodbye, enterprise file server!

Chaos to avoid

- 20 staff sharing separate folders in google drive.

Concerns

- Who has access to those files outside the organization?
- Auditing ; employee turnover ; deletion- 30 days in trash.

Review of Cloud File Storage Services – Google Drive

Accessibility Methods: Web / Sync / Explorer&Finder

- Drive sync
- June 28 backup & Sync
- Insynchq
- Webdrive/Expandrive
- Drive Stream!
- Google Drive Plugin for MS Office

Review of Cloud File Storage Services – Google Drive

Your Personal Exabyte of Storage

Exciting:

- Team Drives
- File Stream ** no more sync
- Offline options
- Recent & Quick Access View

BUT, terms can change

- copy.com
- Amazon Unlimited
- Platform support (Linux yet?)

Other Options

- Using Object Storage in the cloud: NFS to S3 Buckets
- AWS Storage Gateway
- Virtual Drive on Servers
- Desktops

Agenda

1. **CIO Welcome/Introduction – Matt Hall**
2. Security Briefing – Matt Hall & Kevin Schmidt
    a. Palo Alto Deployment
3. Review of Cloud File Storage Services – Google Drive – Steve Miley
4. Windows 10 Upgrade Discussion – Ben Price
5. Sophos Campus Deployment - Scott Nowell & Mershad Moghimi
6. UC Learning Center Upgrade – Doug Drury

Windows 10 Upgrade Discussion - Deployment Considerations

- ➢ *Reasoning behind this effort?*
  - ✓ Expectation from our customers for the natural progression of technology
  - ✓ Microsoft's projected end of support 01/2020
  - ✓ New hardware support for legacy operating systems, drivers, etc.
- ➢ *Concerns and challenges?*
  - ✓ Legacy software compatibility, mostly home grown applications
  - ✓ Funding for hardware and software upgrades
  - ✓ Customer acceptance
- ➢ *Things to consider?*
  - ✓ Retire/remove legacy applications where possible such as Adobe reader, etc.
  - ✓ Enhance desktop security
  - ✓ Customer training as required
  - ✓ Minimum hardware standard, not Microsoft's recommendation
  - ✓ Retire/replace equipment older than 4-5 years, don't upgrade.
  - ✓ OS upgrade is not recommended. Opportunity for clean-up
  - ✓ What are other divisions doing with this effort?

Windows 10 Upgrade Discussion - Administrative Services

Administrative Services high-level planning

- ➢ *Standards hardware/software*
  - ✓ CPU – I5/I7, Memory 8-16Gig, ~500Gig HDD
    - o Looking into leveraging discounts across campus
  - ✓ Fresh install of Windows 10 not upgrade existing (May be some exceptions)
  - ✓ Upgrade application software to latest version wherever possible – Office 2016 standard (local install)
- ➢ *Windows 10 tools*
  - ✓ Software/hardware inventory - GFI
  - ✓ Image build and deploy using Microsoft MDT (SCCM is future consideration)
- ➢ *Testing*
  - ✓ Create test system for each department with departmental suite of tools
  - ✓ Engage 1-2 departmental experts to execute final testing
- ➢ *Phased approach*
  - ✓ Begin with smaller and less complicated departments or departments that are ready for a hardware refresh.
    - o TPS completed late 2016, Police currently under way.
  - ✓ Start with small test group for initial acceptance – Prefer departmental application experts
  - ✓ Parallel environment may be require having two systems in place during transition.

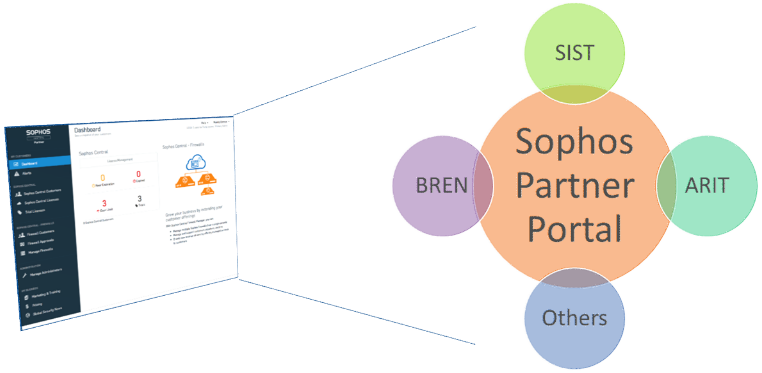
Agenda

1. **CIO Welcome/Introduction – Matt Hall**
2. Security Briefing – Matt Hall & Kevin Schmidt
    a. Palo Alto Deployment
3. Review of Cloud File Storage Services – Google Drive – Steve Miley
4. Windows 10 Upgrade Discussion - Ben Price
5. Sophos Campus Deployment - Scott Nowell & Mershad Moghimi
6. UC Learning Center Upgrade – Doug Drury

Review of Sophos Campus Deployment - Service Model

Sophos Central and the Sophos Partner Portal

Facilitate the management and protection of computers/servers, enforce policies, take action against threats, and generate metrics.



- ○ Licensed for 6,000 endpoints and 420 servers
- ○ Deployed 4,312 endpoints and 229 servers
- ○ Averaging 1,245 malware events monthly
- ○ Impacting ~%5 of all endpoints
- ○ Auto remediation average of 80%

Covered Devices

- ○ Endpoints (excluding BYOD)
- ○ Window and Linux server

Console Types

- ○ Departmental Console – locally administered
- ○ Campus Console – centrally administered

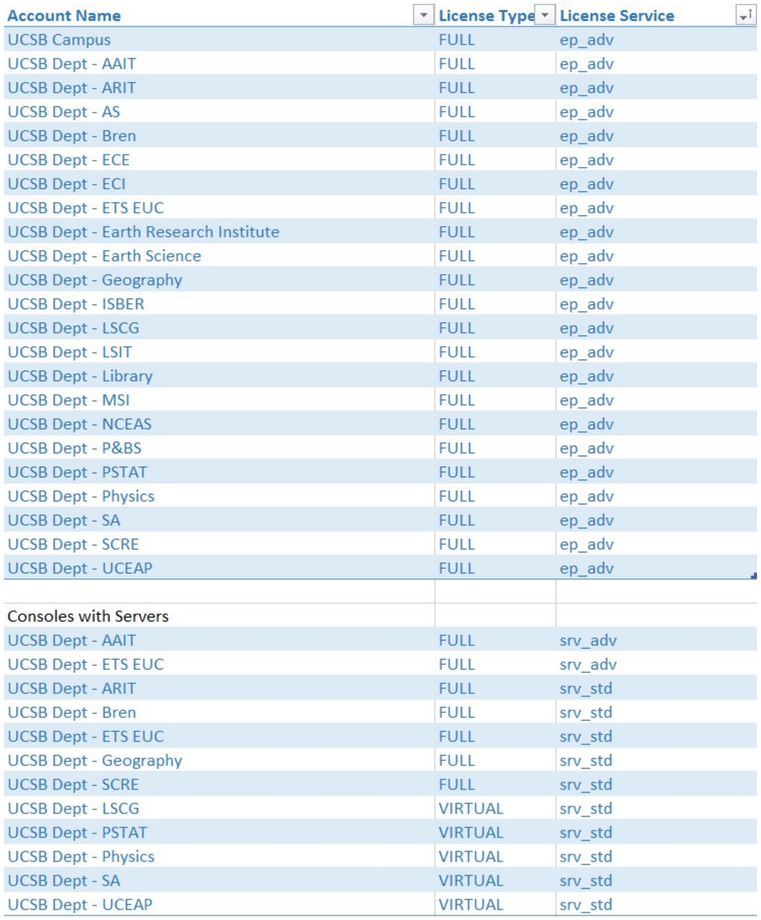
Departmental Consoles Considerations:

- ○ 50+ endpoints required
- ○ Department must assign administrator
- ○ Department responsible for deployment
- ○ Department responsible for monitoring and remediating incidents

Campus Consoles Considerations:

- ○ Department must provide contact for remediation of incidents
- ○ EUCE provides base policy (including weekly scans)
- ○ Other policies can be configured by EUCE based on customer’s request
- ○ Department will provide inventory changes to EUCE

Review of Sophos Campus Deployment - Consoles



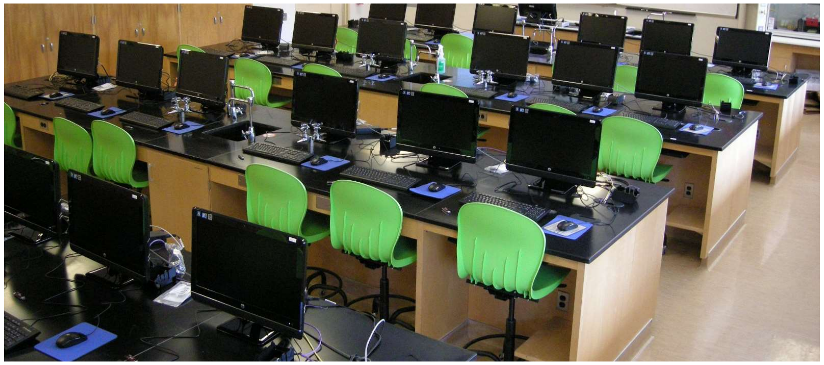
Account Name	License Type	License Service
UCSB Campus	FULL	ep_adv
UCSB Dept - AAIT	FULL	ep_adv
UCSB Dept - ARIT	FULL	ep_adv
UCSB Dept - AS	FULL	ep_adv
UCSB Dept - Bren	FULL	ep_adv
UCSB Dept - ECE	FULL	ep_adv
UCSB Dept - ECI	FULL	ep_adv
UCSB Dept - ETS EUC	FULL	ep_adv
UCSB Dept - Earth Research Institute	FULL	ep_adv
UCSB Dept - Earth Science	FULL	ep_adv
UCSB Dept - Geography	FULL	ep_adv
UCSB Dept - ISBER	FULL	ep_adv
UCSB Dept - LSCG	FULL	ep_adv
UCSB Dept - LSIT	FULL	ep_adv
UCSB Dept - Library	FULL	ep_adv
UCSB Dept - MSI	FULL	ep_adv
UCSB Dept - NCEAS	FULL	ep_adv
UCSB Dept - P&BS	FULL	ep_adv
UCSB Dept - PSTAT	FULL	ep_adv
UCSB Dept - Physics	FULL	ep_adv
UCSB Dept - SA	FULL	ep_adv
UCSB Dept - SCRE	FULL	ep_adv
UCSB Dept - UCEAP	FULL	ep_adv
Consoles with Servers		
UCSB Dept - AAIT	FULL	srv_adv
UCSB Dept - ETS EUC	FULL	srv_adv
UCSB Dept - ARIT	FULL	srv_std
UCSB Dept - Bren	FULL	srv_std
UCSB Dept - ETS EUC	FULL	srv_std
UCSB Dept - Geography	FULL	srv_std
UCSB Dept - SCRE	FULL	srv_std
UCSB Dept - LSCG	VIRTUAL	srv_std
UCSB Dept - PSTAT	VIRTUAL	srv_std
UCSB Dept - Physics	VIRTUAL	srv_std
UCSB Dept - SA	VIRTUAL	srv_std
UCSB Dept - UCEAP	VIRTUAL	srv_std

- Total consoles: 25
- Total consoles with only endpoints: 14
- Total consoles with endpoints and servers: 11

- Total client installed endpoints: 4312
- Total client installed servers: 229

(Totals compiled as of 6/1)

How many endpoints and servers are there @ UCSB?



Where is it and who is the local admin responsible?

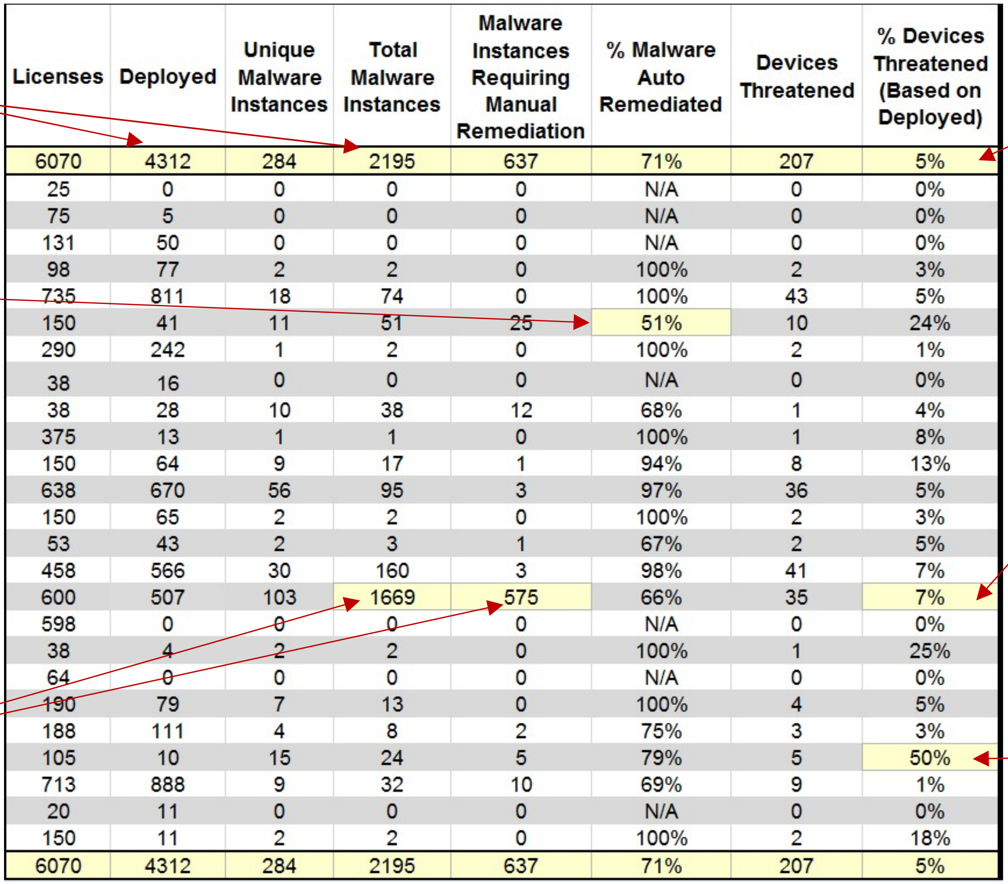
What is it’s OS and IP address? What is it’s security status?

These are questions Sophos allows us to answer, as a campus, that were difficult or impossible before.

Now we can do at a glance for 4700+ devices.

Review of Sophos Campus Deployment - Compiled UCSB Sophos Console Data

- 2195 malware detections on 4312 computers with Sophos
- 51% auto remediation is deceptive, this is really 1 malware instance multiplied 25 times by Time Machine backups
- Most impacted console – 1669 malware detections with 575 requiring manual remediation

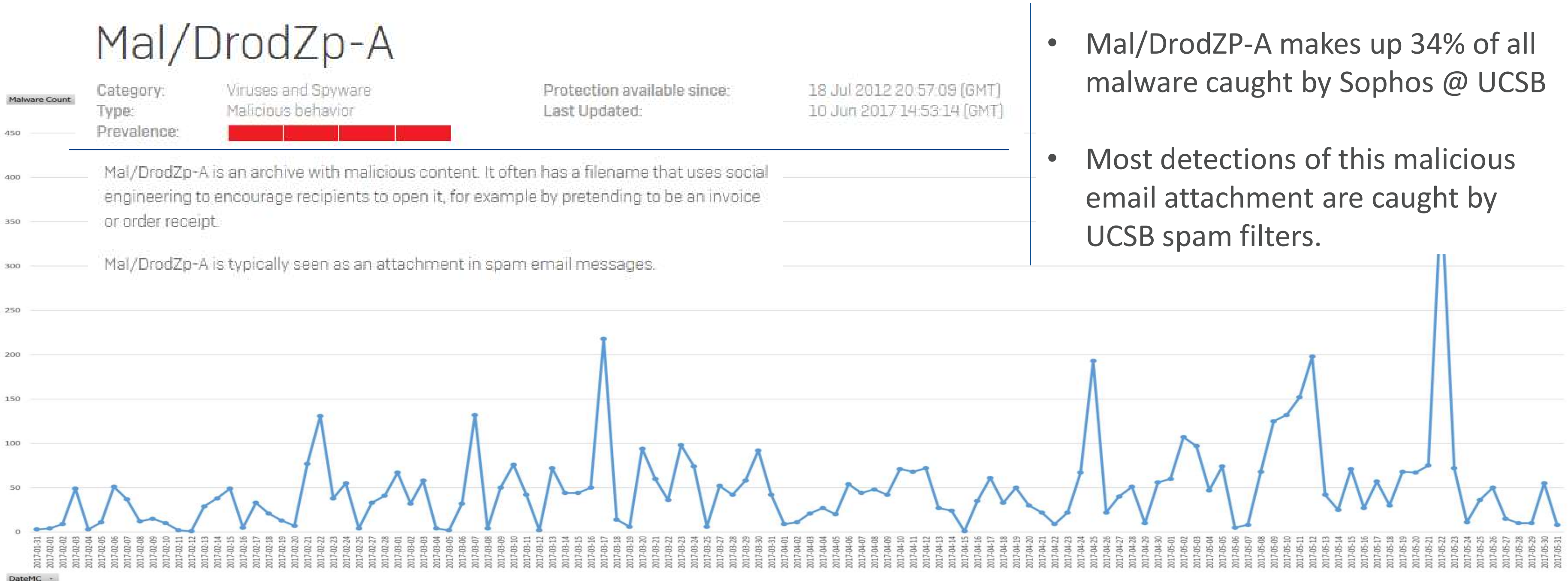


Licenses	Deployed	Unique Malware Instances	Total Malware Instances	Malware Instances Requiring Manual Remediation	% Malware Auto Remediated	Devices Threatened	% Devices Threatened (Based on Deployed)
6070	4312	284	2195	637	71%	207	5%
25	0	0	0	0	N/A	0	0%
75	5	0	0	0	N/A	0	0%
131	50	0	0	0	N/A	0	0%
98	77	2	2	0	100%	2	3%
735	811	18	74	0	100%	43	5%
150	41	11	51	25	51%	10	24%
290	242	1	2	0	100%	2	1%
38	16	0	0	0	N/A	0	0%
38	28	10	38	12	68%	1	4%
375	13	1	1	0	100%	1	8%
150	64	9	17	1	94%	8	13%
638	670	56	95	3	97%	36	5%
150	65	2	2	0	100%	2	3%
53	43	2	3	1	67%	2	5%
458	566	30	160	3	98%	41	7%
600	507	103	1669	575	66%	35	7%
598	0	0	0	0	N/A	0	0%
38	4	2	2	0	100%	1	25%
64	0	0	0	0	N/A	0	0%
190	79	7	13	0	100%	4	5%
188	111	4	8	2	75%	3	3%
105	10	15	24	5	79%	5	50%
713	888	9	32	10	69%	9	1%
20	11	0	0	0	N/A	0	0%
150	11	2	2	0	100%	2	18%
6070	4312	284	2195	637	71%	207	5%

- %5 of devices impacted has been a consistent average since inception
- 7% seems low considering total malware detected, but most infection is on only 2 computers out of 500+
- Small sample size effects

Review of Sophos Campus Deployment - Points of interest from the Data

- ❖ The top console in terms of malware is 12% of all computers, but 76% of the total malware detected @ UCSB
- ❖51% of the malware on the most impacted console in May is coming from only 2 computers, which by themselves are also 39% of all malware detected by Sophos @ UCSB
- ❖ The most common malware caught by Sophos @ UCSB is classified as Mal/DrodZP-A:



Mal/DrodZp-A

Category: Viruses and Spyware
Type: Malicious behavior
Prevalence: 🟥🟥🟥🟥

Protection available since: 18 Jul 2012 20:57:09 (GMT)
Last Updated: 10 Jun 2017 14:53:14 (GMT)

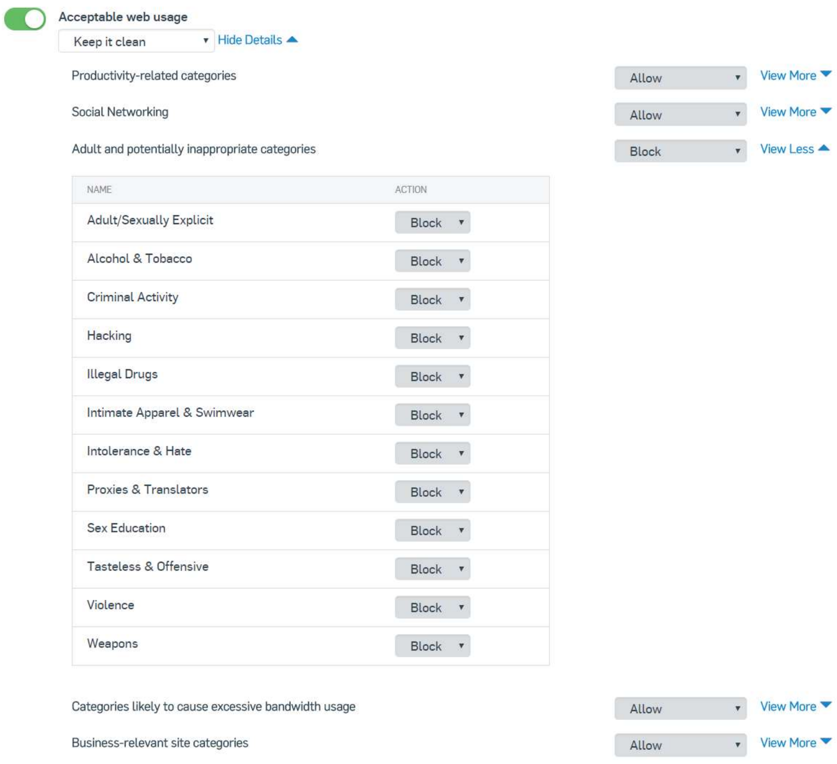
Mal/DrodZp-A is an archive with malicious content. It often has a filename that uses social engineering to encourage recipients to open it, for example by pretending to be an invoice or order receipt.

Mal/DrodZp-A is typically seen as an attachment in spam email messages.

- Mal/DrodZP-A makes up 34% of all malware caught by Sophos @ UCSB
- Most detections of this malicious email attachment are caught by UCSB spam filters.

Review of Sophos Campus Deployment - Sophos Policy Tools

Other Monitoring Tools in Sophos



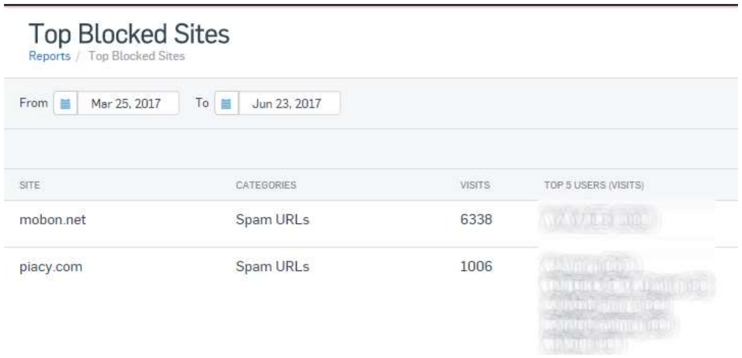
Acceptable web usage

Keep it clean ▾ Hide Details ▲

Productivity-related categories	Allow ▾	View More ▼
Social Networking	Allow ▾	View More ▼
Adult and potentially inappropriate categories	Block ▾	View Less ▲

NAME	ACTION
Adult/Sexually Explicit	Block ▾
Alcohol & Tobacco	Block ▾
Criminal Activity	Block ▾
Hacking	Block ▾
Illegal Drugs	Block ▾
Intimate Apparel & Swimwear	Block ▾
Intolerance & Hate	Block ▾
Proxies & Translators	Block ▾
Sex Education	Block ▾
Tasteless & Offensive	Block ▾
Violence	Block ▾
Weapons	Block ▾

Categories likely to cause excessive bandwidth usage	Allow ▾	View More ▼
Business-relevant site categories	Allow ▾	View More ▼



Top Blocked Sites

Reports / Top Blocked Sites

From Mar 25, 2017 To Jun 23, 2017

SITE	CATEGORIES	VISITS	TOP 5 USERS (VISITS)
mobon.net	Spam URLs	6338	[redacted]
piacy.com	Spam URLs	1006	[redacted]

From the Electronic Communication Policy: …systems personnel shall not intentionally search the contents of electronic communications or transactional information for violations of law or policy. However, if in the course of their duties systems personnel inadvertently discover or suspect improper governmental activity (including violations of law or University policy), reporting of such violations shall be consistent with the Policy on Reporting and Investigating Allegations of Suspected Improper Governmental Activities (the "Whistleblower Policy”).

TL;DR:

Don’t look for it, but if you find it use your judgement. If it is plainly illegal report it. If you aren’t sure, ask your supervisor. If your supervisor isn’t sure, go up the chain until someone is sure.

Agenda

1. **CIO Welcome/Introduction – Matt Hall**
2. Security Briefing – Matt Hall & Kevin Schmidt
   a. Palo Alto Deployment
3. Review of Cloud File Storage Services – Google Drive – Steve Miley
4. Windows 10 Upgrade Discussion - Ben Price
5. Sophos Campus Deployment - Scott Nowell & Mershad Moghimi
6. UC Learning Center Upgrade – Doug Drury

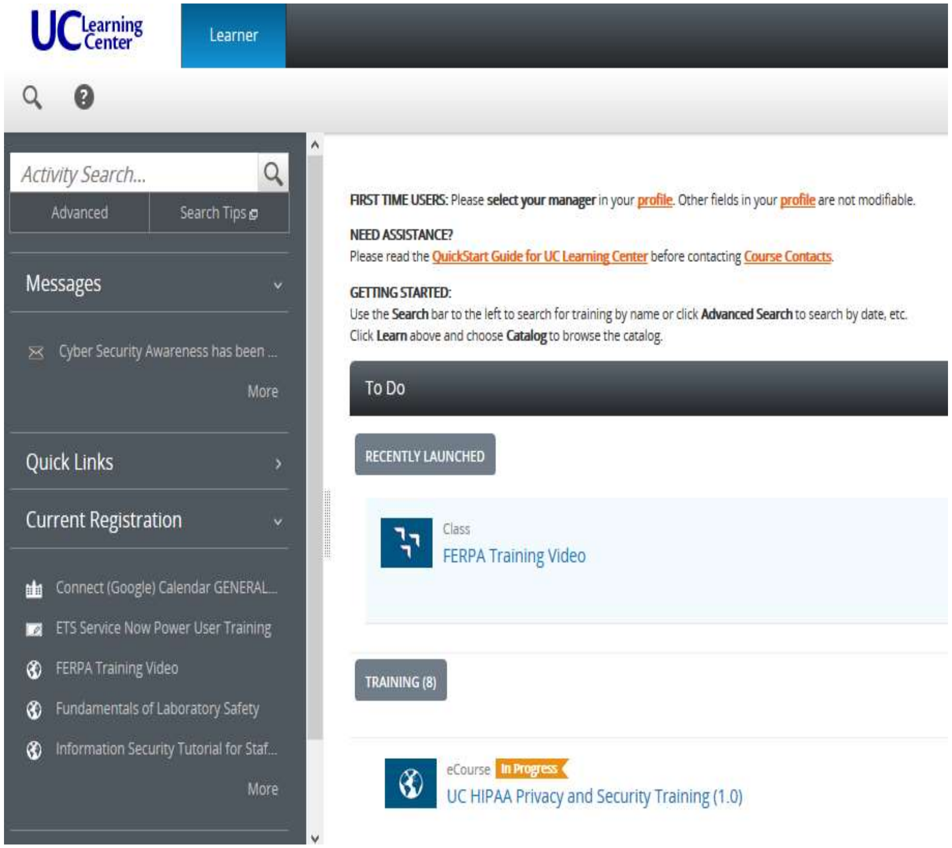
UC Learning Center Update

- The UC Learning Center will undergo an upgrade starting in late July.
- The UC Learning Center will unavailable from:
  - 5:00 p.m. on July 28, 2017
  - 7:00 a.m. on August 9, 2017
- Compliance training due during down time should be completed prior to 5:00 p.m. on July 28.
- Working with campus training providers to coordinate communication with the campus.
- Upgrade will include UCSB SSO integration.
- Use of mobile devices will require use of mobile app:
  - Apple App Store and
  - Google Play Store
- Pop Up windows will still be required to launch online training (but Netscape 4.79 won’t).

UC Learning Center Update

Current look/feel

New look/feel



FIRST TIME USERS: Please **select your manager** in your profile. Other fields in your profile are not modifiable.

NEED ASSISTANCE?
Please read the QuickStart Guide for UC Learning Center before contacting Course Contacts.

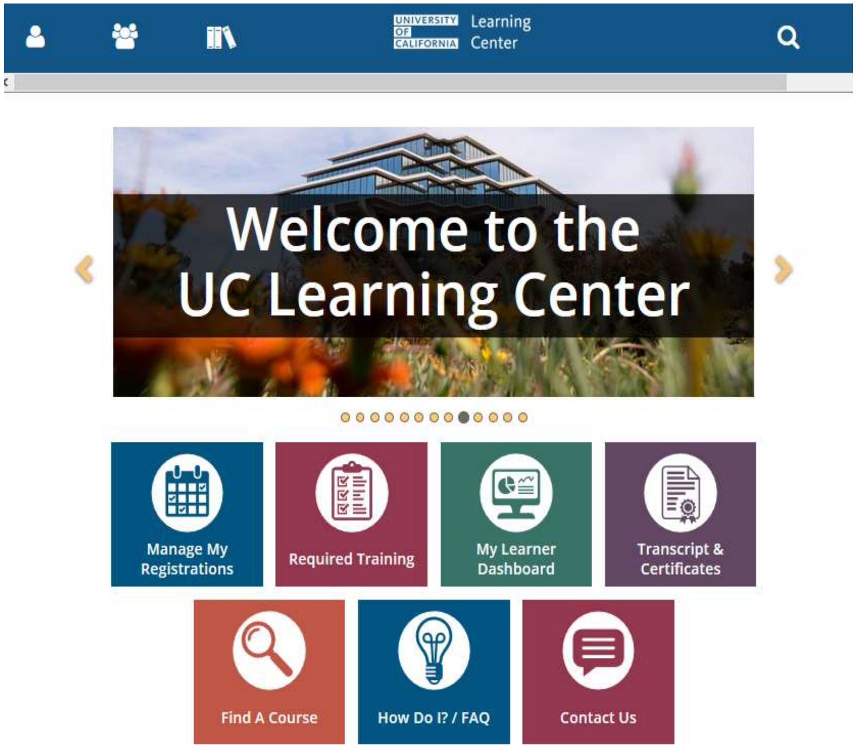
GETTING STARTED:
Use the **Search** bar to the left to search for training by name or click **Advanced Search** to search by date, etc.
Click **Learn** above and choose **Catalog** to browse the catalog.

Cyber Security Awareness has been ...

- Connect (Google) Calendar GENERAL...
- ETS Service Now Power User Training
- FERPA Training Video
- Fundamentals of Laboratory Safety
- Information Security Tutorial for Staf...

Class
FERPA Training Video

eCourse In Progress
UC HIPAA Privacy and Security Training (1.0)



UNIVERSITY OF CALIFORNIA Learning Center
Welcome to the UC Learning Center
Manage My Registrations
Required Training
My Learner Dashboard
Transcript & Certificates
Find A Course
How Do I? / FAQ
Contact Us

Questions & Open Discussion