AGENDA

• Welcome
• InfoSec/Project Updates
• SOC Updates
• Vulnerability Management
• SSO Adoption
• DHCP/DNS Kickoff
INFOSEC/PROJECT UPDATES

• DUO Multi-Factor Authentication Update
• PII Reduction Project
DUO 2-FACTOR AUTHENTICATION

Overall Duo Enrollment ---includes students and employees in Workforce groups A and Faculty (and voluntary Workforce group C)---

[Graph showing enrollment trends over time]
DUO 2-FACTOR AUTHENTICATION

Mandatory Employee Enrollment — includes employees in Workforce groups A and Faculty —

- Enrolled Campus Employees: 34%
- Campus Employees Not Yet Enrolled: 66%
PII REDUCTION

• Continued Support of Distributed IT’s Efforts
  • Meetings with ISL contacts – 16 of the 26 identified ISLs
  • Spirion scans – Recently finished scanning 16 TB of data

• Next Actions
  • Meet with the remaining 10 ISLs
  • Promote the Spirion DLP scanning solution
  • Work with ISLs to identify and reduce the PII footprint
AGENDA

• Welcome
• InfoSec/Project Updates
• SOC Updates
• Vulnerability Management
• SSO Adoption
• DHCP/DNS Kickoff
SOC UPDATES – ENDPOINT

• Currently evaluating advanced endpoint protection (EPP) / endpoint Detection and Response (EDR) products
  • Planning a proof-of-value (POV) test deployment in Aug
    • Looking for a school, department, etc. who would like to be part of the POV, contact Paul Walker if interested
  • Current plans are for a small purchase and deployment following a successful POV and a larger purchase next FY
SOC UPDATES – SOPHOS AV

• UAB IT has historically made Sophos AV available for Macs via the UAB software download site
• Looking at reducing count in light of the endpoint project
• However, a small number of these licenses will still be available
  • UAB-owned Macs only
  • Should mainly be used on Macs that are non-primary use workstations or that can’t run the new EPP agent when available
SOC UPDATES – MISC

• SSL Certificate requests – last year EISO began sending reminders if a cert was requested for a system for which data attestation had not been completed
  • Starting August 1, a cert will not be issued for a system which has not been attested in BlueCat

• Blocking “adult” sites – at last ISL meeting it was announced we were investigating blocking URL requests for sites in the “adult” category
  • Current recommendation is click-to-continue and log request
  • Recommendation will be presented to Faculty Senate at the Fall 2019 meeting
AGENDA

- Welcome
- InfoSec/Project Updates
- SOC Updates
- Vulnerability Management
- SSO Adoption
- DHCP/DNS Kickoff
VULNERABILITY MANAGEMENT

• Transport Layer Encryption
  • TLS1.2 - Minimum per UAB Encryption Guideline
  • SSLv3 & TLS1.0 must be deprecated by December 2019
  • Triple-DES (DES-CBC3-SHA) & RC4 Cipher Suites

SSL Labs - www.ssllabs.com (Internet-facing websites only)
VULNERABILITY MANAGEMENT

• End of Life Update

  https://www.uab.edu/it/home/os-status

  • Microsoft SQL 2008 July 2019
  • Oracle 12.1.0.2 July 2019
  • MacOS Sierra September 2019
  • Windows 10 v1703 October 2019
  • Windows 7 & Windows Server 2008 January 2020
  • Ubuntu 19.04 January 2020
  • VMWare ESXi/vCenter Server 6.0 March 2020
  • Debian 8 LTS June 2020
  • Redhat EL6 November 2020
VULNERABILITY MANAGEMENT

• Key Findings - Credentialed Scanning
  • Outdated Adobe Flash Player
  • .NET Framework Issues
    • 1.1 SP1, 2.0, 3.0 and 3.5 - Unsupported
    • 3.5 SP1 + Patches – Supported in some cases
    • 4, 4.5, and 4.5.1 – Unsupported
    • 4.5.2 – Supported for life of parent OS
    • 4.6 through 4.8 – Supported
  • Unsupported Adobe Reader or Creative Suite products
  • End of Life versions of Windows 10 (1507, 1511, 1607, 1703)
  • Web Browser Updates
    • Firefox 67.0.1 (as of June 4)
    • Chrome 74.0.3729.169 (May 21 stable release)
  • 7-Zip
  • Oracle Java
VULNERABILITY MANAGEMENT

• “BlueKeep” RCE Vulnerability (CVE-2019-0708)
  • Affects Remote Desktop Services
  • Likely worm-able in similar way to WannaCry/Petya malware
  • Patches released:
    • Desktop: Windows XP, Vista, and 7
    • Servers: 2003, 2008, and 2008R2
  • Scan data indicates < 60 systems missing patch.

“Our recommendation remains the same. We strongly advise that all affected systems should be updated as soon as possible.” – MSRC Team (May 30)

https://blogs.technet.microsoft.com/msrc/2019/05/30/a-reminder-to-update-your-systems-to-prevent-a-worm/
Summary report for UAB.EDU for May 2019

Overview

689
URLs scanned by Donkbot

0
Verified vulnerabilities

0
High risk vulnerabilities

Vulnerability Variants

No results found.

Vulnerabilities Trend [last 6-months]

No results found.

Comparison by Entity Classification for R1: Doctoral Universities — Very high research activity

0
Your vulnerabilities

105
Entities in Classification

1
Average vulnerabilities per entity

7
Max vulnerabilities
AGENDA

• Welcome
• InfoSec/Project Updates
• SOC Updates
• Vulnerability Management
• SSO Adoption
• DHCP/DNS Kickoff
UAB Single Sign-On

Identity and Access Management
Simple Authentication vs. Centralized Authentication vs. SSO vs. Federated SSO

**Simple Authentication:** Users are authenticated using credentials stored in separate application backend data store.
- User management done by the application
- Users need to remember multiple sets of authentication credentials

**Centralized Authentication:** Users are authenticated using credentials stored in a centralized backend data store.
- Users don’t need to remember multiple sets of authentication credentials
- The applications they are logging into can share user data
Simple Authentication vs. Centralized Authentication vs. SSO vs. Federated SSO (Continued)

**Single Sign-On:** Users are authenticated only once, regardless of how many other applications they attempt to access after the initial login.
- Users don’t need to enter authentication information multiple times
- Users credentials are always handled by the SSO IDP

**Federated Sign-On:** Users are authenticated only once, regardless of how many other applications they attempt to access after the initial login by establishing a federated trust.
- Users can be auto-provisioned
- Additional attributes can be passed to the application for authorization
SSO Benefits

- Improves customer satisfaction
- Increases efficiency and improves productivity
- Accelerates user adoption of company-promoted applications
- Reduces help desk costs
- Improves compliance and security capabilities (MFA and SOC visibility)
- Reduces risk by minimizing bad password habits
- Facilitates application-to-application and business-to-business collaboration
- Enables auto-provisioning
- Eases disaster recovery and business continuity efforts
Impetus for SSO

- Digital disruptions in the cloud (Governance and Contracts also a driver)
- Push from university leadership to get to a true SSO environment
- Stepping away from a monolithic, single platform and into the "best of breed" platform approach to meet the growing demands
<table>
<thead>
<tr>
<th>Hour of the Day</th>
<th>Sun</th>
<th>Mon</th>
<th>Tue</th>
<th>Wed</th>
<th>Thu</th>
<th>Fri</th>
<th>Sat</th>
</tr>
</thead>
<tbody>
<tr>
<td>00</td>
<td>●</td>
<td></td>
<td>●</td>
<td></td>
<td>●</td>
<td></td>
<td>●</td>
</tr>
<tr>
<td>01</td>
<td>●</td>
<td></td>
<td></td>
<td>●</td>
<td></td>
<td>●</td>
<td></td>
</tr>
<tr>
<td>02</td>
<td></td>
<td>●</td>
<td></td>
<td>●</td>
<td></td>
<td>●</td>
<td></td>
</tr>
<tr>
<td>03</td>
<td></td>
<td></td>
<td>●</td>
<td></td>
<td>●</td>
<td></td>
<td>●</td>
</tr>
<tr>
<td>04</td>
<td></td>
<td></td>
<td></td>
<td>●</td>
<td></td>
<td>●</td>
<td></td>
</tr>
<tr>
<td>05</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>●</td>
<td>●</td>
<td></td>
</tr>
<tr>
<td>06</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>●</td>
</tr>
<tr>
<td>07</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>08</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>●</td>
</tr>
<tr>
<td>09</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>17</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>19</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>20</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>21</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>22</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>23</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

190+ CAS apps
(263000+ logins/week)

85+ Shib apps
(101,000 + logins/week)
Helpful resources

- Identify the right SSO protocol
  - Create an AskIT ticket to whitelist an application or set federated trust
  - Schedule a vendor or internal call with the IDM team if needed

- Move configurations into production

CAS url: https://padlock.idm.uab.edu/cas/login
Shib metadata URL: https://padlock.dpo.uab.edu/uab-shib-metadata.xml

CAS: https://apereo.github.io
SHIBBOLETH: https://www.shibboleth.net/
IDM team: idm-developers@mail.ad.uab.edu
Help-desk: askit@uab.edu
CAS Clients

https://apereo.github.io/cas/6.0.x/integration/CAS-Clients.html

Official Clients

- .NET CAS Client
- Java CAS Client
- PHP CAS Client
- Apache CAS Client

Other Clients

Other unofficial or incubating CAS clients may be found here. Given the above projects are unofficial and not under direct maintenance of CAS, their availability and accuracy may vary.

Samples

- CASified Python web application using Flask
- CASified Java web application using Java CAS Client
- Go CLI for CAS admin endpoints
- Smoke Testing CAS HA Deployments
- CASified Bootiful Java web application

Framework Support

The following programming frameworks have built-in support for CAS:

- Spring Security
- Apache Shiro
- Pac4j
Any questions?

Thank you!
AGENDA

• Welcome
• InfoSec/Project Updates
• SOC Updates
• Vulnerability Management
• SSO Adoption
• DHCP/DNS Kickoff
IPAM PROJECT – AKA BLUECAT
DNS/DHCP/Attestation
PROJECT UPDATE – MEET THE TEAM

- Mark Shumate – Technical Lead
- Chuck White - Project Manager
- Christian Cummings – Project Originator / Executive Sponsor
PROJECT UPDATE – WHERE HAVE WE BEEN?

2017
• Project Initiation and Build
• Original Import of Attestation Data

2018
• Project Move from InfoSec to Networking
• DHCP Functions Implemented
• Work Begins on a Custom UI
PROJECT UPDATE – WHERE WE ARE TODAY?

- DHCP Migrations
  - VoIP
  - Wireless
  - Desktop – Internal
  - Desktop – External
- Custom UI in BETA
- Planning DNS migration
PROJECT UPDATE – WHERE ARE WE GOING?

TownHall Event coming soon!

DN

- Migration (Summer 19)
- AD DNS Integration
- Departmental Networks

DHCP

- v1 – Public Release
- v2 – Bulk Import Feature
- v3 – Self Registration Tools
- v4 – DNS functionality

Custom UI
CUSTOM UI - SCREENSHOTS

BlueCat Lookup Tool - BlueCat MAC Address & IP Address lookup tool.
BlueCat Attestation - BlueCat Attestation tool.
CUSTOM UI - SCREENSHOTS
CUSTOM UI - SCREENSHOTS
CUSTOM UI - SCREENSHOTS
<table>
<thead>
<tr>
<th>IPName</th>
<th>IPAddress</th>
<th>System Owner</th>
<th>System Owner Contact</th>
<th>Compliance Requirements</th>
<th>Number of Records</th>
<th>System Criticality</th>
<th>Data Classification</th>
<th>MACAddress</th>
<th>Edit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sample1</td>
<td>164.111.249.1</td>
<td><a href="mailto:jdoe@sample.com">jdoe@sample.com</a></td>
<td>205-555-1234</td>
<td>None</td>
<td>0</td>
<td>Supportive</td>
<td>Public</td>
<td>Static</td>
<td>Edit</td>
</tr>
<tr>
<td></td>
<td>164.111.249.2</td>
<td><a href="mailto:jdoe@sample.com">jdoe@sample.com</a></td>
<td>205-555-1234</td>
<td>None</td>
<td>0</td>
<td>Supportive</td>
<td>Public</td>
<td>Static</td>
<td>Edit</td>
</tr>
<tr>
<td>Sample1</td>
<td>164.111.249.1</td>
<td><a href="mailto:jdoe@sample.com">jdoe@sample.com</a></td>
<td>205-555-1234</td>
<td>None</td>
<td>0</td>
<td>Supportive</td>
<td>Public</td>
<td>Static</td>
<td>Edit</td>
</tr>
<tr>
<td>Sample1</td>
<td>164.111.249.2</td>
<td><a href="mailto:jdoe@sample.com">jdoe@sample.com</a></td>
<td>205-555-1234</td>
<td>None</td>
<td>0</td>
<td>Supportive</td>
<td>Public</td>
<td>Static</td>
<td>Edit</td>
</tr>
<tr>
<td>Sample1</td>
<td>164.111.249.3</td>
<td><a href="mailto:jdoe@sample.com">jdoe@sample.com</a></td>
<td>205-555-1234</td>
<td>None</td>
<td>0</td>
<td>Supportive</td>
<td>Public</td>
<td>Static</td>
<td>Edit</td>
</tr>
<tr>
<td>Sample1</td>
<td>164.111.249.4</td>
<td><a href="mailto:jdoe@sample.com">jdoe@sample.com</a></td>
<td>205-555-1234</td>
<td>None</td>
<td>0</td>
<td>Supportive</td>
<td>Public</td>
<td>Static</td>
<td>Edit</td>
</tr>
<tr>
<td>Sample1</td>
<td>164.111.249.5</td>
<td><a href="mailto:jdoe@sample.com">jdoe@sample.com</a></td>
<td>205-555-1234</td>
<td>None</td>
<td>0</td>
<td>Supportive</td>
<td>Public</td>
<td>Static</td>
<td>Edit</td>
</tr>
<tr>
<td>Sample1</td>
<td>164.111.249.6</td>
<td><a href="mailto:jdoe@sample.com">jdoe@sample.com</a></td>
<td>205-555-1234</td>
<td>None</td>
<td>0</td>
<td>Supportive</td>
<td>Public</td>
<td>Static</td>
<td>Edit</td>
</tr>
</tbody>
</table>
TESTER(S) WANTED
SEE US AFTERWARDS
Questions
THANK YOU