UC Merced CyberRisk Update

April 13, 2016

High level plan

Operationally we are focused on vulnerability scanning/management/remediation.

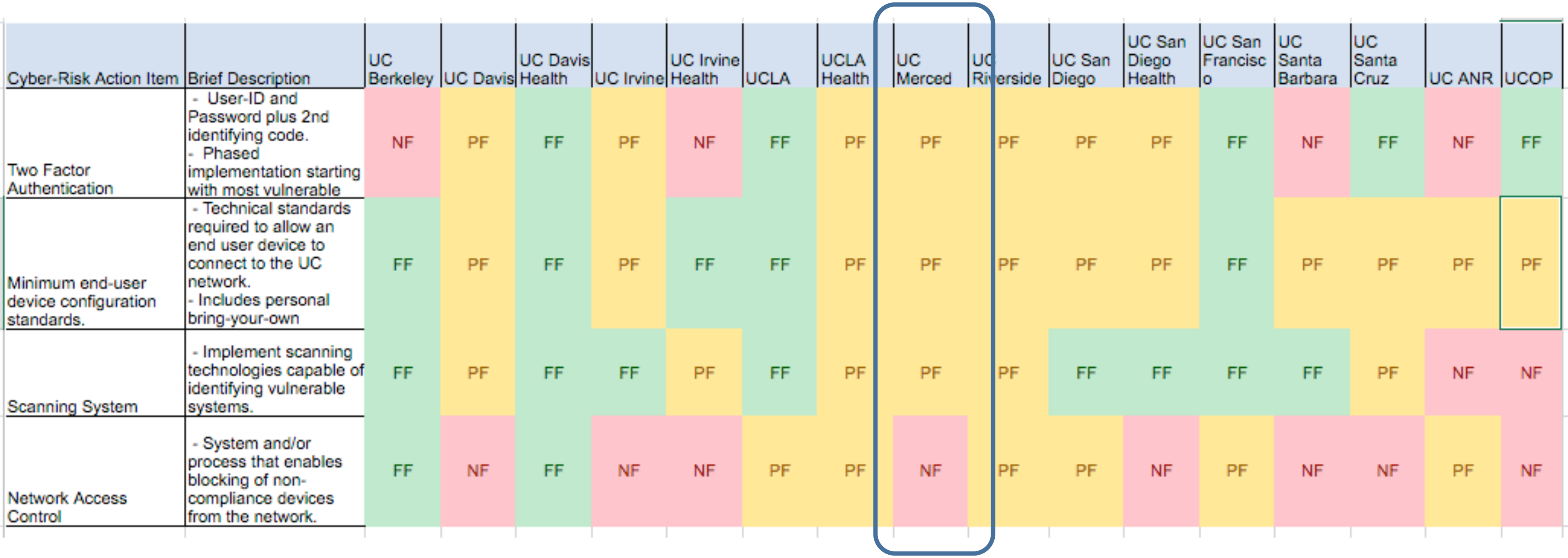
Strategically we are conducting scoping & budgeting exercises for the 4 CRGC priority areas:

1. Vulnerability scanning,
2. Two Factor Authentication
3. Endpoint management
4. Network Access Control

Campus Risk Assessment currently planned for Summer, pending UC wide discussion.

Resulting report will identify extensive remediation needs that must be managed through governance, policy and process adoption, and standardization.

CRGC Action Plan – Funding Status

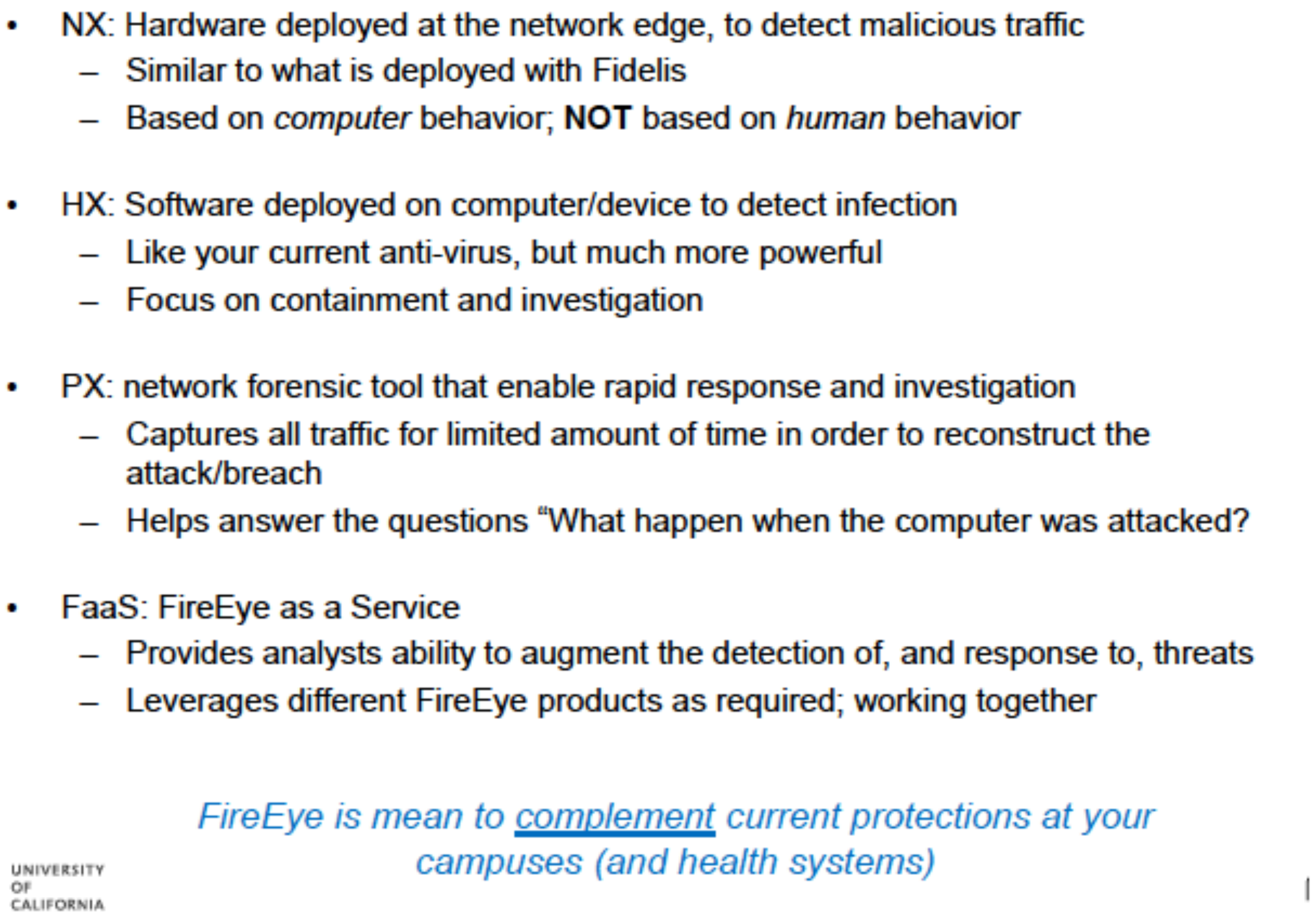


Cyber-Risk Action Item	Brief Description	UC Berkeley	UC Davis	UC Davis Health	UC Irvine	UC Irvine Health	UCLA	UCLA Health	UC Merced	UC Riverside	UC San Diego	UC San Diego Health	UC San Francisco	UC Santa Barbara	UC Santa Cruz	UC ANR	UCOP
Two Factor Authentication	- User-ID and Password plus 2nd identifying code. - Phased implementation starting with most vulnerable	NF	PF	FF	PF	NF	FF	PF	PF	PF	PF	PF	FF	NF	FF	NF	FF
Minimum end-user device configuration standards.	- Technical standards required to allow an end user device to connect to the UC network. - Includes personal bring-your-own	FF	PF	FF	PF	FF	FF	PF	PF	PF	PF	PF	FF	PF	PF	PF	PF
Scanning System	- Implement scanning technologies capable of identifying vulnerable systems.	FF	PF	FF	FF	PF	FF	PF	PF	PF	FF	FF	FF	FF	PF	NF	NF
Network Access Control	- System and/or process that enables blocking of non-compliance devices from the network.	FF	NF	FF	NF	NF	PF	PF	NF	PF	PF	NF	PF	NF	NF	PF	NF

UC Merced IT Security Team

1 Chief Information Security Officer
1 IT Security Analyst
1 vacant IT Security Analyst – in recruitment
IT WFP included request for 2 IT Security Analyst FTE

FireEye Solutions



- NX: Hardware deployed at the network edge, to detect malicious traffic
  - Similar to what is deployed with Fidelis
  - Based on *computer* behavior; **NOT** based on *human* behavior
- HX: Software deployed on computer/device to detect infection
  - Like your current anti-virus, but much more powerful
  - Focus on containment and investigation
- PX: network forensic tool that enable rapid response and investigation
  - Captures all traffic for limited amount of time in order to reconstruct the attack/breach
  - Helps answer the questions “What happen when the computer was attacked?
- FaaS: FireEye as a Service
  - Provides analysts ability to augment the detection of, and response to, threats
  - Leverages different FireEye products as required; working together

FireEye is mean to complement current protections at your campuses (and health systems)

UNIVERSITY
OF
CALIFORNIA

UC System Funding Commitment not yet finalized

UCMERCED

1. Vulnerability Management and Patching

What it is: Vulnerability scanning systems are a critical component of a “Defense in Depth” strategy that provide security teams with the necessary information and automation to quickly identify network, system and application vulnerabilities and conduct remediation efforts to prevent future attacks. Multiple levels of scan capability include asset discovery, network port scans, network vulnerability scans, application security testing and policy compliance. Requires 3 levels of scrutiny:

1. Conduct basic network scans that provide host discovery and are designed to search for open network ports and services that attackers could use as illicit entry points .

2. Conduct enhanced network vulnerability scans that interrogate each exposed port and service for specific vulnerabilities.

3. Conduct authenticated host scans (also called trusted scans) that provide detailed vulnerability data by looking “inside” the system.

Why we need it: Cyber-risk indicators and bad actors are constantly evolving. Social engineering results in uneducated and naive and users increasing vulnerabilities. Automation provides insight into network and system security postures via constant scanning and scoring of vulnerabilities

Current Status: UCM uses a $1500. toolset that lacks sophisticated analysis. At present, focused on levels 1 and 2. Gating factor is sufficient FTE to allocate to deep analysis and remediation upon discovery.

What is costs: $50,000 - $75,000. for a full service product. Lack of FTE is a gating factor. With increased scanning and discovery ability, increased FTE is required to analyze logs and execute remediation

Next Step:. A UC System-wide procurement is underway to select a common solution. Procurement details currently in discussion

2. Two Factor Authentication

What it is: A means to certifying authentication of an end user using two forms of identifying criteria, e.g. something a person knows and something a person has. E.g., text send via SMS to a cell phone number, in addition to log-in via a username and pwd.

Why we need it: People are sloppy with alphanumeric passwords. Two factor auth establishes a higher threshold to account for all to common password theft

Current Status: Selected product solution is DUO implemented in 2015 for all IT staff accessing IT servers and applications. License costs of $6,000. included all Faculty and Staff.

What is costs: $17,000 additional to include for students. This is an increase of $11,000. for the next FY. License model is based on FTE and IPEDS

Next Step:. Campus implementation is currently pending on an upgrade to Shibboleth Single Sign-On scheduled for Summer 2016. A VPN (virtual private network) POC (proof of concept) is up and running and informing the developing of a project plan and timeline to roll out DUO campus-wide by Fall.

3. End-Point Management

What it is: Endpoints include any computing or mobile devices used by university faculty, staff, students, and external users. These devices may range from UC-owned and managed devices to personal devices owned by employees and students. These endpoints, both work and personal, can access UC networks, including Wi-Fi, as well as use any Internet browser to access many UC applications and data. End-point management includes a combination of policies, processes and technology solutions that reduce the use of rogue devices and protect against loss or theft. Best practice end-point management includes at least 3 key technology solutions: (1) Encryption, (2) Malicious software protection, (3), Mobile device management, (4) end-point back-up. End-user education is a critical success factor.

Why we need it: Software is embedded in devices such as smart phones, and increasingly, *things* that share, exchange, and access data and PII.

Current Status*:* Current policy exists*:* **Minimum Security Standards for Networked Devices.** Encryption is currently supported. CrashPlan desktop / laptop backup provided for all faculty and staff.

What is costs: Currently supported by multiple vendor solutions delivering anti-virus and encryption for a total cost of approximately $7,500. Costs can be managed within current IT budget through FY 17 via internal reallocations, but will increase with growth due to licensing models based on FTE and enrollment

Next Step: Full implementation is pending finalization of IS-3 standards. Currently reviewing solutions to push out anti-virus/anti-malware and OS and application patching to end-points and mobile device management via the network upon authentication to the network. Cross-platform support is available. Adoption of standard desktop and mobile device platform across faculty, staff and students will minimize risk. See for example, the Berkeley Desktop.

4. Network Access Control

What it is: Network Access Control (NAC) is the practice of limiting access to network resources by authenticating the user and/or validating the device requesting access, and placing the device on an appropriate network segment. With NAC in place, network-based resources can choose to trust (or reject) connections based on policies. Policies may be identity-based (e.g. a regular end user should not be allowed to reach sensitive subnets within a data center) or device security posture-based (e.g. a client computer does not meet a location's antivirus requirement and should be placed on a network segment that only has access to the Internet). NAC is needed across 5 risk areas: (1) enterprise IT systems (servers), (2) distributed IT systems, (3) desktop and mobile computing, (4) research systems, and (5) control systems and specialized devices including critical infrastructure.

Why we need it: Reduce the impact of unauthorized, misconfigured, or infected devices on UC networks that risk confidentiality, integrity, and availability of UC electronic information, computing, and network resources.. Administrative safeguards (policy) can be difficult to enforce without technical controls.

Current Status*:* The implementation of the Next Gen Network has enabled NAC using the 802.1x compliant routers and switches.

What is costs: Vendor professional services for deployment and training using Aruba Clear Pass and 802.1x. Standards costs can be managed with current IT budget. CapEx implementation covered by NG Funding. Ongoing OpEx funding has not been allocated.

Next Step: Complete Next Gen Network for wired and wireless access and adopt best practices for network design and management. Different network segments require different levels of compliance; segments containing regulated or confidential information should have more stringent endpoint requirements than other segments.