Utilizing Keylight Sm – Vulnerability Management

Keylight leverages the web application scanning capabilities of Qualys and presents those results to help users identify and fix vulnerabilities in those web applications.

**Managing Vulnerabilities**

*If you’re reviewing systems but you have not received any notifications:*

1. Navigate to <https://itcompliance.bsd.uchicago.edu/>
	1. This website is only available on-campus or by utilizing the VPN
2. Click *Single Sign On*
	1. You will be directed to the University of Chicago Shibboleth/SAML portal.
3. Login using your CNET credentials
	1. If you do not have CNET credentials, a portal account will be created for you upon request.
	2. You will be forwarded to the LockPath Dashboard.



1. In the upper right corner, mouse over *Sm* and click the *Home* option

*If you have received a Vulnerability Finding email and have clicked on the deep link:*

1. You will be directed to the University of Chicago Shibboleth/SAML portal.
	1. Login using your CNET credentials
		1. If you do not have CNET credentials, a portal account will be created for you upon request.
	2. Upon login you will land on the specific vulnerability finding you were alerted to via email.
		1. Here you will find all relevant information about the system and status of the specific alert.
2. Under the heading *Connector Plugin,* click the name of the specific vulnerability finding.



1. Here you will be greeted with all relevant information regarding the specific vulnerability finding, including:
	1. Connector
	2. Plugin Identifier
	3. Family
	4. Publication Date
	5. Auto-Apply Status
	6. Description
	7. **Solutions**
	8. CVEs
	9. References
	10. Exploits
	11. Malware

 *\*\*\* Information regarding the Risk Score is also available \*\*\**

1. After applying the suggested solutions to the system or opting for mitigate/false positive status, navigate back to the vulnerability finding tab and click *Edit*.
2. Take the following actions:
	1. Select a *Resolution*
		1. If mitigate/false positive then enter *Mitigating Controls*
	2. Enter *Resolution Details*
	3. Add any additional comments under the *Comments* tab if necessary
	4. Click *Save*
	5. Mouse over *Actions*

**

* 1. Choose action based on Resolution:
	2. Submit for Review (Mitigate/False Positive)
	3. Remediate & Close

Appendix A – Vulnerability Management

