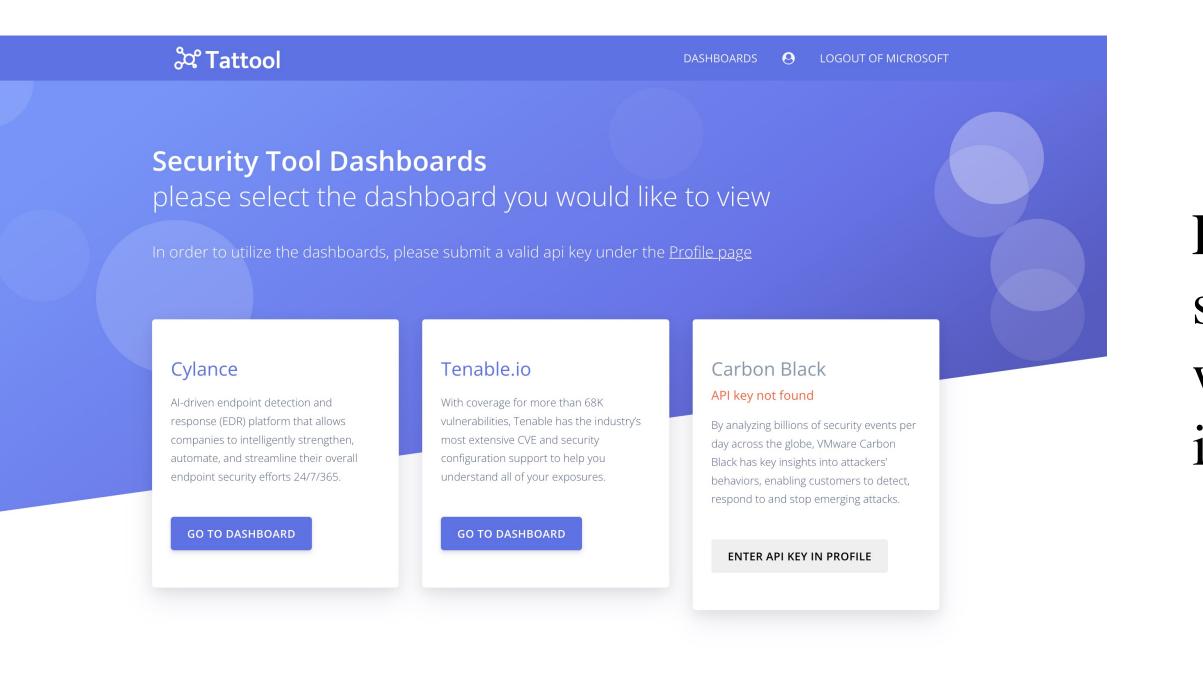




Background

- Consistent growth of cybercrime necessitates improvements in vulnerability monitoring
- Analyzing the output of cybersecurity tools is a timeconsuming task
- Shortages of cybersecurity specialists requires increasing their efficiency



An example dashboard for Carbon Black that sorts devices by their target values

Key Features

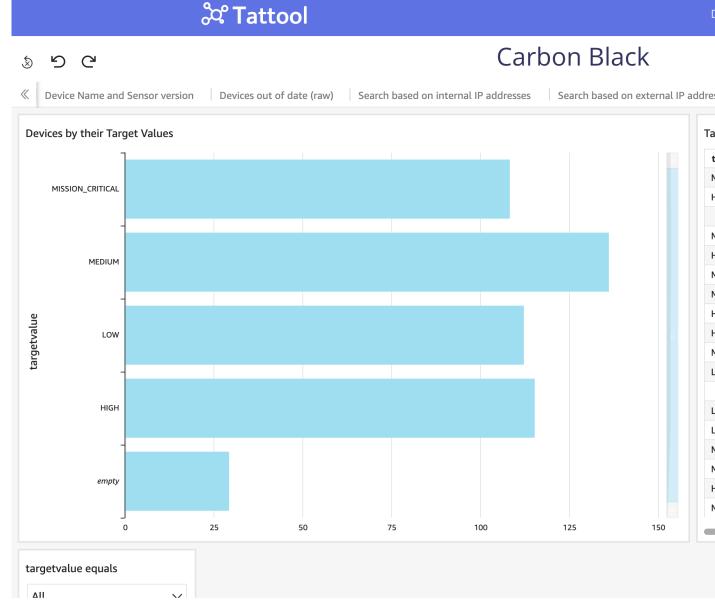
- Automated data refresh from cybersecurity tools:
 - Tenable.io
 - Cylance
 - Carbon Black
- Secure user system and cybersecurity data pipeline
- Automatic data analysis of potential security breaches
- Business intelligence visuals to quickly and easily identify probable vulnerabilities



Tattool: The Security Analyst Tool

Tyler Brennan, Brian Garten, Iryna Onyshko Affiliation: Department of Computer Science, Trinity College Advisor: Dr. Ewa Syta

> List of supported security tools, each with relevant business intelligence dashboards



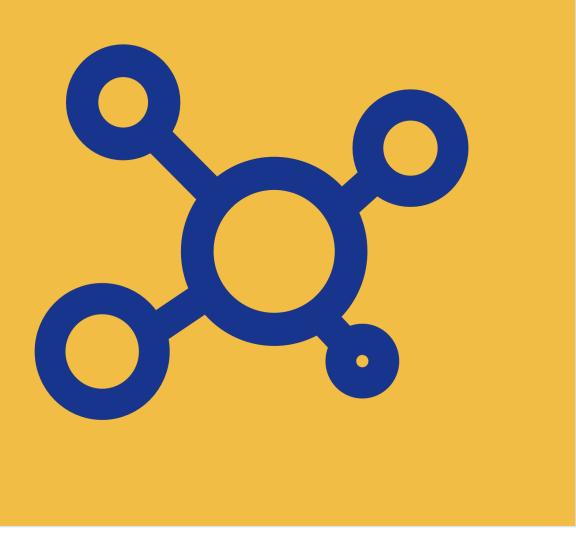
Brennan, Tyler O. (Student)

DASHBOARDS 🛛 🕙 LOGOUT OF MICROSOF

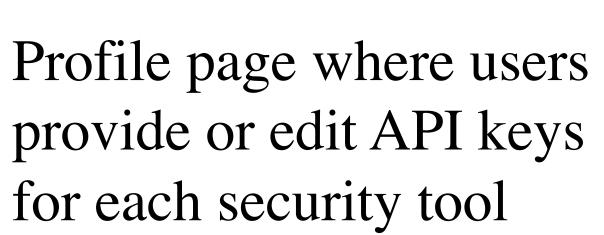
tbrenna2 tbrenna2@trincoll.edu

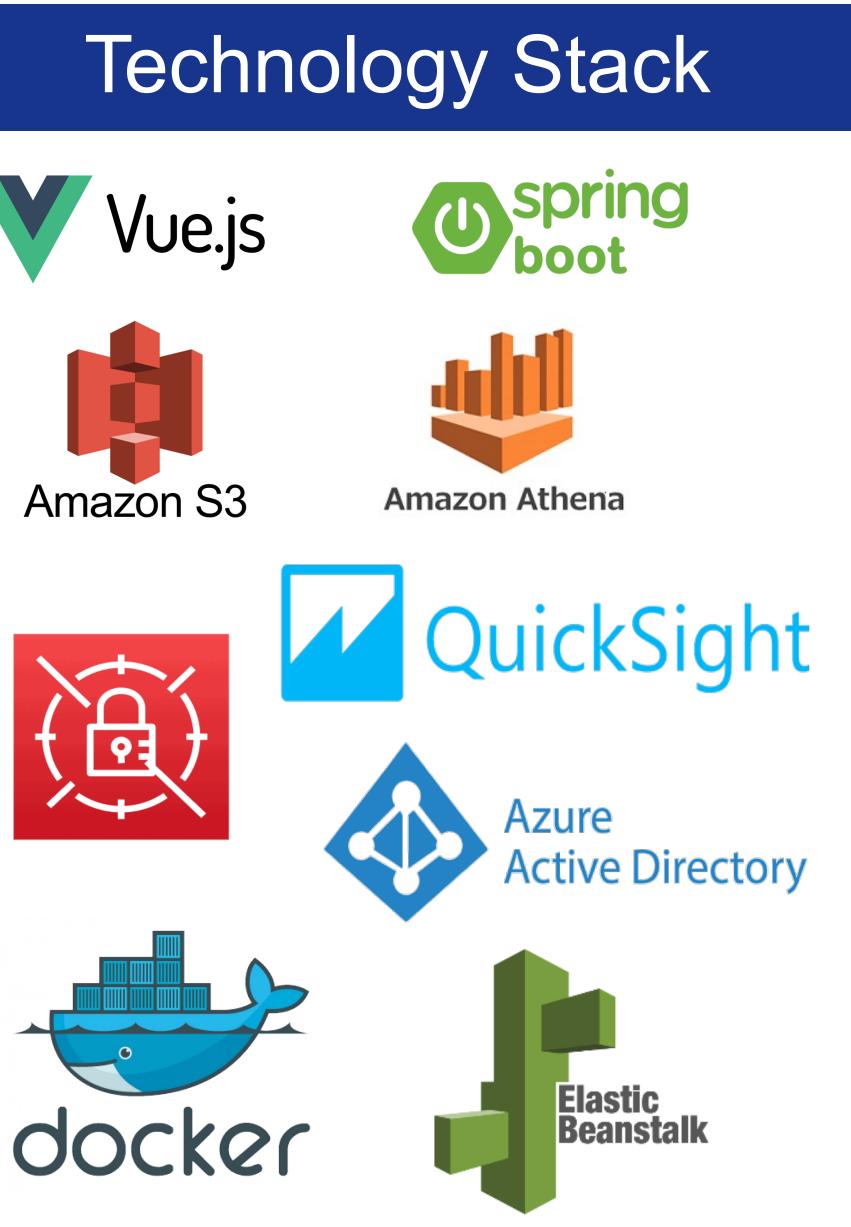
Security Tool Information

Cylance: 92ed7622-131b-4e8c-bdb9-5d738d2c49b2 Tenable.io: 7d365492-9d84-4b16-b8d9-ab44dc8d91f Carbon Black: a EDIT KEYS



DASHBOARDS	O LOGOUT OF M		
esses List assets	by scan states Searc	h by Target Value Se	ensor State
argetvalue, Lastinte	rnalipaddress, Lastexter	rnalipaddress, and Nan	ne
targetvalue	lastinternalipaddress	lastexternalipaddress	name
MEDIUM	89.0.44.72	70.201.241.107	aasp2d
HIGH	165.236.67.151	172.105.43.117	abachshell4u
			abarnfieldc0
MISSION_CRITICAL	21.147.198.34	92.158.1.199	abeckittal
HIGH	66.116.237.243	192.95.144.16	abelford8b
MISSION_CRITICAL	131.108.235.24	100.175.26.27	ablowendm
MEDIUM	69.26.80.147	85.186.56.243	aborrott4y
HIGH	35.119.23.52	251.232.128.63	abrackenda
HIGH	173.22.108.57	215.22.68.210	achuneyaf
MEDIUM	62.162.45.52	11.31.14.79	aclarricoates
LOW	111.240.167.189	25.157.145.200	aclimpson0
			acommucci57
LOW	112.161.245.112	243.51.87.5	acornelius93
LOW	126.182.32.7	78.59.33.219	aderuggero3
MISSION_CRITICAL	93.61.85.255	110.116.227.202	adilliwaybq
MISSION_CRITICAL	32.247.201.185	218.0.235.96	adrable9z
HIGH	119.143.207.46	165.128.18.99	adrought6c
MEDIUM	165.119.91.55	133.27.120.40	afosse7j





Acknowledgements

- Dr. Ewa Syta
- Continued support and mentorship
- Hybrid Pathways
- Guidance and cybersecurity scenarios
- Travelers
- Funding our pursuit of knowledge



