



Carson Kramer

IS INTERN SUMMER 2023

IDENTITY ACCESS MANAGEMENT, SECURITY OPERATIONS, AND
VULNERABILITY MANAGEMENT TEAMS

Identity Access Management

Director: Kevin McCullough

Reported to: Seth Brenneman, Sarah Garman

- Developed/Tested/Delivered RPA UiPath bot
 - Automated account provisioning and deprovisioning for Fluency Direct
 - 111 requests received per week

Impact: Saving 635 hours a year of manual account provisioning



Security Operations (Part 1)

Sr. Manager: Jeremy Smith

Reported to: Doug Myers, Suraj Patel

- CREATED: “Day in the life of a Device” Splunk Dashboard
 - Details about device involved in investigation
 - Provides: Compliance state, AV/Carbon Black install, DLP Protection, DLP Events, EDR alerts, Helpdesk, User & Vulnerabilities
- CREATED: “Device Traffic” Dashboard
 - Shows successful and blocked traffic to/from a device IP
- CREATED: Splunk Alert Summery Report and Dashboard
 - Daily email reporting alerts from last 24 hours
 - Identify increased amounts of a given alert type
 - Allows users to see trends over different windows of time



“Day in the life
of a Device”
Splunk
Dashboard

Investigator - Device Details

Day in the life of a device. Enter either a Host Name or Host IP

Week to date

Host Name
djmyers

Host IP
192.168

Hide Filters

djmyers

Device Type

OS

Windows 10

Compliance

Metric	Last Update Time	Compliance State
Endpoint	2023-	
Endpoint	2023-	
Endpoint	2023-	
Endpoint	2023-	

DLP Incidents

No results found.

Alerts - Carbonblack

Computer Name	Reason	Severity	Count
SELECT\	The application invoked a system application on behalf of		
SELECT\	The application attempted to modify the system configuration.		
SELECT\	The application invoked another application		

Authentication

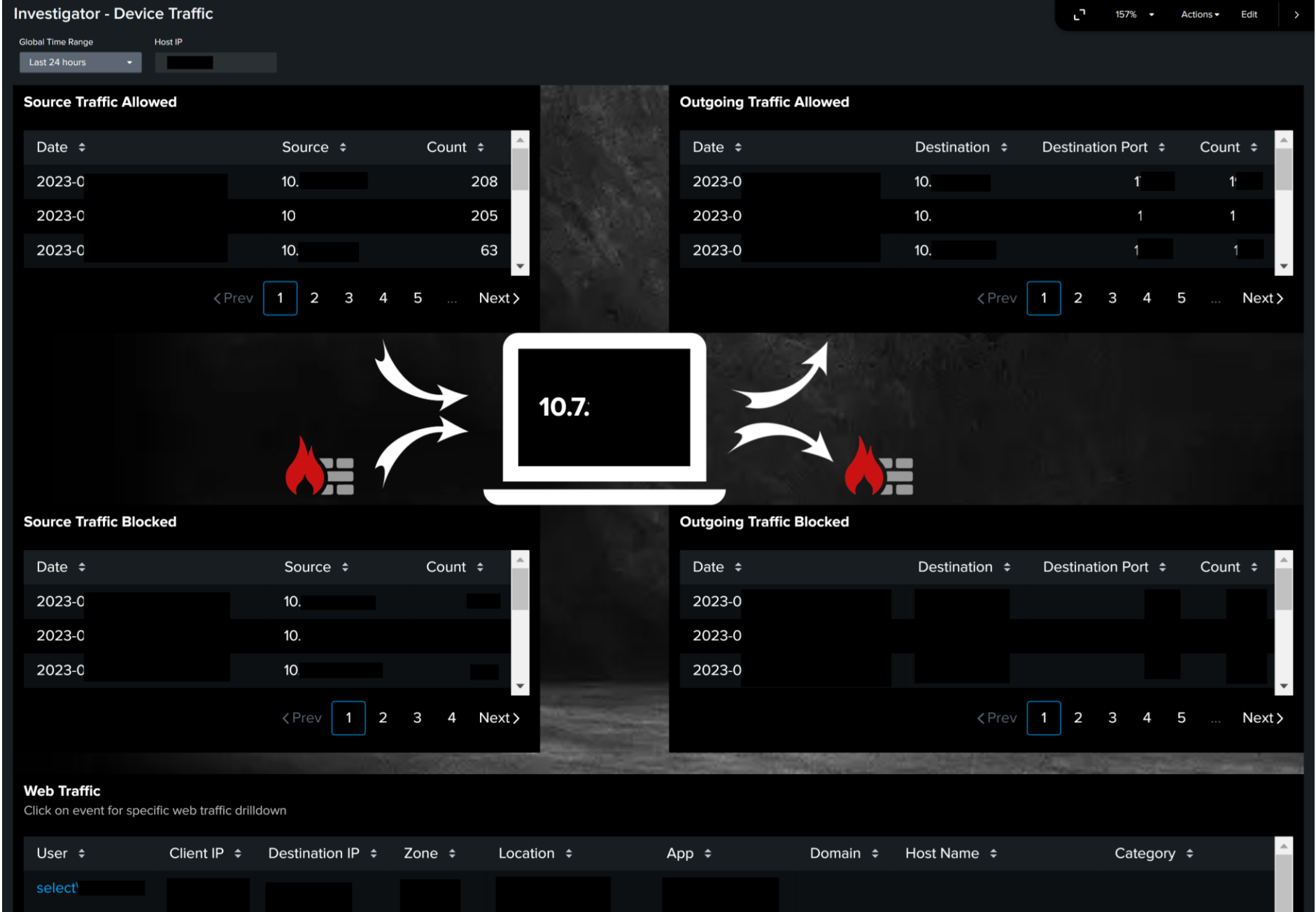
src_ip	User	Login Time	Status
192.168		2023	
192.168		2023	
192.168		2023	
192.168		2023	
192.168		2023	
192.168		2023	
192.168		2023	
192.168		2023	
192.168		2023	

Qualys

QID	Publish Date	Last Found Date	Severity
	20	20	
	20	20	
	20	20	
	10	20	

DLP Violations

No results found.



“Device Traffic”
Splunk
Dashboard

Security Operations (Part 2)

Sr. Manager: Jeremy Smith

Reported to: Doug Myers, Suraj Patel, Lance Dibblee

- SUPPORTED: Existing Dashboard Enhancement
 - Forescout Datacenter IP Blocks Dashboard
- SUPPORTED: Cloudflare DNS Migration
 - API import of 225 parked domains from CSC to Cloudflare for DNS



Vulnerability Management

Sr. Manager: Dan Klinger

Reported to: Kevin Thomas, Jayson Coulter

- **CREATED:** WAS Sitecore Apps Dashboard
 - Provides result analysis for digital strategy / marketing
- **SUPPORTED:** Prosthetic Solutions Burp Suite Pen Test
 - Confirmation and remediation of flagged vulnerabilities from Qualys
- **SUPPORTED:** Risk Assessment for Prosthetic Solutions
 - Created Qualys and Burp Suite reports for 3rd party development teams





Any

All

Last 30 Days



Total Widgets Count: 8 / 80

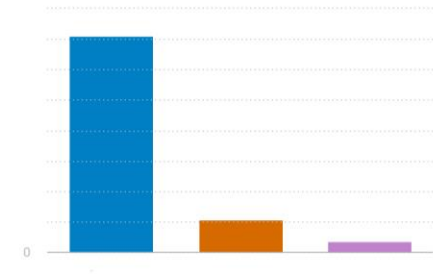


TOTAL APPLICATIONS SCANNED

TOTAL VULNERABILITIES

HIGH SEV VULNS

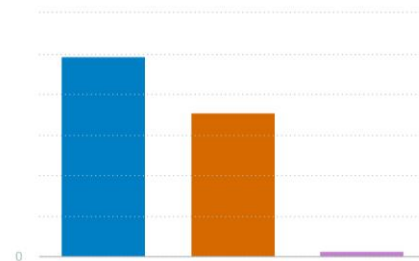
VULNERABILITIES BY STATUS



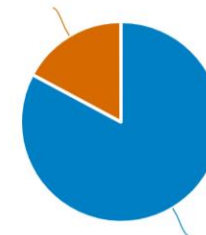
VULNERABILITY AGE

VULNERABILITY AGE	COUNT
[181 .. +]	0
[91 .. 180]	0
[61 .. 90]	0
[31 .. 60]	0
[0 .. 30]	0

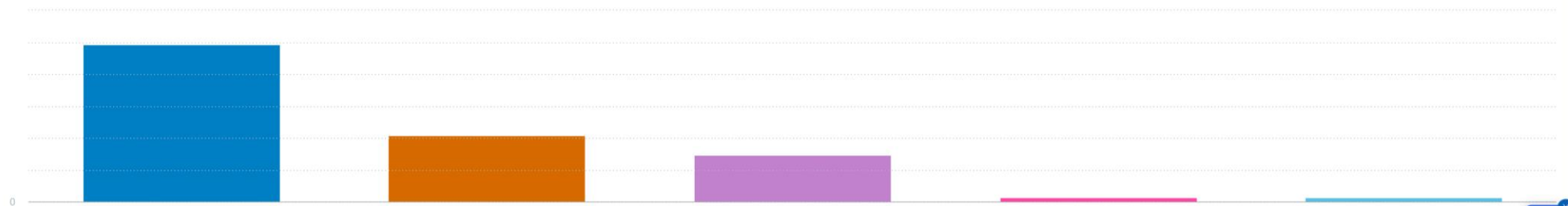
VULNERABILITIES BY GROUP



FINDINGS BY SEVERITY



OWASP TOP 10 2021 VULNERABILITIES



WAS
Sitecore
Apps
Dashboard

Internship Key Takeaways



- Applying classroom concepts in real-world scenarios
- Teamwork and collaboration in a hybrid work environment
- Cybersecurity importance and practical integration in business
- System development life cycle and code review process (UIPath)
- Log management and search filtering techniques (Splunk)
- How to use industry standard open source tools to identify and exploit vulnerabilities (Burp Suite)

Q & A

