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)

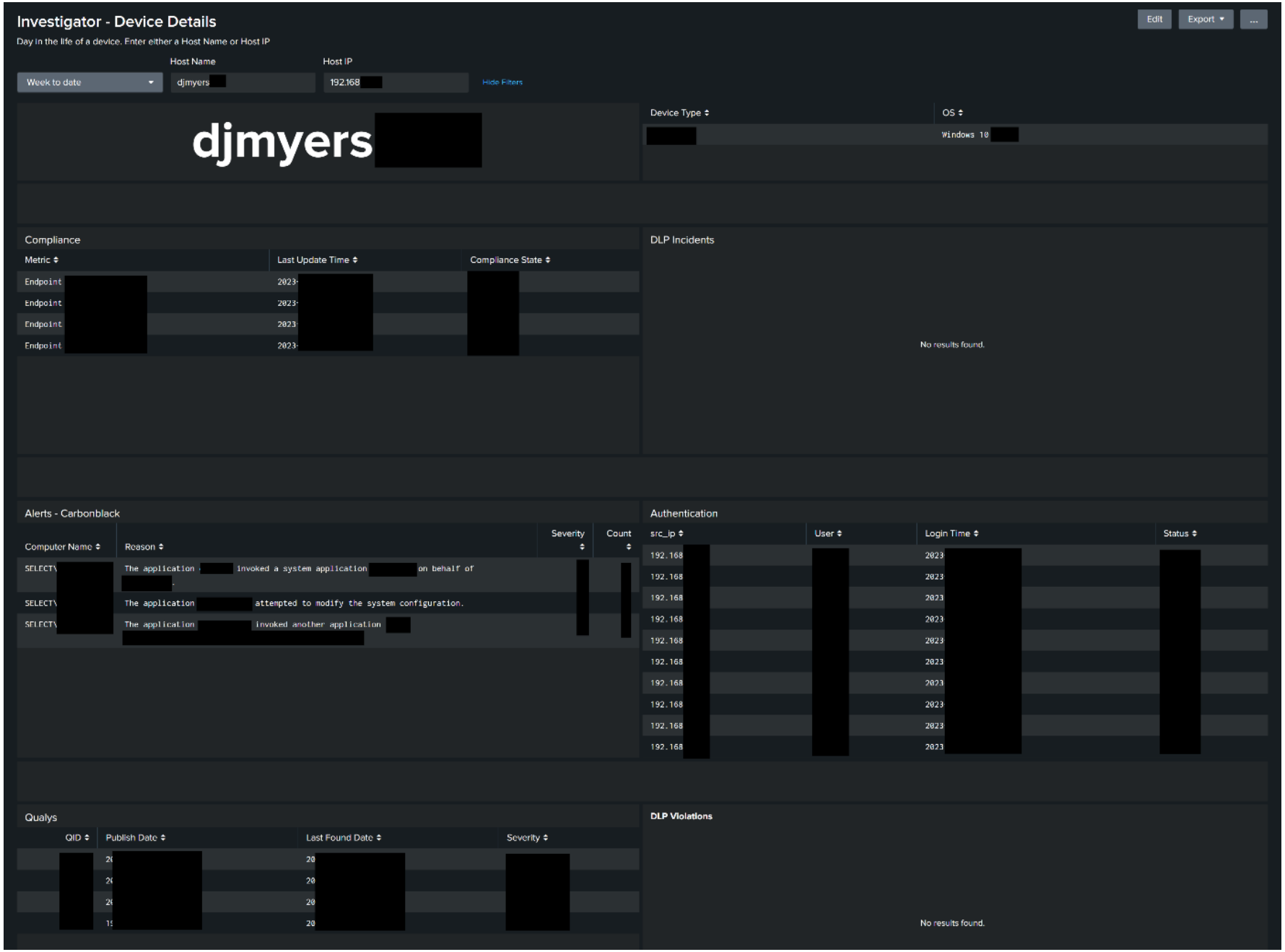
Sr. Manager: Jeremy Smith

Reported to: Doug Myers, Suraj Patel

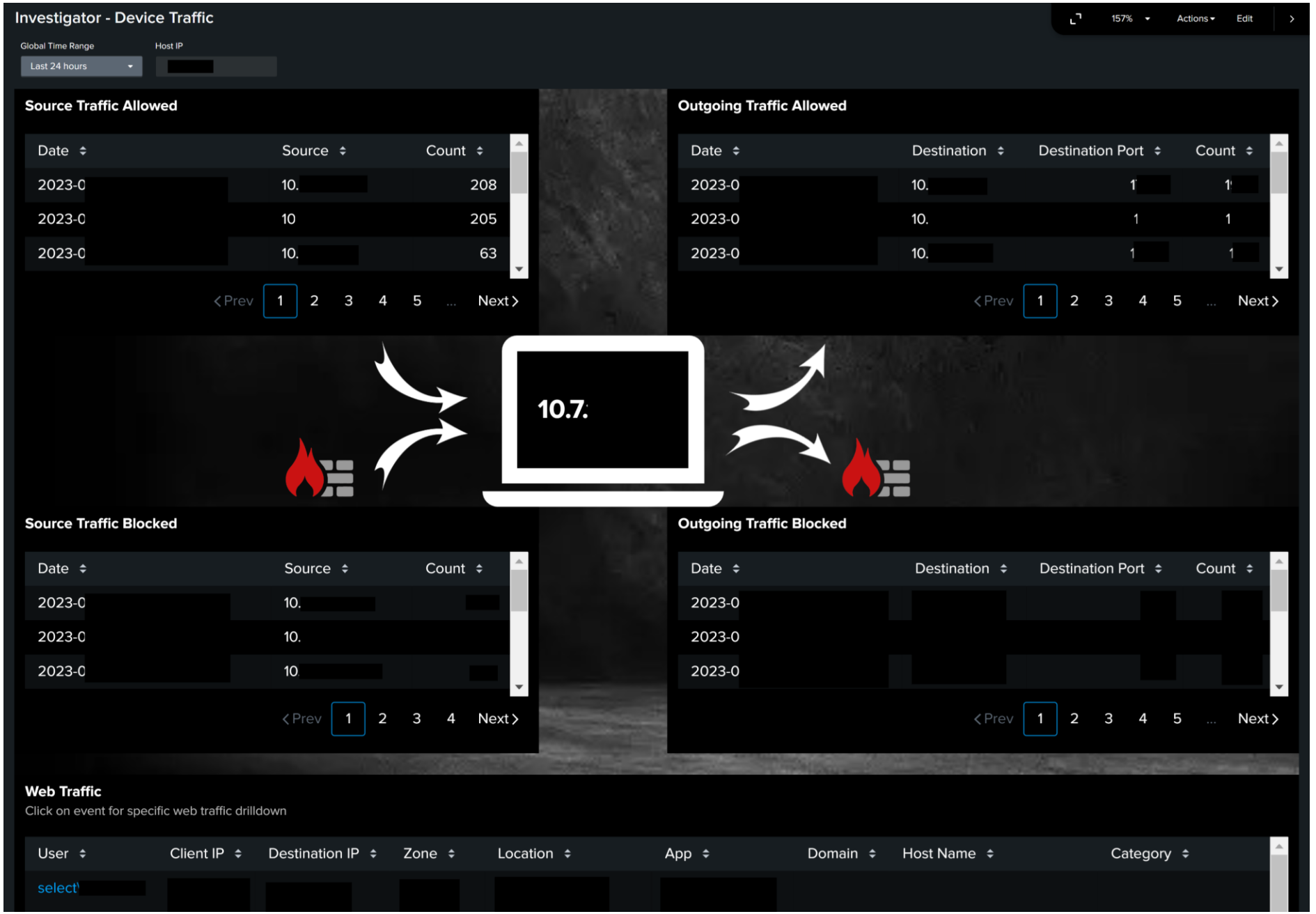
- CREATED: “Day in the life of a Device” Splunk Dashboard
  - Details about device involved in investigation
  - Provides: Compliance state, AV/Carbon Black install, DLP Protection, DLP Events, EDR alerts, Helpdesk, User & Vulnerabilities
- CREATED: “Device Traffic” Dashboard
  - Shows successful and 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

splunk>

“Day in the life of a Device” Splunk Dashboard



“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

CLOUDFLARE®

Vulnerability Management

Sr. Manager: Dan Klinger

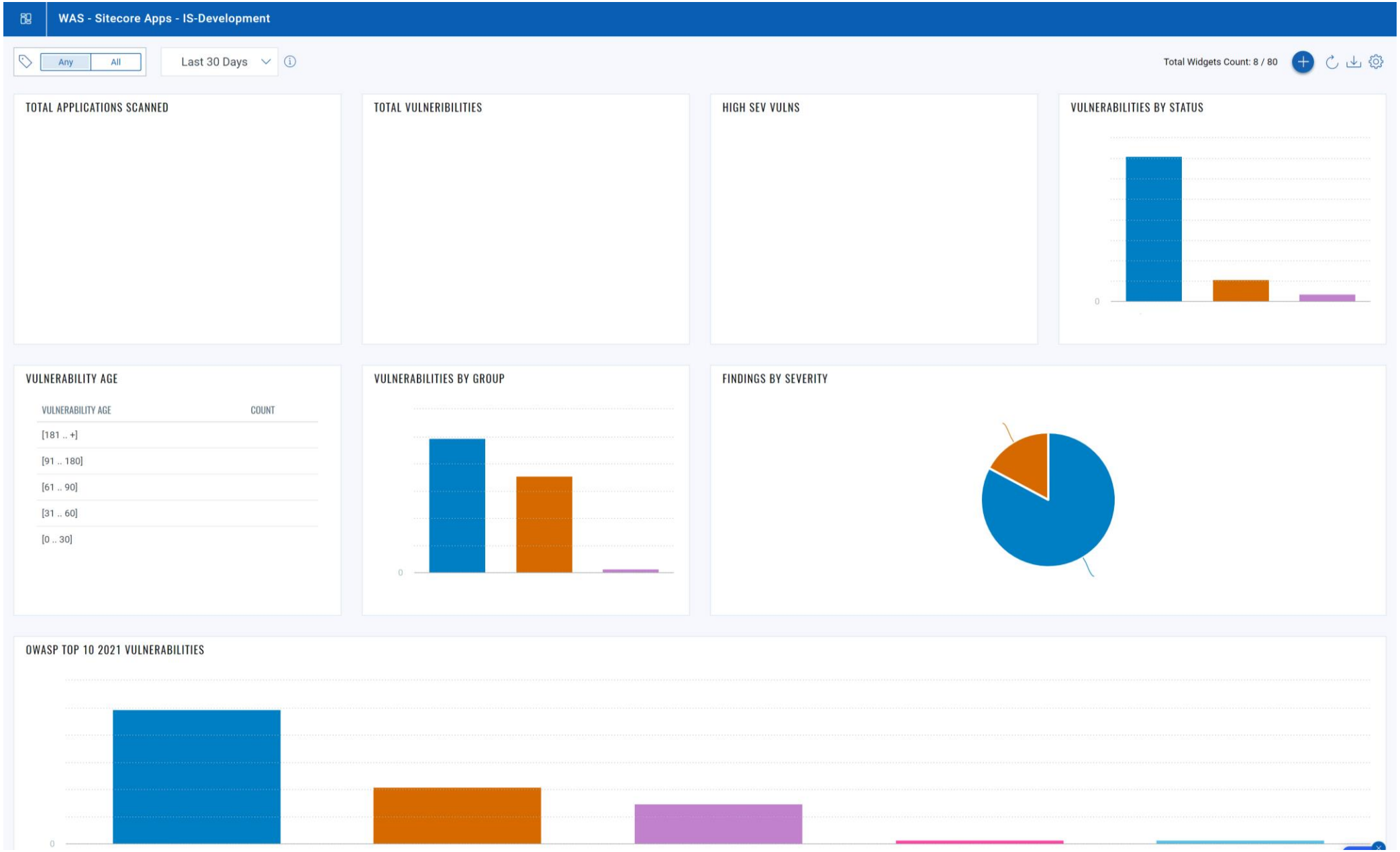
Reported to: Kevin Thomas, Jayson Coulter

- 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

Qualys.

BURPSUITE

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