PowerBI Cybersecurity Dashboard

Mayah Bosworth

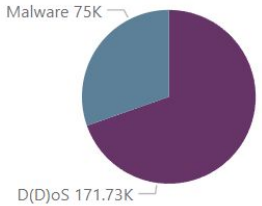
Company Software Security Analysis Dashboard: Overview

Instances Captured

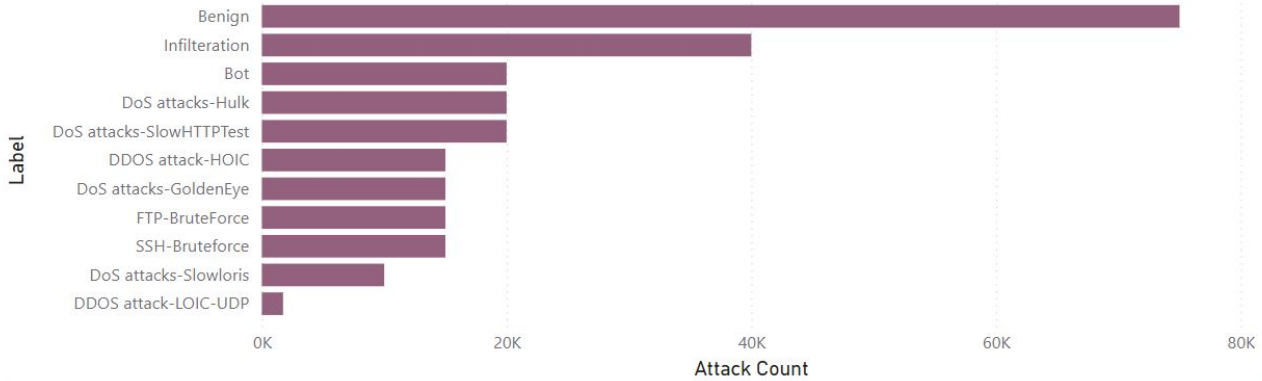
247K

Attack Count by Attack Category

Method of Attack



Attack Count by Label

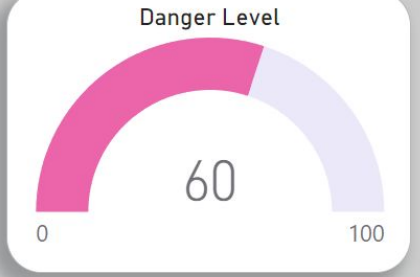


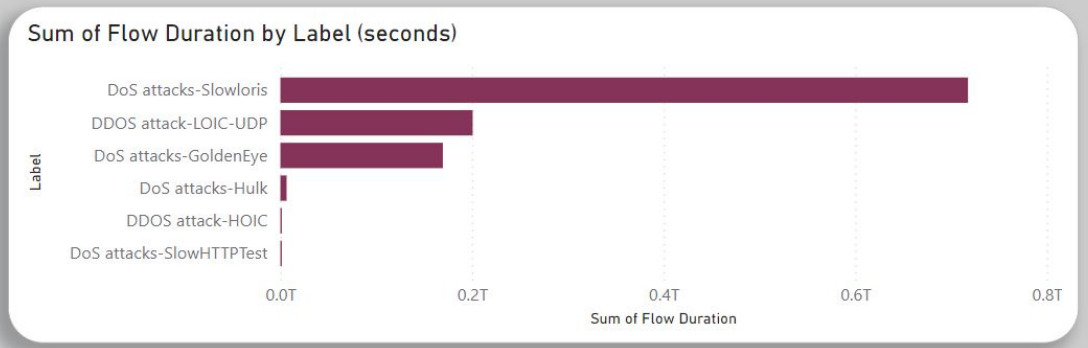
Company Security Analysis: D(D)oS Attacks

Active / Idle Time Detected

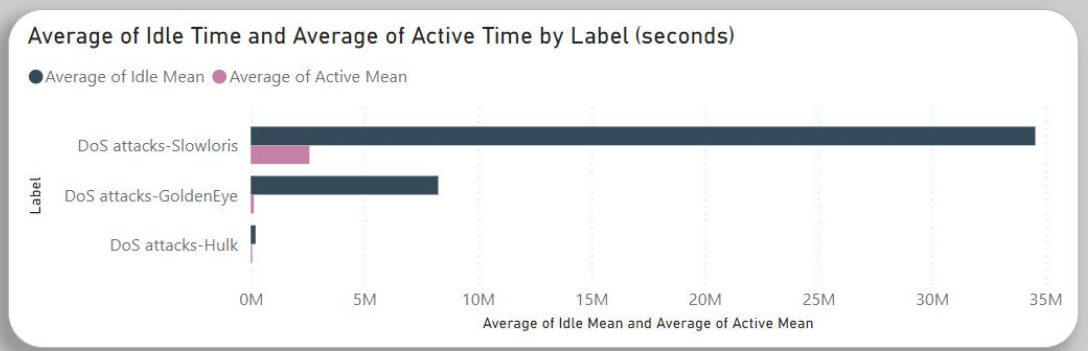
No Active / Idle Time Detected

Active / Idle Time Detected





- Disrupt service availability
- Periods of activity and rest (harder to detect)

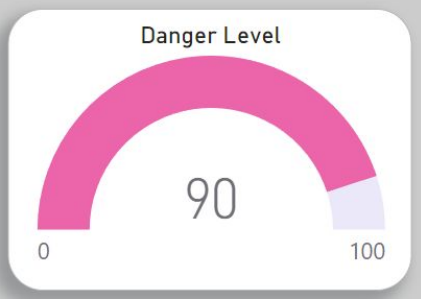


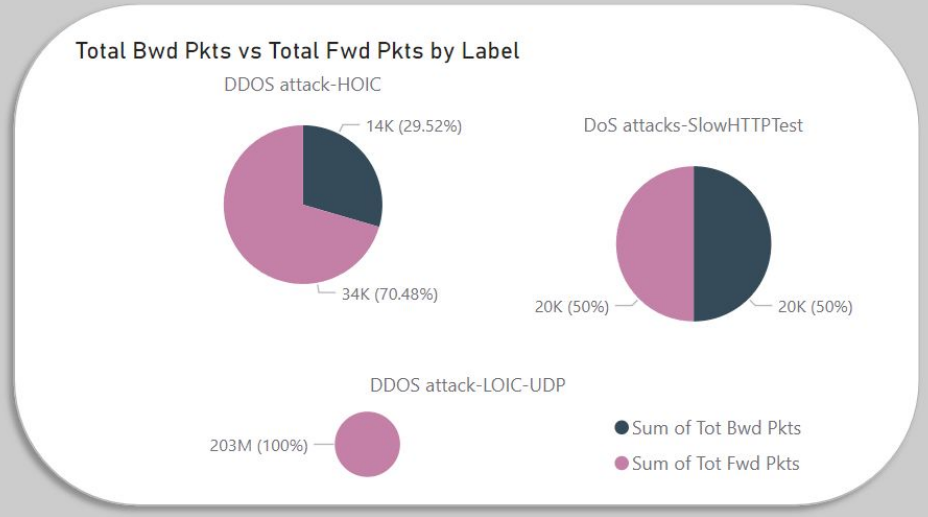
Company Security Analysis: D(D)oS Attacks

Active / Idle Time Detected

No Active / Idle Time Detected

No Active / Idle Time Detected





- Prolonged connectivity
- High volume of packets
- Immediate service disruption

DDOS attack-HOIC

48K

Sum of Total Packets

DDOS attack-LOIC-UDP

203M

Sum of Total Packets

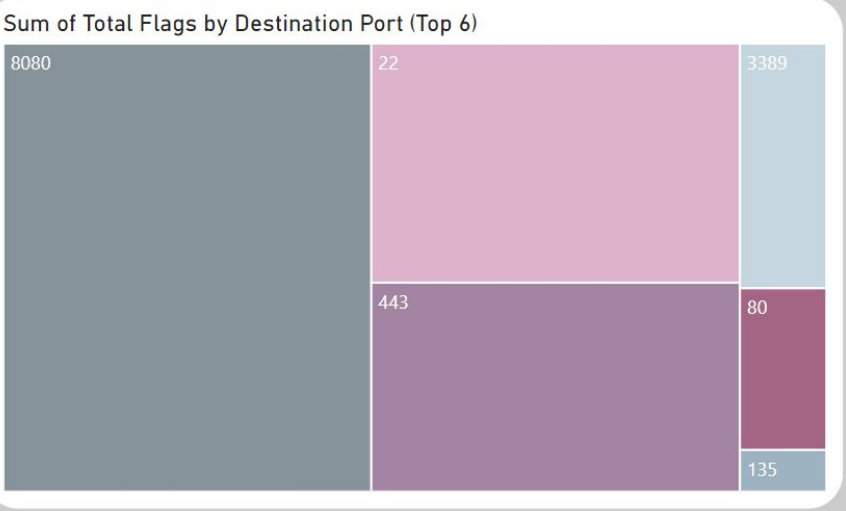
DoS attacks-SlowHTTPTest

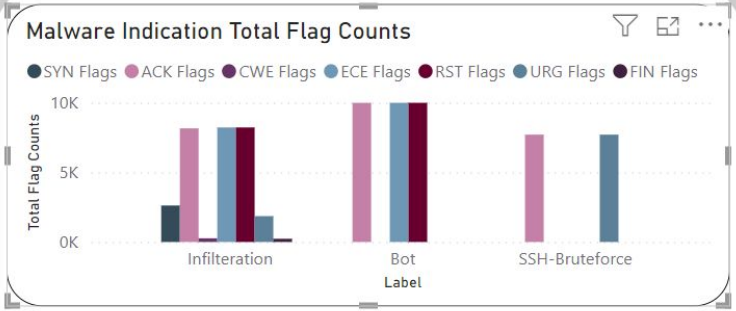
40K

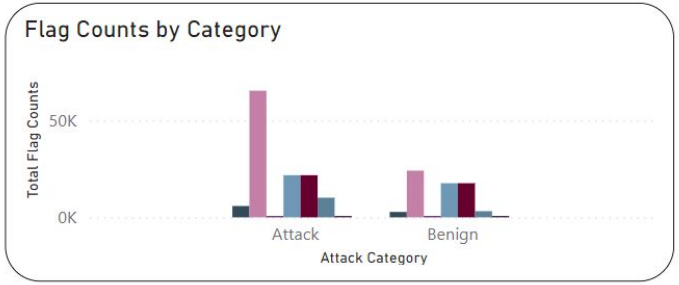
Sum of Total Packets

Company Security Analysis: Malware

Malware Overall







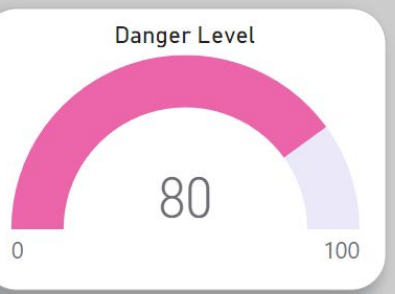
Company Security Analysis: Malware

Malware Overall

Web Traffic

Remote Network & Access Managment

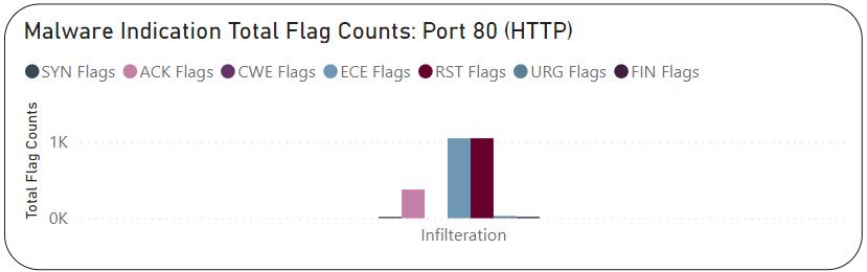
Web Traffic

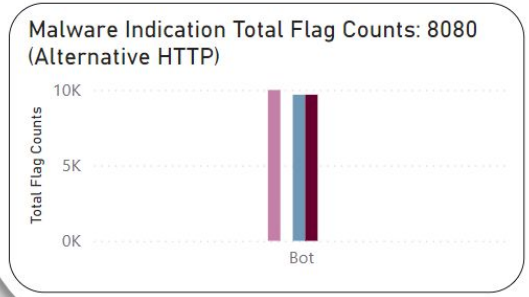


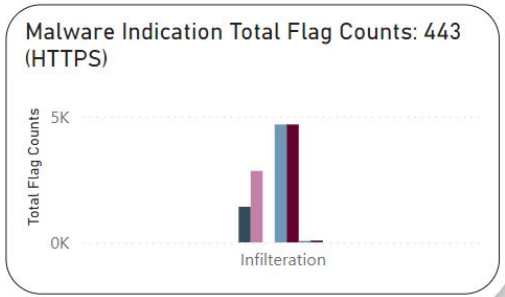
Port 80 (HTTP Web Traffic):
- No SYN flags indicate overwhelming existing browser connections

Port 8080 (Alternative HTTP Web Traffic)
- Disruption for dev and/or testing webpages

Port 443 (HTTPS Web Traffic):
- SYN and ACK flags indicate successful connections
- Prone to data exploitation

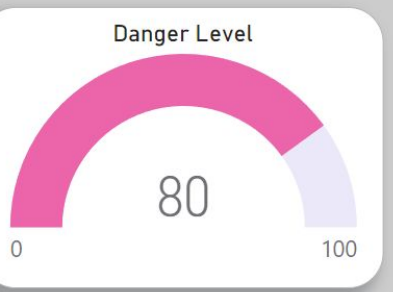






Company Security Analysis: Malware

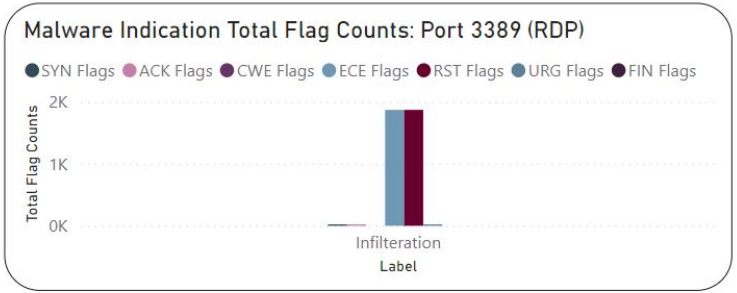
Remote Network & Access Management

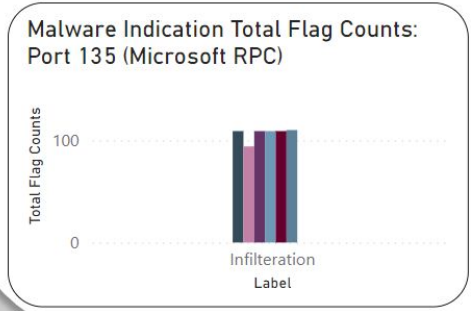


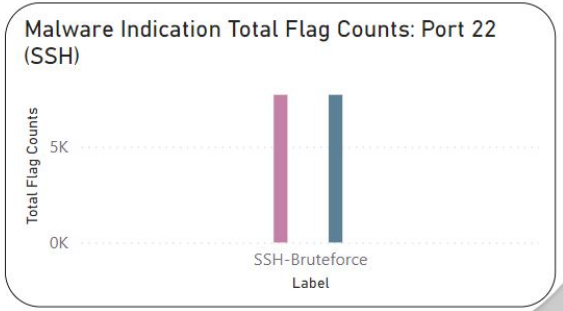
Port 3389 (Remote Desktop Protocol):
- High ECE and RST flags indicate network congestion

Port 135 (Microsoft Remote Procedure Call)
- No FIN flag indicates no closed connection

Port 22 (Secure Shell):
- High ACK and URG flags indicate many log in attempts







Company Security Analysis: Recommendations and Ideal KPIs




Current Overall Company Danger Ranking

Step 1:
Install Anti-Malware Software

Projected Overall Company Danger Ranking

Step 2:
Install Web Application Firewalls

Projected Overall Company Danger Ranking

Step 3:
Rate Limiting for UDP Floods

Ideal Overall Company Danger Ranking