

CAE

TECHNOLOGY ON POINT

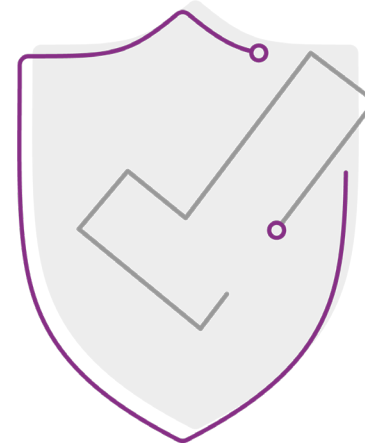
Cybersecurity Review

Company H

Cybersecurity Review

Prepared by: <Consultant>

Contact: cybersecurityreview@iamcae.com



Cybersecurity Review

This review provides analysis of applications, threat exposure and security risks at Company H and the customers connecting to their networks. The data used for this analysis was gathered by CAE Technology Services during the report period.



Cybersecurity Review

The report provides actionable intelligence and risk assessment around the applications, URL traffic, and types of content that are traversing the Company H network.



Executive Summary



Application Risk



Vulnerability Exploits



SaaS Applications



Malware



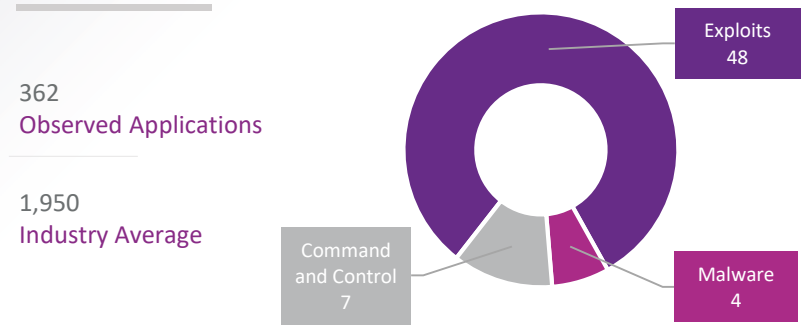
URL Activity



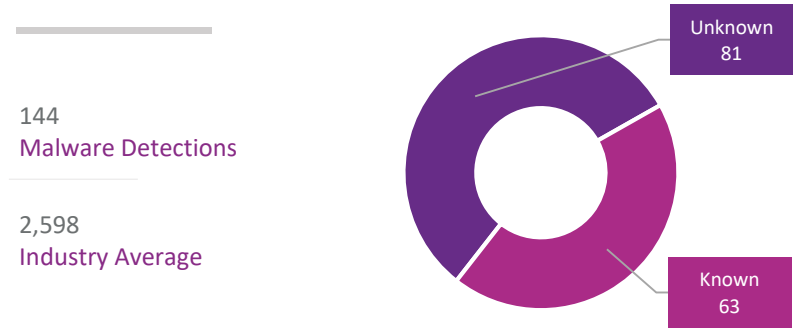
Recommendations

Executive Summary

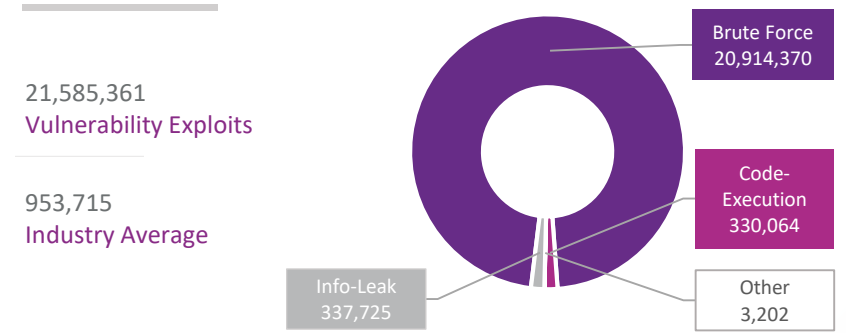
Applications Delivering Threats



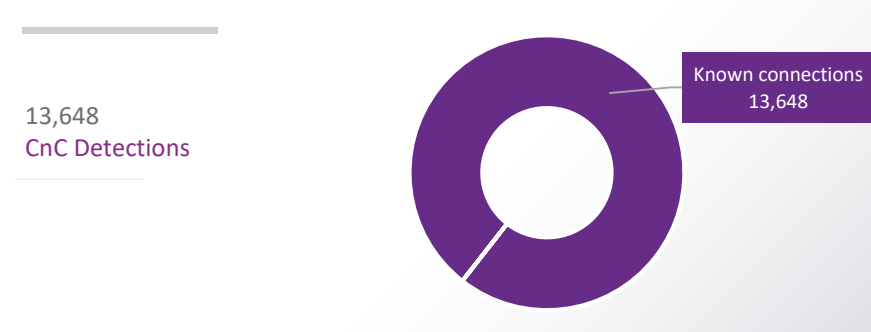
Title needed



Title needed

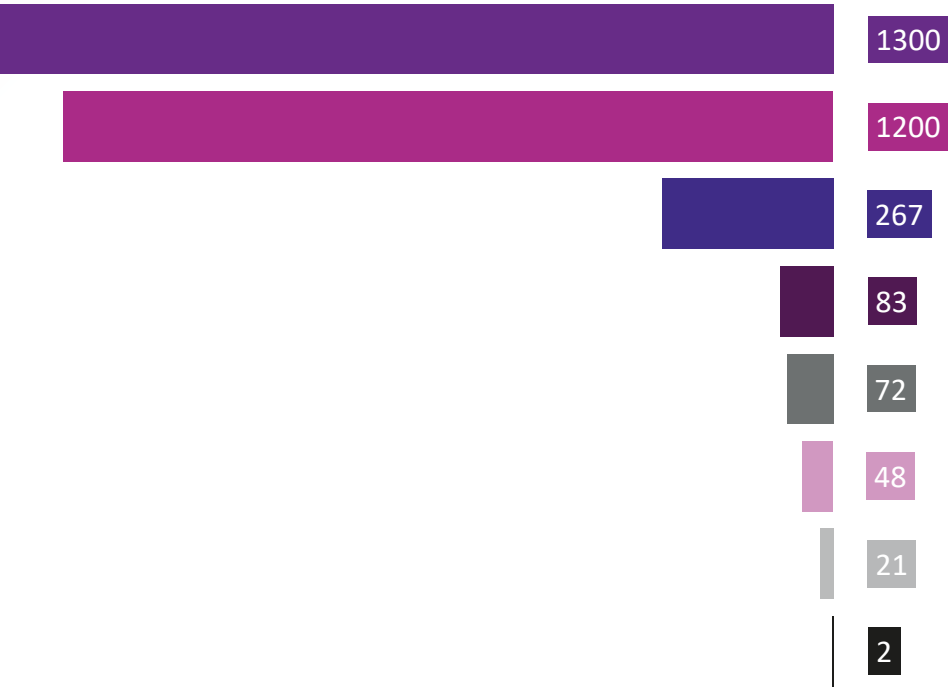


Title needed



Application Risk

Top 8 Applications Introducing Risk (Gigabytes)



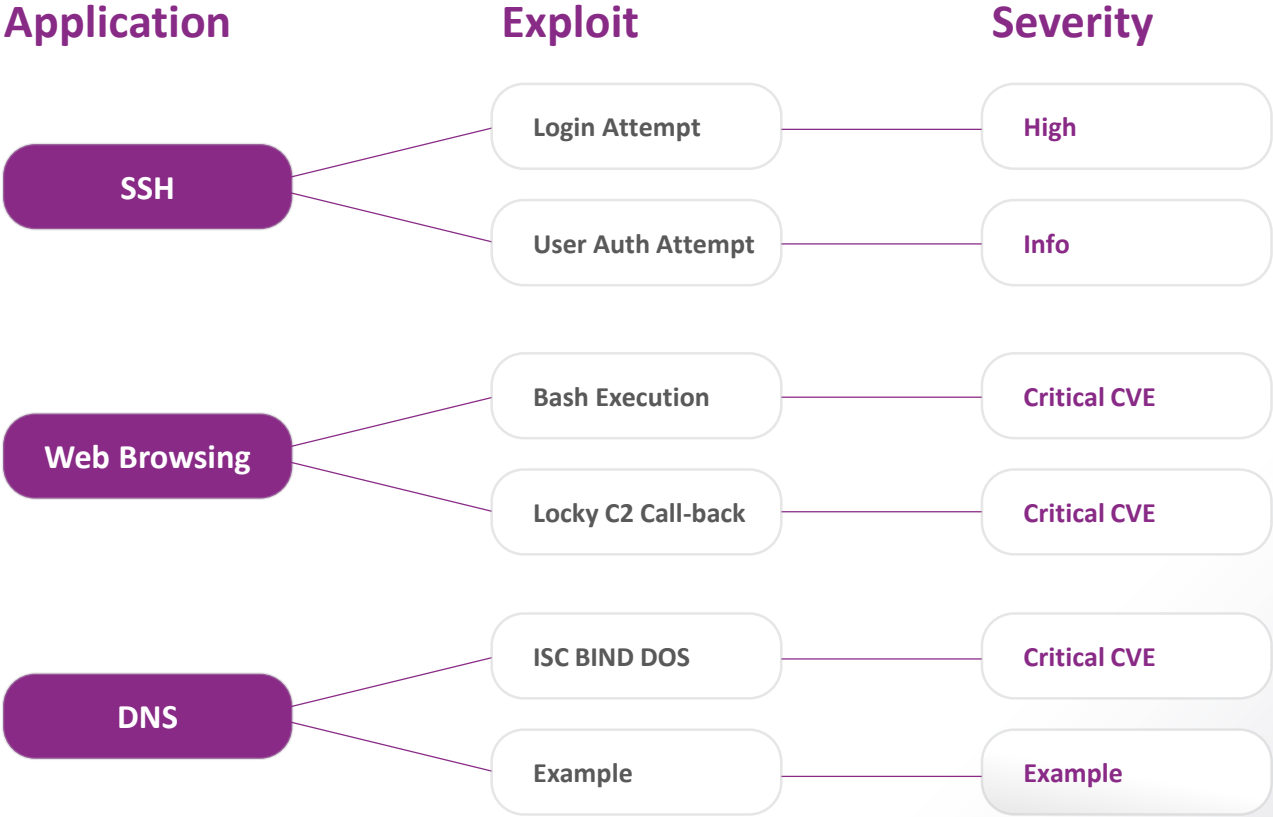
Highest Risk Level Apps Observed

Email	POP3	Hotmail
Encrypted-Tunnel	SSL	SSH
Remote-Access	MS-RDP	
File-Sharing	FTP	Google-Drive WEb
Photo-Video	YouTube-base	Facebook-video
Social-Networking	Facebook-base	
Instant-Messaging	Jabber	
Proxy	psiphon	http-proxy

Vulnerability Exploits

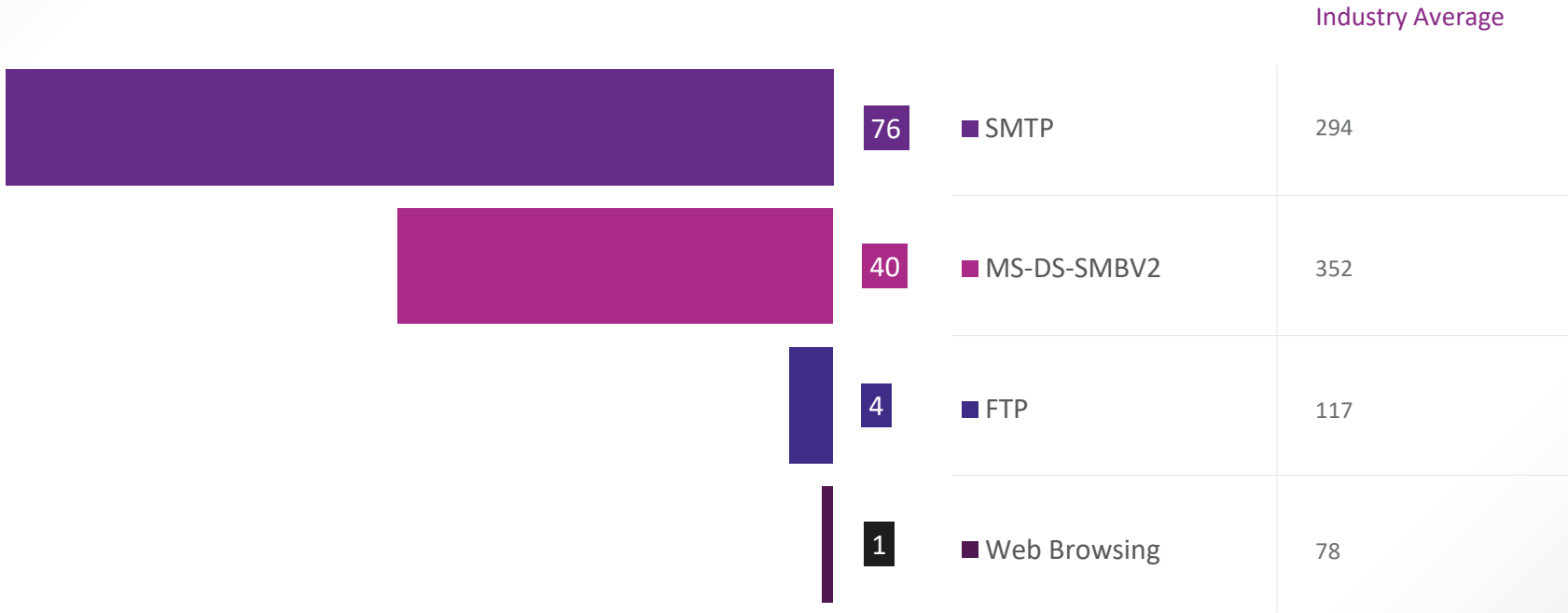


Top 3 Application Vulnerabilities



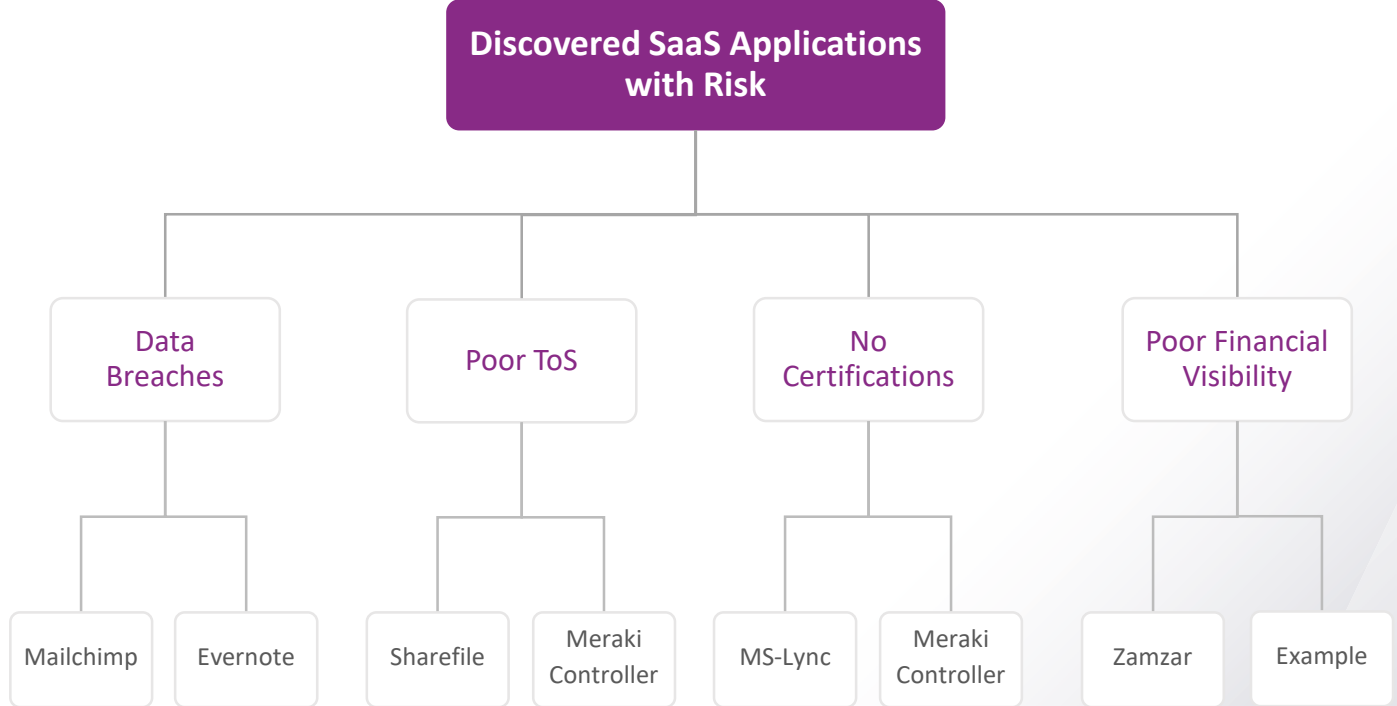
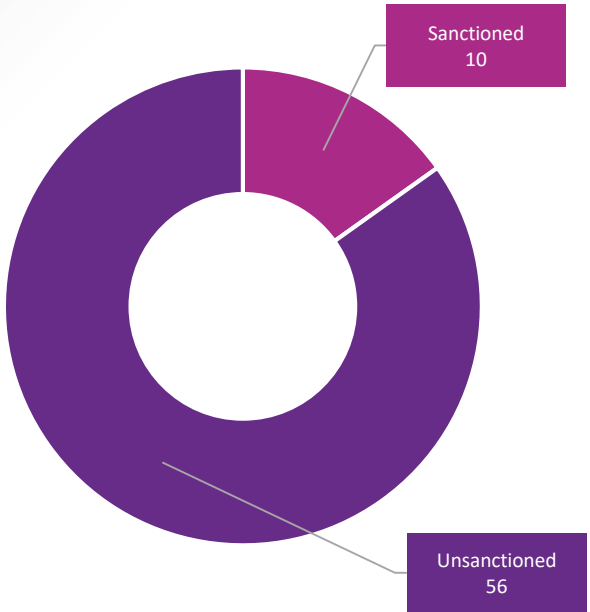
Malware

Count of Malware being Delivered Per Application



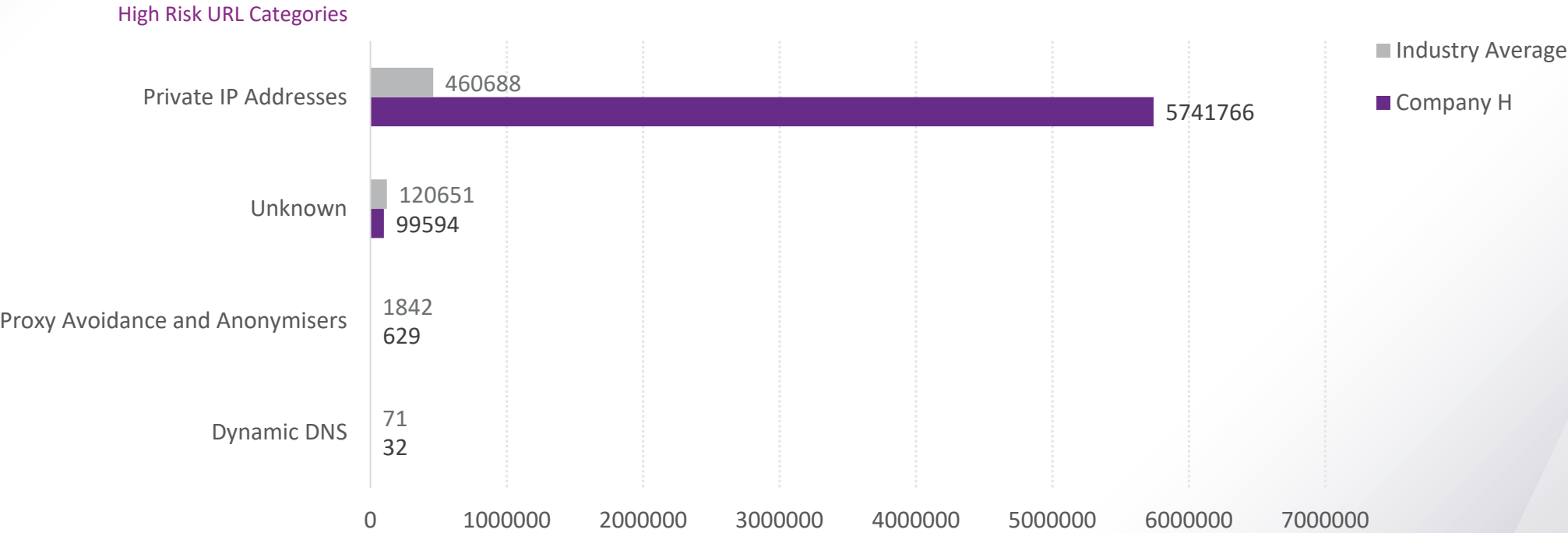
SaaS Applications

Discovered Software-as-a-Service Applications



URL Activity

Users visited a total of 66,118,379 URLs during the report time period across 59 categories



Recommendations



Application Visibility

- Implement policy based on applications rather than TCP or UDP ports
- Only allow applications that use default ports

High Risk Applications

- Deny or restrict
- Monitor or restrict unsanctioned SaaS applications

User Visibility

- Integrate a solution with directory services
- Implement policy based on user rather than host IP address or subnet

Threat Protection

- Deploy a solution that can use global threat intelligence to protect your environment from emerging threats
- Deploy threat and malware prevention to identify and block unknown and known threats

Restrict High Risk URLs

- Allow for fast blocking of undesired or malicious sites
- Support quick categorisation and investigation of unknowns

Alert and Report

- Alert the relevant systems and people when a threat is identified
- Schedule regular reporting to help identify trends and potential issues