DIGITAL DEFENSE®
INCORPORATED

Insight By Vertical Report

Report Data Source: Active View
Date Sourced: Wednesday, July 17, 2019

Prepared for: Demo Account
Businessgroup: Enterprise Admins
Date Generated: Monday, July 22, 2019
Data Options: Default | Include Acceptable Risk | 201 day window
9000 Tesoro Drive, Ste 100 San Antonio, TX 78217

1 Identification and Purpose

Frontline Insight provides peer analysis of Active View trending and statistical data. This document presents the most current findings as defined by the selected insight metric "Vertical: Uncategorized" for Demo Account.

The following sections provide a summary of findings that includes the Security GPA trend for Demo Account as compared to its peers as well as a breakdown of all peer groups and their current Security GPAs. Additionally, critical vulnerabilities for Demo Account and for its peers are also highlighted in detail.

2 Security GPA Breakdown By Vertical

Below is a depiction of the internal and external Security GPAs broken out by vertical. Demo Account has an external Security GPA of **0.00**, an internal unauth Security GPA of **1.09** and an internal overall Security GPA of **1.09**.

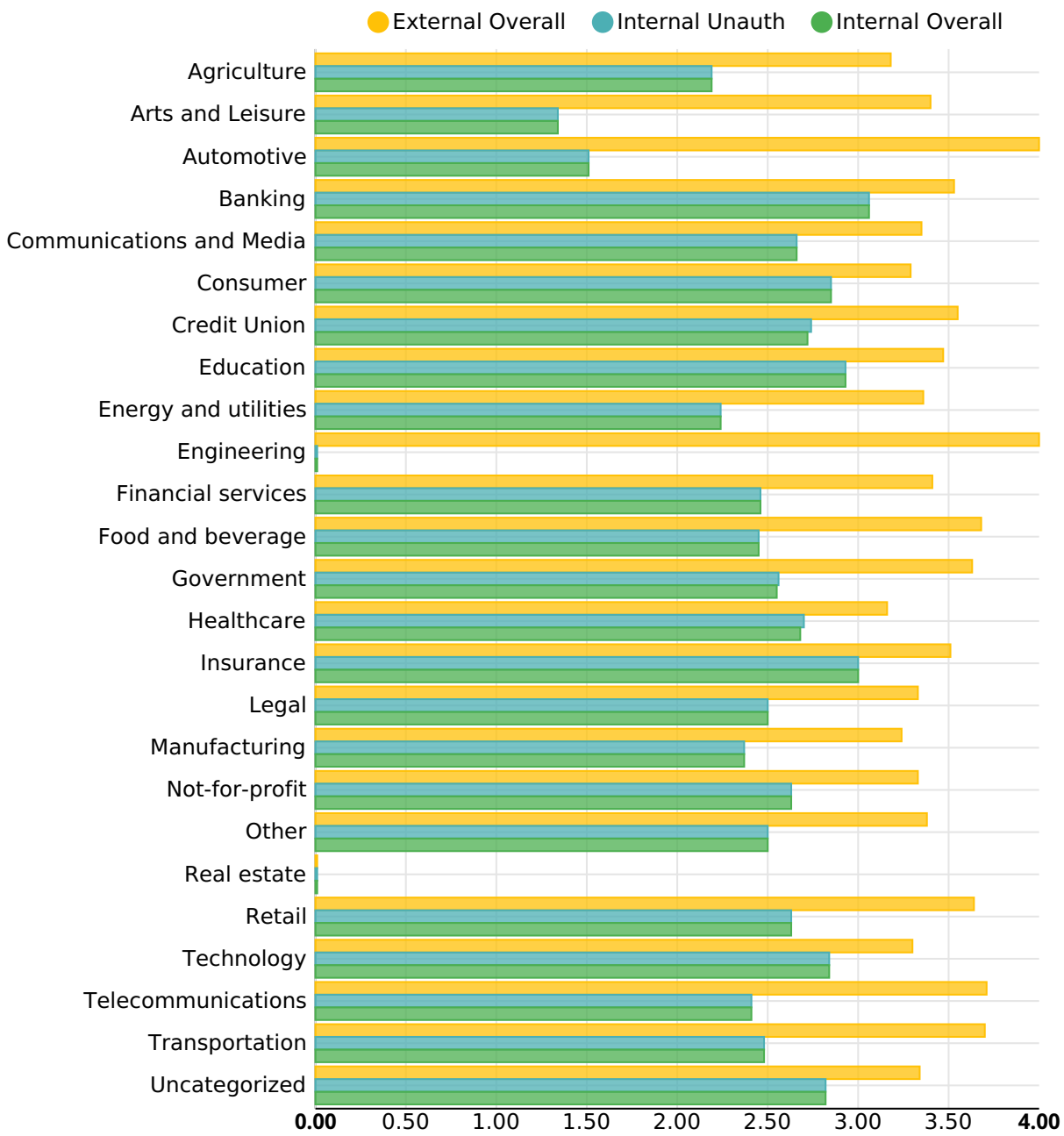

Figure 2 The bar chart depicts the current Security GPA across segmented vertical categories.

3 Detailed Peer Analysis By Vertical: Uncategorized

3.1 Trending Information

Trending provides a quick and easy way to see how well you are doing over time as compared to your peers in the Uncategorized category.

Security GPA Trends

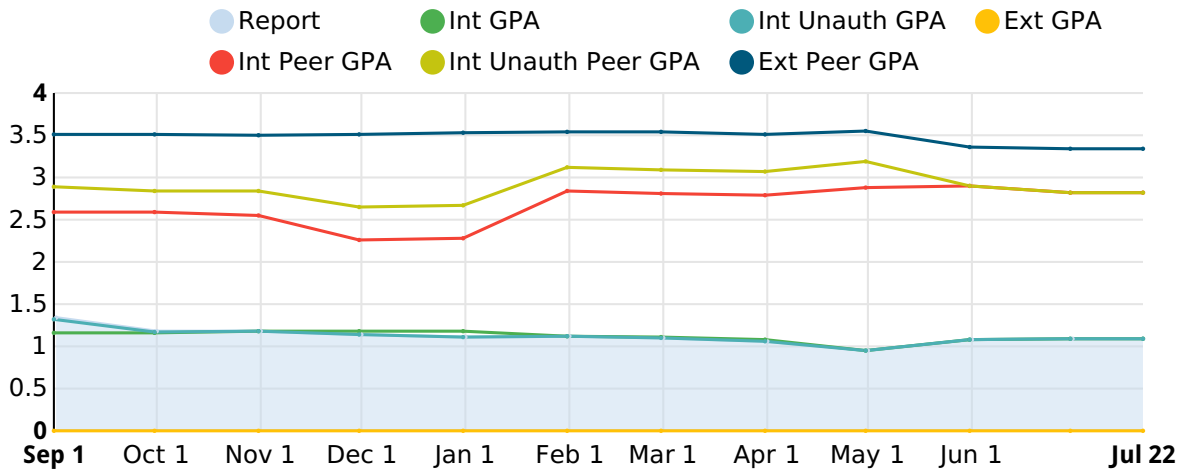

Figure : Security GPA trending graphs by vertical: Uncategorized shows trends over the past year as compared to your peers.

4 External Overall Peer Analysis

4.1 External Vulnerability Summary

This section covers unique top external vulnerabilities for the Uncategorized category. A list of top 5 external vulnerabilities segmented by severity are presented below as well as a side by side comparison of your individual top 5 external vulnerabilities for each severity segment to your peers.

#	Peer External Vulnerability	Your External Vulnerability	Severity
Critical Severity Top 5			
1	Client-Specific Application Vulnerability (Critical) (118677)	*N/A*	Critical
2	Adobe Coldfusion BlazeDS Deserialization RCE (123782)	*N/A*	Critical
3	MS17-010: SMB Remote Code Execution Vulnerability (Network Check) (122051)	*N/A*	Critical
4	Unix Server Common Password (100151)	*N/A*	Critical
5	HTTP Server "ShellShock" BASH Command Injection Vulnerability (116792)	*N/A*	Critical
High Severity Top 5			
1	Client-Specific Application Vulnerability (High) (101897)	*N/A*	High
2	Apache HTTP Server 'ap_get_basic_auth_pw' Authentication Bypass (290284)	*N/A*	High
3	Web Server Cross-Site Scripting (104554)	*N/A*	High
4	OpenSSH Security Bypass Vulnerability (126647)	*N/A*	High
5	OpenSSH 'session.c' Local Security Bypass Vulnerability (126635)	*N/A*	High
Medium Severity Top 5			

1	SSL Connection: SSLv3 CBC Mode Cipher POODLE Vulnerability (116818)	*N/A*	Medium
2	Web Server Generates CORS Headers Using User Supplied Values (122550)	*N/A*	Medium
3	SSL Connection: Server Vulnerable to DROWN Attack (119065)	*N/A*	Medium
4	Slowloris Resource Depletion And Denial Of Service (104012)	*N/A*	Medium
5	SSL Connection: TLS CBC Mode Cipher ZOMBIE POODLE Vulnerability (128820)	*N/A*	Medium

4.2 Time To Fix External Vulnerabilities

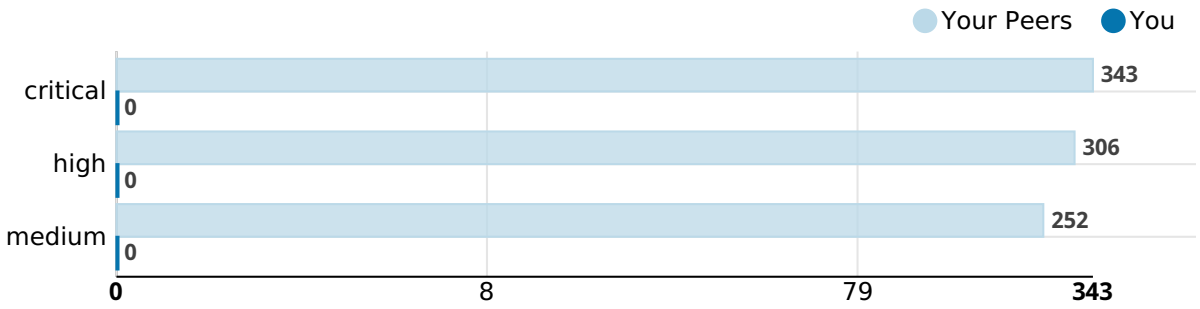

Figure 4.2 The bar chart depicts the time to fix external vulnerabilities by severity for you and your peers in the Uncategorized category.

5 Internal Unauth Only Peer Analysis

5.1 Unauth Internal Vulnerability Summary

This section covers unique top unauth internal vulnerabilities for the Uncategorized category. A list of top 5 unauth internal vulnerabilities segmented by severity are presented below as well as a side by side comparison of your individual top 5 unauth internal vulnerabilities for each severity segment to your peers.

#	Peer Unauth Internal Vulnerability	Your Unauth Internal Vulnerability	Severity
Critical Severity Top 5			
1	MS19-MAY: Microsoft RDP 'BlueKeep' Unauthenticated Remote Code Execution (Network Check) (128831)	Easily Guessable SSH Credentials (104120)	Critical
2	MS17-010: SMB Remote Code Execution Vulnerability (Network Check) (122051)	MS17-010: SMB Remote Code Execution Vulnerability (Network Check) (122051)	Critical
3	Cisco Smart Install Multiple Vulnerabilities (122875)	SSL Connection: Server Vulnerable to Heartbleed Attack (113790)	Critical
4	Ricoh Printer Web Image Monitor Default Credentials (112310)	MS08-067 Microsoft Windows Server Service Stack Overflow (Network Check) (103802)	Critical
5	Passwordless Lantronix Device (101230)	MS19-MAY: Microsoft RDP 'BlueKeep' Unauthenticated Remote Code Execution (Network Check) (128831)	Critical
High Severity Top 5			
1	SNMP Writeable Communities (104067)	MS12-020 Remote Desktop Protocol Use-After-Free Vulnerability (Network Check) (104735)	High
2	OpenSSH Security Bypass Vulnerability (126647)	MS15-034: Microsoft IIS HTTP.sys Remote Code Execution (Network Check) (117590)	High
3	OpenSSH 'ssh-agent.c' Untrusted Search Path Vulnerability (283439)	Easily Guessable Telnet Credentials (111915)	High
4	OpenSSH 'session.c' Local Security Bypass Vulnerability (126635)	Windows 10 End of Life (125528)	High

5	OpenSSH X11 Forwarding Access Bypass (276485)	Web Server Directory Traversal (100905)	High
Medium Severity Top 5			
1	SNMP Default Communities (100149)	MS16-047: Windows SAM and LSAD Downgrade Vulnerability - Badlock (Network Check) (121756)	Medium
2	OpenSSH kex.c and packet.c NULL Pointer Dereference Denial of Service (299655)	MS11-030: Vulnerability In DNS Resolution Allows Remote Code Execution (Network Check) (104419)	Medium
3	OpenSSH 'before 7.6' 'process_open function in sftp-server.c' subcomponent Does not Properly Prevent Write Operations in Readonly Mode Vulnerability (296108)	MS10-012 Vulnerabilities In SMB Server Allow Remote Code Execution (Network Check) (104133)	Medium
4	OpenSSH Account Enumeration Vulnerability (126640)	MS12-020: Terminal Server Denial Of Service (Network Check) (104778)	Medium
5	OpenSSH User Enumeration Vulnerability (126863)	MS09-001 SMB Remote Code Execution (Network Check) (103879)	Medium

5.2 Time To Fix Unauth Internal Vulnerabilities

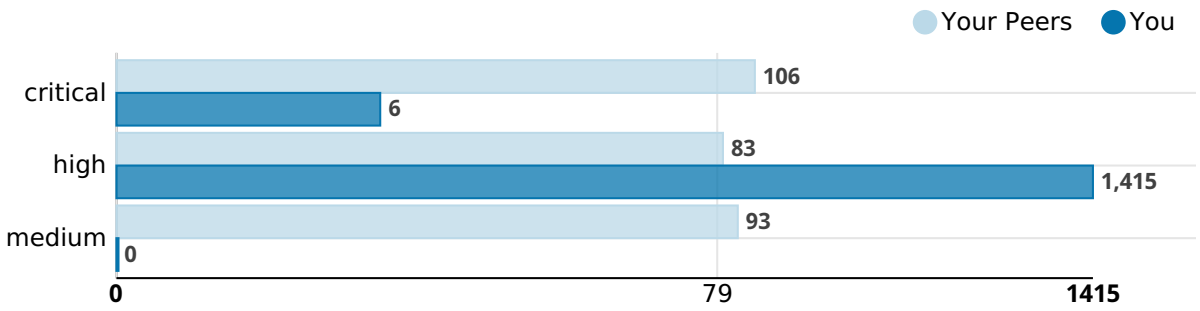

Figure 5.2 The bar chart depicts the time to fix unauth internal vulnerabilities by severity for you and your peers in the Uncategorized category.

6 Internal Overall Peer Analysis

6.1 Overall Internal Vulnerability Summary

This section covers unique top overall internal vulnerabilities for the Uncategorized category. A list of top 5 overall internal vulnerabilities segmented by severity are presented below as well as a side by side comparison of your individual top 5 overall internal vulnerabilities for each severity segment to your peers.

#	Peer Overall Internal Vulnerability	Your Overall Internal Vulnerability	Severity
Critical Severity Top 5			
1	MS19-MAY: Microsoft RDP 'BlueKeep' Unauthenticated Remote Code Execution (Network Check) (128831)	Easily Guessable SSH Credentials (104120)	Critical
2	MS17-010: SMB Remote Code Execution Vulnerability (Network Check) (122051)	MS17-010: SMB Remote Code Execution Vulnerability (Network Check) (122051)	Critical
3	Cisco Smart Install Multiple Vulnerabilities (122875)	SSL Connection: Server Vulnerable to Heartbleed Attack (113790)	Critical
4	Ricoh Printer Web Image Monitor Default Credentials (112310)	Threat Detected: Trojan Variant (126460)	Critical
5	Passwordless Lantronix Device (101230)	MS08-067 Microsoft Windows Server Service Stack Overflow (Network Check) (103802)	Critical
High Severity Top 5			
1	MS19-JUL: Microsoft Internet Explorer Security Update (129102)	MS12-020 Remote Desktop Protocol Use-After-Free Vulnerability (Network Check) (104735)	High
2	MS19-JUL: Microsoft Windows Security Update (129103)	MS15-034: Microsoft IIS HTTP.sys Remote Code Execution (Network Check) (117590)	High
3	SNMP Writeable Communities (104067)	Easily Guessable Telnet Credentials (111915)	High
4	MS19-JUN: Microsoft Windows Security Update (128962)	Windows 10 End of Life (125528)	High

5	MS19-JUN: Microsoft Internet Explorer Security Update (128961)	Web Server Directory Traversal (100905)	High
Medium Severity Top 5			
1	MS17-JUN: Microsoft Internet Explorer Security Update - Registry Entry Not Set (128597)	MS16-047: Windows SAM and LSAD Downgrade Vulnerability - Badlock (Network Check) (121756)	Medium
2	MS17-SEP: Microsoft Internet Explorer Security Update - Registry Entry Not Set (128598)	MS11-030: Vulnerability In DNS Resolution Allows Remote Code Execution (Network Check) (104419)	Medium
3	MS19-MAY: Microsoft Windows Security Update (ZombieLoad) - Registry Entry Not Set (128823)	MS10-012 Vulnerabilities In SMB Server Allow Remote Code Execution (Network Check) (104133)	Medium
4	SNMP Default Communities (100149)	MS12-020: Terminal Server Denial Of Service (Network Check) (104778)	Medium
5	MS18-NOV: Microsoft Windows Security Update - Registry Entry Not Set (128666)	Threat Scan: Unsigned Software Processes (127839)	Medium

6.2 Time To Fix Overall Internal Vulnerabilities

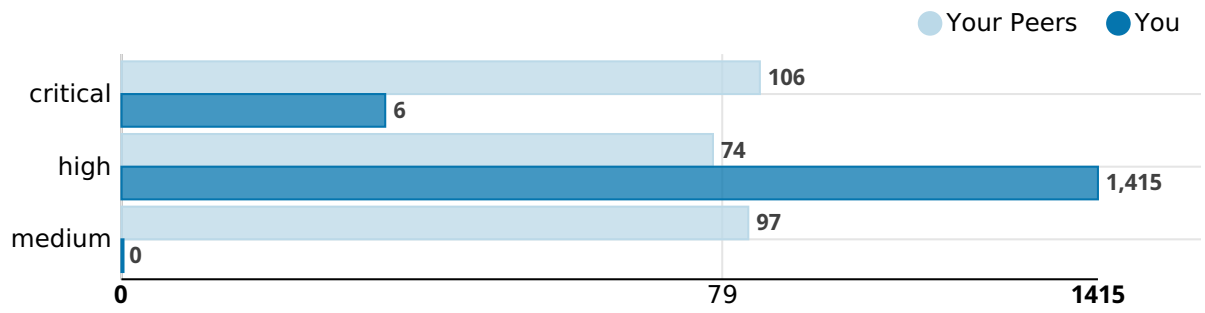

Figure 6.2 The bar chart depicts the time to fix overall internal vulnerabilities by severity for you and your peers in the Uncategorized category.