EXTERNAL ATTACK SURFACE THREAT INTELLIGENCE REPORT

Prepared for

SAMPLE

SAMPLE CORPORATION

Managed Asset/Domain:

SAMPLE.COM

Date: 1 September 2023
Revision: 1.0
Reference: SAMPLE/CODERED/2023/09/YM

PRIVATE AND CONFIDENTIAL

Confidentiality Notice

This document contains proprietary and sensitive information that is confidential to SAMPLE CORPORATION. Disclosure of this document in full or in part, may result in material damage to SAMPLE CORPORATION system. Written permission shall be obtained from SAMPLE CORPORATION prior to the disclosure of this document to third party.

This document is prepared and submitted by:
PROVINTELL TECHNOLOGIES SDN. BHD.
Co. Registration No. 1013237-V
F-68-2, Zenith Corporate Park, Jalan SS7/26, Kelana Jaya,
47301 Petaling Jaya, Selangor Darul Ehsan, MALAYSIA.
T: +603 7661 0891 F: +603 7661 0897
www.provintell.com

Information Security Management ISO 27001 Certified

LIMITATION OF USE AND DISCLOSURE

This document contains the sensitive and confidential information on the current security issues and risks of **SAMPLE**. PROVINTELL recommends that special precaution shall be taken to protect the confidentiality of the information contained in this document. PROVINTELL has securely retained a copy of this document for future reference. The softcopy of this document is protected by password and securely delivered by PROVINTELL representative to the appointed representatives of **SAMPLE** via email, secured file sharing and/or DVD. PROVINTELL does not recommend to print and deliver this document in hardcopy to minimize the risks of document mishandling, loss and theft.

While PROVINTELL is confident that the major security issues and risks have been identified and presented in this document for **SAMPLE**. There is no assurance that all the security issues and exposure risks can be identified in this report due to the limitations and constraints implied. The findings and recommendations provided in this document are based on the technologies and known security issues as of the date of this document. As the technologies and risks may change over time, deviation may occur in the findings and recommendations provided in this document.

ORGANIZATION BACKGROUND

Company Name: SAMPLE CORPORATION

Business Sector: Ecommerce

Domains: sample.com

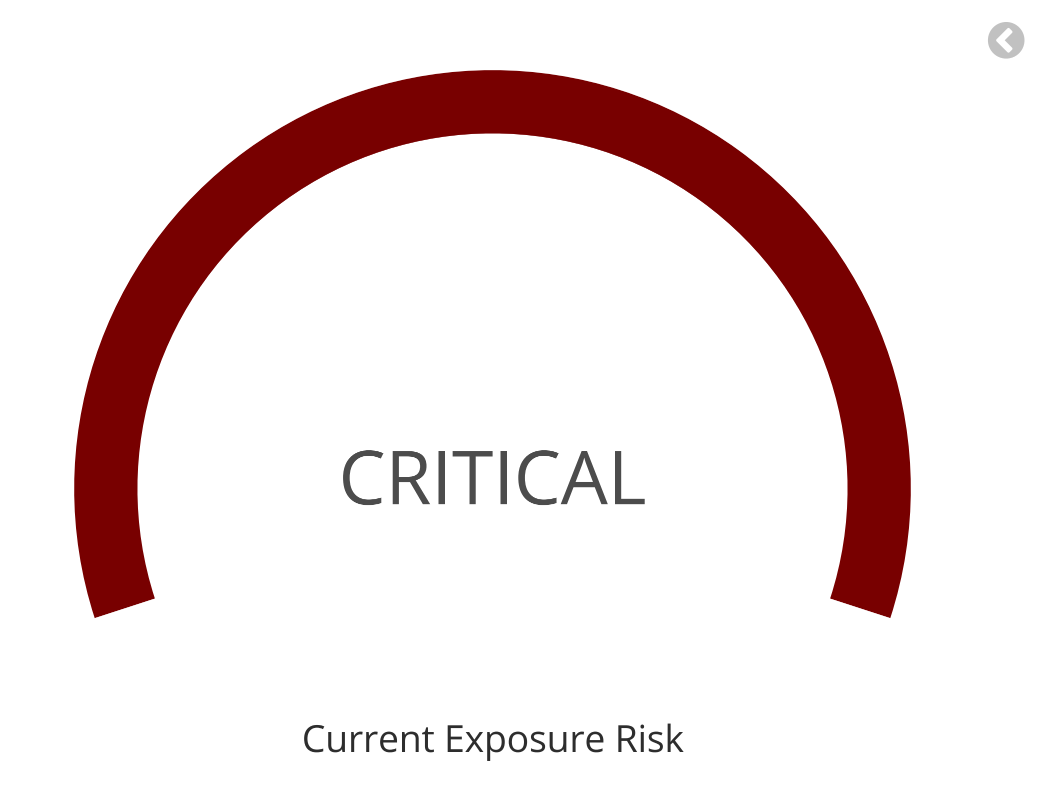
REQUESTOR DETAILS

Requestor Full Name: Nicholas Ng

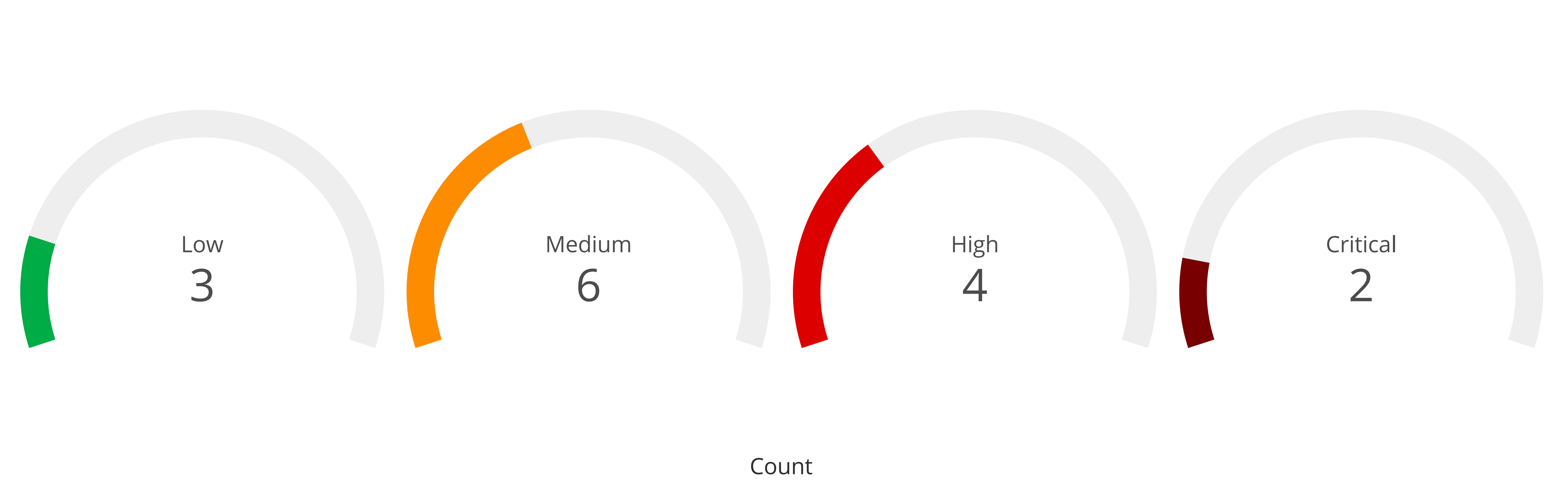
Email: nicholas.ng@provintell.com

Designation: CEO

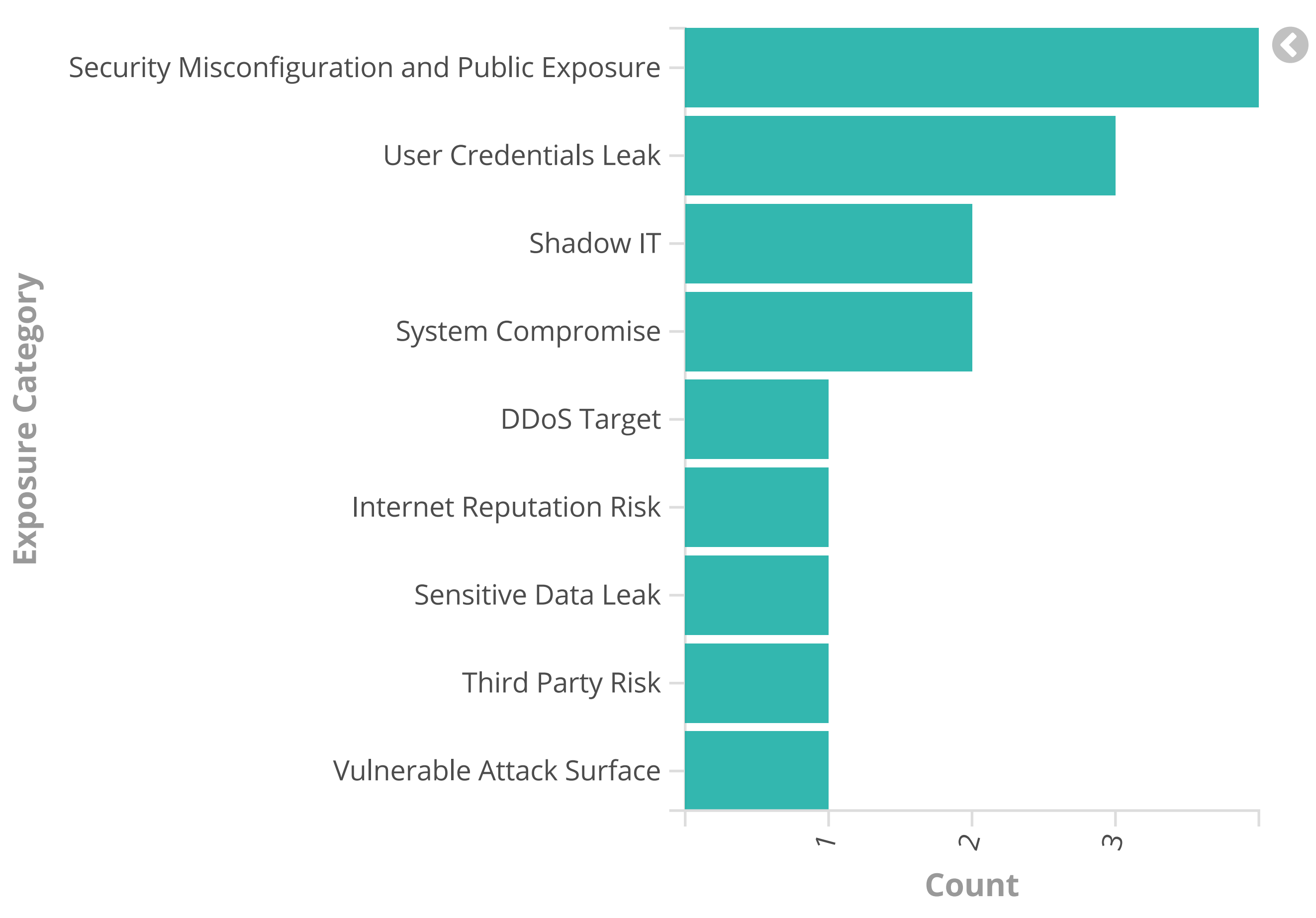
Contact No: 012-3015186



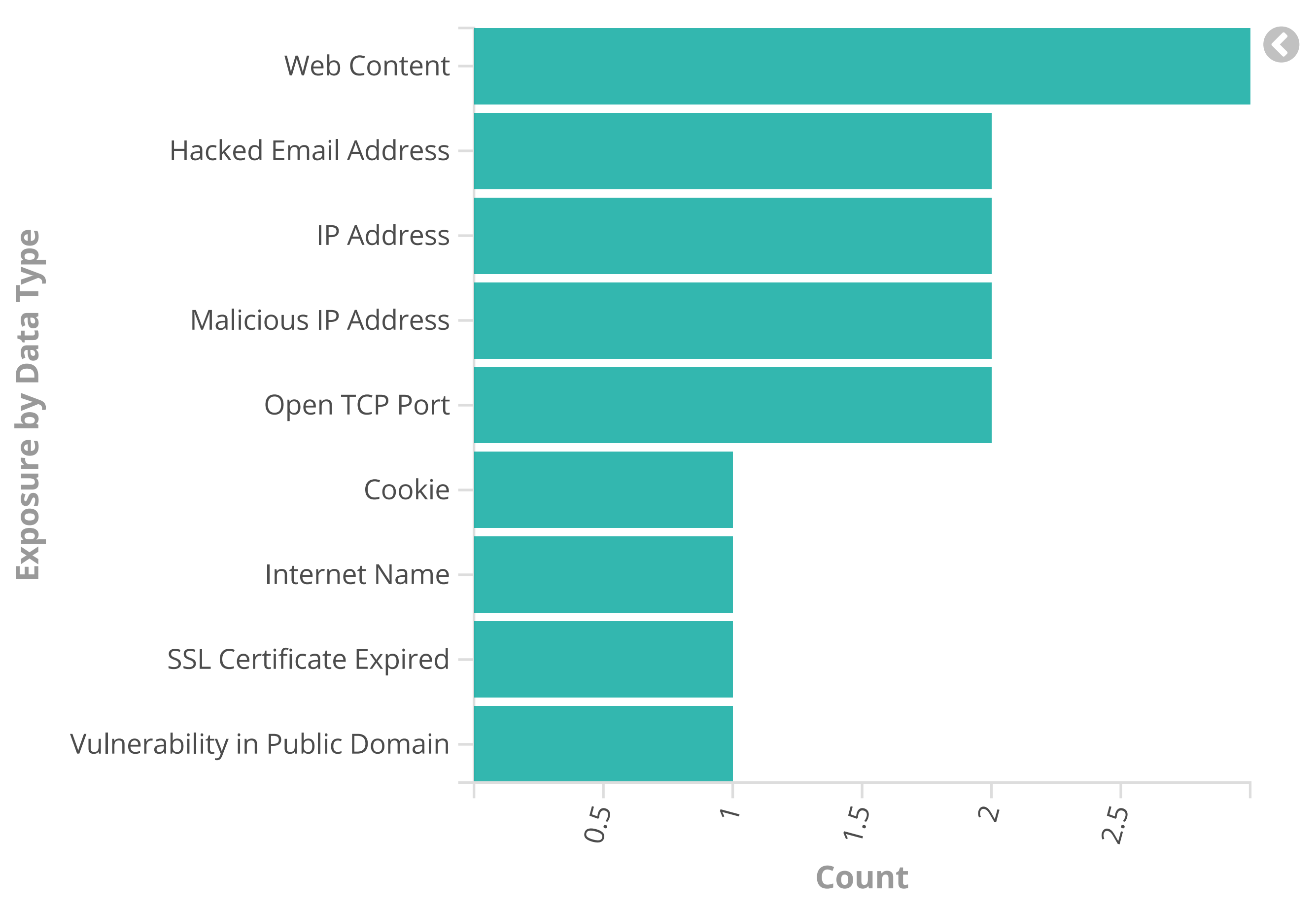
1.0 Exposure Risk Overview



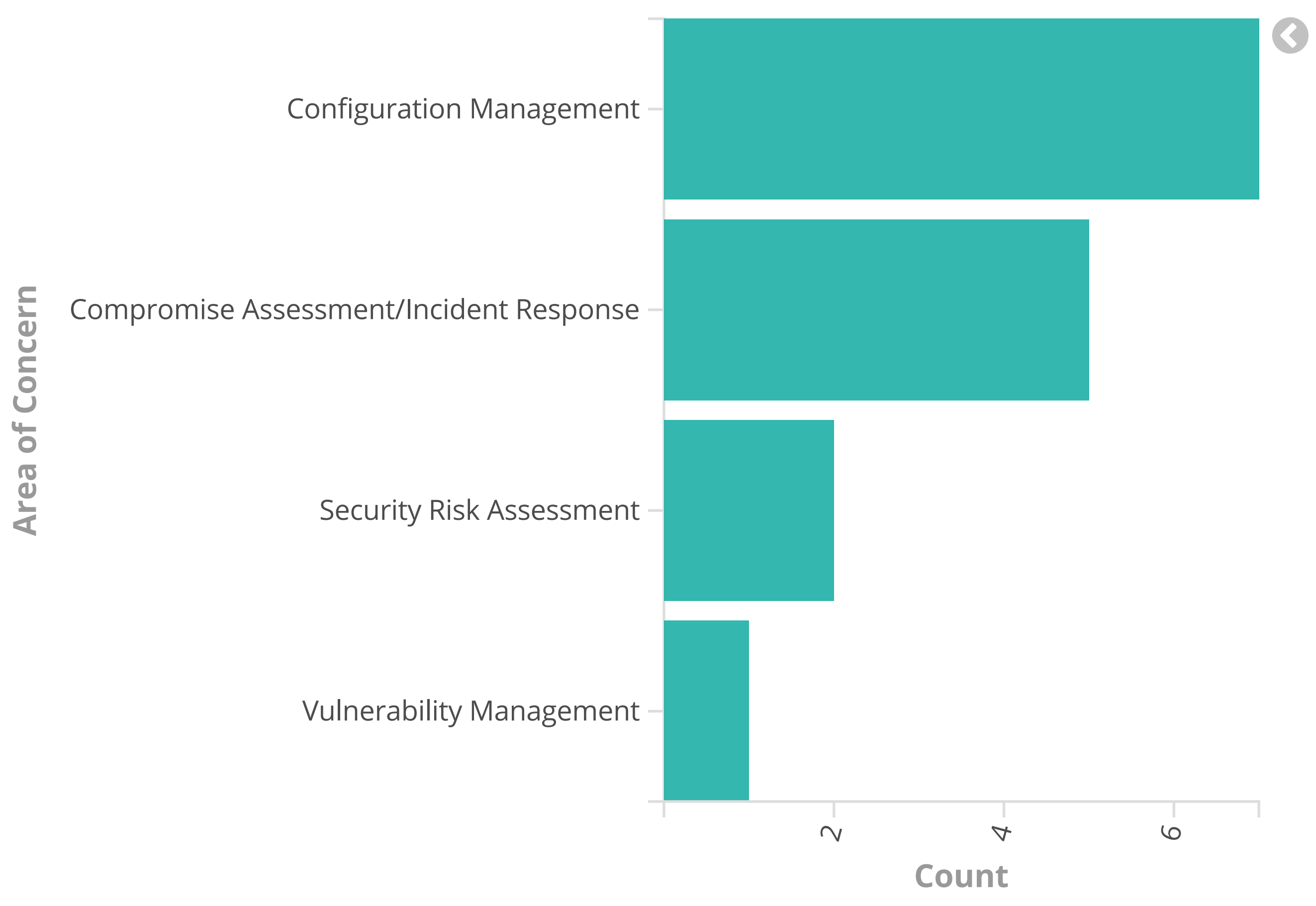
Exposure Category



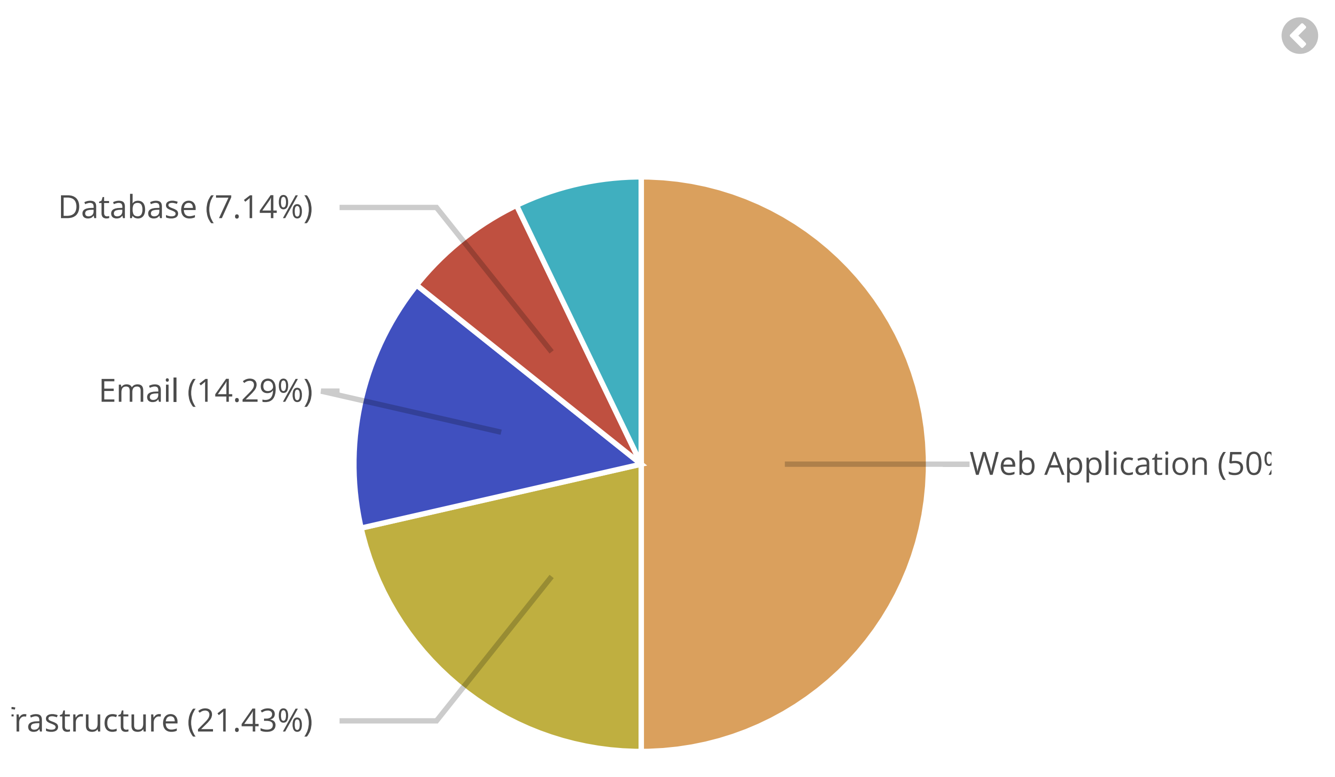
Exposure by Data Type



Area of Concern



Attack Surface Analysis



CODERED Ticket Summary

Ticket Number	Title	Priority
8614624	System Compromise - Host Compromised by Malware and Enlisted in Botnet (CRITICAL)	Critical
8614285	User Credentials Leak - Leaked Employee User Credentials (HIGH)	Critical
8614813	Internet Reputation Risk - Host Engaged in Internet Scanning and Probing Activities (HIGH)	High
8614769	User Credentials Leak - Leaked Corporate User Credentials (HIGH)	High
8614634	Vulnerable Attack Surface - High Risk Vulnerability in Public Domain (HIGH)	High
8614630	System Compromise - Website Redirecting Users to Malicious Site (HIGH)	High
8614091	Security Misconfiguration and Public Exposure - MySQL Service is Observed on the Default Port (LOW)	Low
8614632	Security Misconfiguration and Public Exposure - RDP Service is Observed on the Default Port (LOW)	Low
8614613	User Credentials Leak - Session Cookie Leaked Through Compromised Client (LOW)	Low
8614820	DDoS Target - DDoS Amplification Threat (MEDIUM)	Medium
8614702	Shadow IT - Staging Website Exposed to Public (MEDIUM)	Medium
8614696	Third Party Risk - Webmail Login Page Exposed to Public (MEDIUM)	Medium
8614628	Security Misconfiguration and Public Exposure - SSL/TLS Certificate Expired (MEDIUM)	Medium
8614626	Shadow IT - Unmanaged Web Service (MEDIUM)	Medium
8614619	Security Misconfiguration and Public Exposure - Direct IP Access Allowed (MEDIUM)	Medium

Export: Raw Formatted

2.0 CODERED Findings and Observations

Ticket Number	Exposure Risk	Title	Description	Attack Surface	Affected Target / Asset	Recommendations
8614624	Critical	System Compromise - Host Compromised by Malware and Enlisted in Botnet (CRITICAL)	Based on our observation, we have discovered that one of the hosts in your network infrastructure has been compromised by malware and is now a part of a botnet, with a command and control (C&C) server orchestrating malicious activities. This poses significant risks, including unauthorized access, data breaches, information theft, system instability, and service disruptions. Emergency incident response and compromise assessment activities are required to contain and mitigate the active threat. Malware family: 1. pushdo/cutwai	Infrastructure	1. 13.13.123.123	-For paid subscribers only- If you wish to subscribe, please contact our team
8614285	Critical	User Credentials Leak - Leaked Employee User Credentials (CRITICAL)	Based on our observation, a number of usernames and passwords associated with your company name email domain has been exposed. The exposure of your employee accounts and/or sensitive system information in the dark web that is possibly due to malware or password stealer that has infected your employees' computer devices. Emergency incident response and compromise assessment activities are required to contain and mitigate the active threat. Infected Employee Record: 23	Email	1. sample.com	-For paid subscribers only- If you wish to subscribe, please contact our team

Ticket Number	Exposure Risk	Title	Description	Attack Surface	Affected Target / Asset	Recommendations
			(Subscribe to uncover the compromised credentials)			
8614813	High	System Compromise - Host Engaged in Internet Scanning and Probing Activities (HIGH)	Based on observation, we have observed that the hosts engaged in scanning activities with the intention of detecting vulnerable services, thereby providing an opportunity for threat actors to exploit them. The presence of such scanning behavior in the hosts frequently indicates an early sign of compromise or infection. Emergency incident response and compromise assessment activities are required to contain and mitigate the active threat.	Infrastructure	1. 13.10.123.123	-For paid subscribers only- If you wish to subscribe, please contact our team
8614769	High	User Credentials Leak - Leaked Corporate User Credentials (HIGH)	Based on our observation, a number of usernames and passwords associated with your company email domain have been leaked in data breaches and available on the internet. The leaked records contain either reversed plaintext passwords or hashed passwords, which have been exposed in previous data breaches. As a result, your employee may be susceptible to credentials stuffing, account takeover attack (ATO), and phishing attacks, which can lead to unauthorized access to sensitive data or other malicious activity. Emergency incident response and compromise assessment activities are required to contain and mitigate the active threat. Infected Corporate Record: 217	Email	1. sample.com	-For paid subscribers only- If you wish to subscribe, please contact our team

Ticket Number	Exposure Risk	Title	Description	Attack Surface	Affected Target / Asset	Recommendations
			(Subscribe to uncover the compromised credentials)			
8614634	High	Vulnerable Attack Surface - High Risk Vulnerability in Public Domain (HIGH)	Based on our observation, we have identified outdated components within your web services, compromising the security and integrity of your systems and data. This vulnerability exposes your web service to exploitation by malicious actors, leading to unauthorized access, data breaches, or disruption of service. Vulnerable components: 1. PHP/5.6.40	Web Application	1. app.sample.com	-For paid subscribers only- If you wish to subscribe, please contact our team
8614091	High	System Compromise - Website Redirecting Users to Malicious Site (HIGH)	Based on our observation, we have identified a security issue in which the affected subdomain is redirecting users to a malicious site, which is believed to be compromised. This issue exposes your users to a range of security risks, including the theft of sensitive data, installation of malware, and other malicious activities. Emergency incident response and compromise assessment activities are required to contain and mitigate the active threat.	Web Content	1. spl.sample.com	-For paid subscribers only- If you wish to subscribe, please contact our team
8614820	Medium	DDoS Target - DDoS Amplification Threat (MEDIUM)	Based on our observation, there is a DDoS amplification threat directed at the identified DDoS target. A DDoS amplification threat refers to an attack technique where the attacker exploits vulnerable services or protocols to generate a high volume of malicious traffic, overwhelming the target's network resources. This type of attack leverages the amplification effect, where a small	Infrastructure	1. 13.12.123.11:161/udp	-For paid subscribers only- If you wish to subscribe, please contact our team

Ticket Number	Exposure Risk	Title	Description	Attack Surface	Affected Target / Asset	Recommendations
			request triggers a much larger response from the targeted servers or infrastructure			
8614702	Medium	Shadow IT - Staging Website Exposed to Public (MEDIUM)	The findings of this exposure category are related to the unmanaged IT assets (old or unused IT assets), non-production IT assets or services that are NOT supposed to be publicly accessible. The shadow assets would easily become the primary targets of the threat actor to circumvent or compromise your existing security controls. Staging websites may contain unfinished designs and incomplete content. Public access to these staging websites could damage a business if it leads to premature exposure of a new campaign or business decision, and could get company in to legal trouble.	Web Application	1. stg.sample.com	-For paid subscribers only- If you wish to subscribe, please contact our team
8614696	Medium	Third Party Risk - Webmail Login Page Exposed to Public (MEDIUM)	An exposed and obvious WHM login panel can make it significantly easier for attackers to breach the site, especially if access controls are limited to username and password combinations alone. This situation allows for simple brute forcing, signing in with compromised credentials/obtaining credentials, or in the case of unpatched systems, access by exploiting vulnerabilities. Even in cases where the admin login panel URL is complex and hard to guess, path disclosure vulnerabilities can be used to locate it.	Web Application	1. mail.sample.com	-For paid subscribers only- If you wish to subscribe, please contact our team
8614626	Medium	Shadow IT - Unmanaged Web Service (MEDIUM)	The findings of this exposure category are related to the unmanaged IT assets (old or unused IT assets), non-production IT assets or services that are NOT supposed to be publicly accessible. The shadow	Web Application	1. evt3.sample.com	-For paid subscribers only- If you wish to

Ticket Number	Exposure Risk	Title	Description	Attack Surface	Affected Target / Asset	Recommendations
			assets would easily become the primary targets of the threat actor to circumvent or compromise your existing security controls. Unmanaged websites may contain unfinished designs and incomplete content. Public access to these websites could damage a business if it leads to premature exposure of a new campaign or business decision, and could get company in to legal trouble.			subscribe, please contact our team
8614628	Medium	Security Misconfiguration and Public Exposure - SSL/TLS Certificate Expired (MEDIUM)	An SSL/TLS session that uses an expired certificate should not be trusted. Accepting an expired certificate makes users vulnerable to man-in-the-middle (MITM) attacks. When SSL/TLS Certificate gets expire, "Not Secure" cautioning sign shows up on the location bar alongside the message like "Your connection isn't private" or "Cautioning: Potential Security Risk Ahead" of all the well-known internet browsers like Google Chrome and Mozilla Firefox, at whatever point somebody attempts to get to the site.	Web Application	1. 13.13.123.35:443/tcp 2. 13.13.123.10:443/tcp 3. 13.13.123.18:443/tcp 4. 13.13.123.22:443/tcp 5. 13.13.123.98:443/tcp 6. 13.13.123.13:443/tcp 7. 13.13.123.14:443/tcp 8. 13.13.123.21:443/tcp 9. 13.13.123.28:443/tcp	-For paid subscribers only- If you wish to subscribe, please contact our team
8614619	Medium	Security Misconfiguration and Public Exposure - Direct IP Access Allowed (MEDIUM)	Based on our observation, we have noted that the website can be accessed using its public IP address instead of its designated domain name. This presents a risk, as it allows attackers to purchase negative connotations and associate them with your IP, leading to reputation damage by binding the website to malicious domain names. Furthermore, this method allows attackers to bypass firewall restrictions, making it easier to exploit this weakness	Infrastructure	1. 15.32.80.233:443/tcp 2. 13.13.60.160:80/tcp 3. 13.13.60.189:80/tcp 4. 13.176.44.212:80/tcp 5. 13.176.44.10:443/tcp 6. 13.176.44.29:443/tcp	-For paid subscribers only- If you wish to subscribe, please contact our team

Ticket Number	Exposure Risk	Title	Description	Attack Surface	Affected Target / Asset	Recommendations
			and gain unauthorized access to sensitive information.			
8614632	Low	Security Misconfiguration and Public Exposure - RDP Service is Observed on the Default Port (LOW)	Based on our observation, we noted that the RDP service is exposed to the public, it allows attacker to attempt to gain access to your network and sensitive information. Attackers can exploit vulnerabilities in RDP or employ brute force attacks to guess login credentials, leading to unauthorized access, data breaches, and manipulation of your systems. If the RDP service is open to the internet it becomes an entry point for an adversary to perform attacks.	Web Application	1. 13.13.61.42:3389/tcp 2. 13.13.61.30:3389/tcp 3. 13.13.61.97:3389/tcp	-For paid subscribers only- If you wish to subscribe, please contact our team
8614613	Low	User Credentials Leak - Session Cookie Leaked Through Compromised Client (LOW)	Based on our observation, we noted that your consumer accounts were compromised when logging in from a compromised client device. When using consumer accounts on a compromised client device, attackers can steal login credentials and gain unauthorized access to sensitive data. Compromised client devices are those that have been infected with malware or are otherwise under the control of an attacker. Attackers can use these devices to intercept login credentials, hijack user sessions, or perform other malicious activities. Stolen session cookies records: 40 *(Subscribe to uncover the compromised credentials)*	Web Application	1. sample.com	-For paid subscribers only- If you wish to subscribe, please contact our team
8614630	Low	Security Misconfiguration and Public Exposure - MySQL Service	MySQL is an open source Relational Database Management System (RDBMS)	Database	1. 13.13.61.15:3306/tcp 2. 13.13.60.27:3306/tcp	-For paid subscribers only-

Ticket Number	Exposure Risk	Title	Description	Attack Surface	Affected Target / Asset	Recommendations
		is Observed on the Default Port (LOW)	that utilizes Structured Query Language (SQL). Port 3306 is the default port used by MySQL protocol. It's used to connect to MySQL clients and utilities such as *mysqldump*. By having port 3306 unmonitored and opened to public access, data (except for passwords) are transmitted in clear, unencrypted form, and the protocol itself may be hacked to permit attackers access to your system.		3. 13.13.60.12:3306/tcp	If you wish to subscribe, please contact our team

---END OF REPORT--