CODEREDASM™

Provintell

EXTERNAL ATTACK SURFACE THREAT INTELLIGENCE TRIAL REPORT

Prepared for

Date: 7 Feb 2024
Revision: 1.0
Reference: SAMPLE/CODERED/2024/02/EN

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

LIMITATION OF USE AND DISCLOSURE

This document contains the sensitive and confidential information on the current security issues and risks of **SAMPLE CORPORATION**. 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 CORPORATION** 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 CORPORATION**. 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

Domain: abc.com

REQUESTOR DETAILS

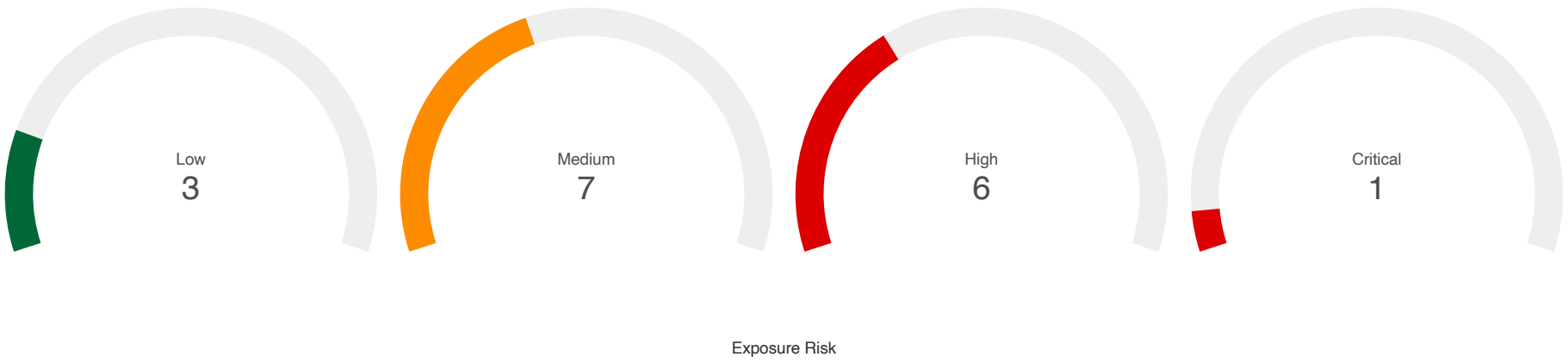
Requestor Full Name: Nicholas Ng

Business Email: nicholas.ng@provintell.com

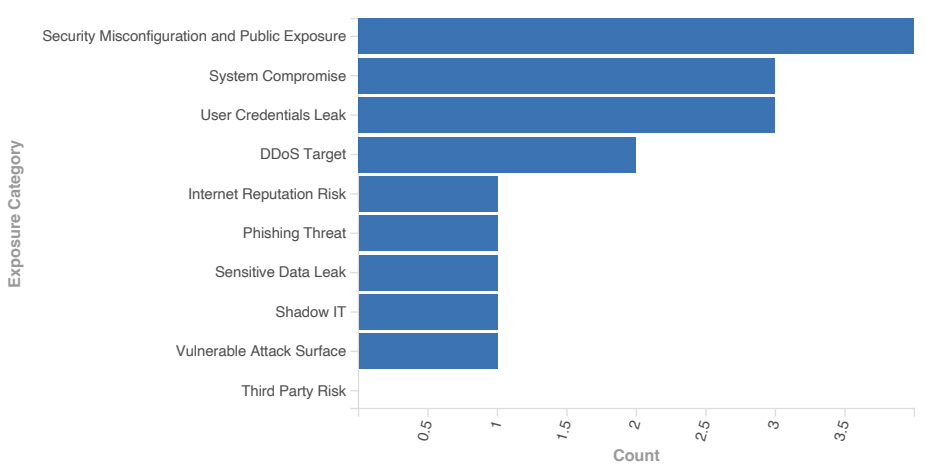
Designation: CEO

Contact No: 012-3015186

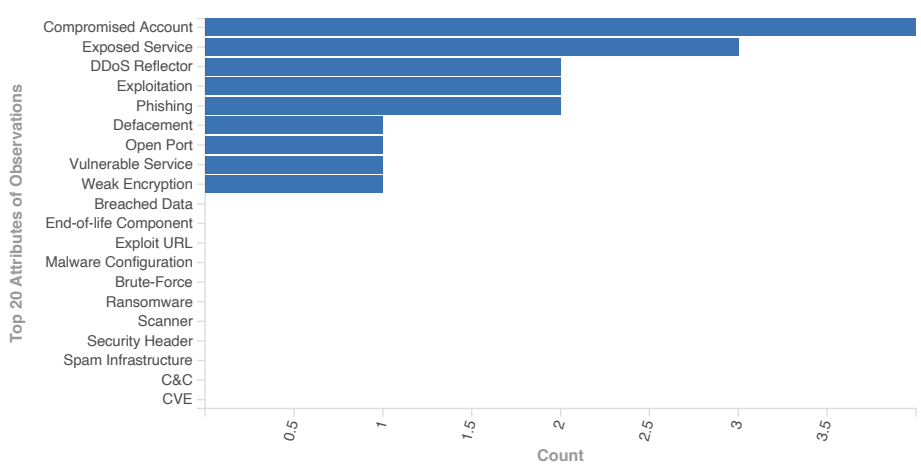
1.0 Exposure Risk Overview



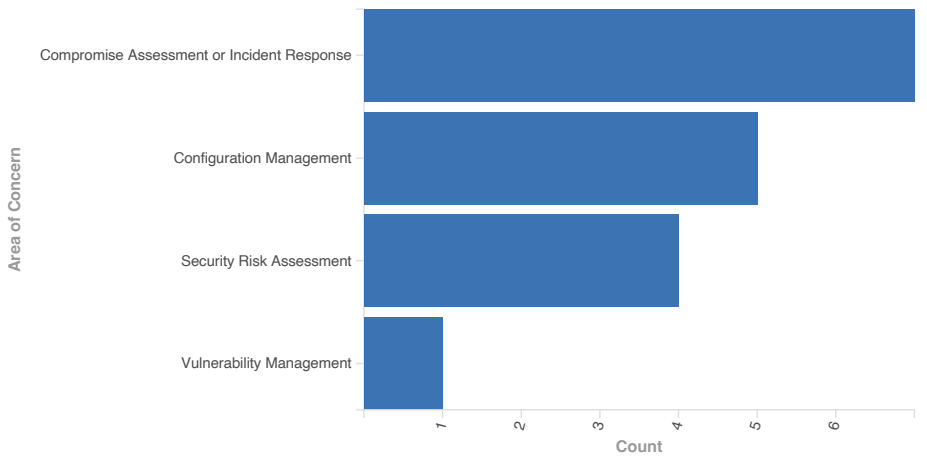
Exposure Category



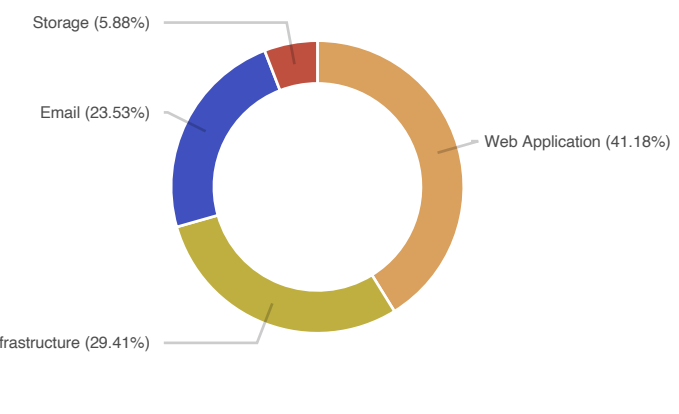
Top 20 Attributes of Observations



Area of Concern



Attack Surface Analysis



Ticket Summary

Ticket ID	Title	Exposure Risk	Status
8617191	User Credentials Leak - Leaked Employee Accounts [ABC.COM] (CRITICAL)	Critical	Open
8617319	System Compromise - Host Attempted to Exploit Vulnerable Services on External Systems [ABC.COM] (HIGH)	High	Open
8617197	System Compromise - Host Under Threat Actor Control for Bidding [ABC.COM] (HIGH)	High	Open
8617114	User Credentials Leak - Leaked Corporate Accounts [ABC.COM] (HIGH)	High	Open
8616982	Vulnerable Attack Surface - High Risk Vulnerability in Public Domain [ABC.COM] (HIGH)	High	Open
8616402	Sensitive Data Leak - Sensitive Information Disclosure of Personal Identifiable Information (ABC.COM) (HIGH)	High	Open
8616396	System Compromise - Website Redirecting Users to Malicious Site [ABC.COM] (HIGH)	High	Open
8616435	User Credentials Leak - Leaked Consumer Accounts [ABC.COM] (LOW)	Low	Open
8616430	Security Misconfiguration and Public Exposure - Misconfiguration of DMARC Record [ABC.COM] (LOW)	Low	Open
8616399	Security Misconfiguration and Public Exposure - Web Directory Listing Exposed to Public [ABC.COM] (LOW)	Low	Open
8616820	DDoS Target - Exposed SNMP Service Vulnerable to UDP Reflection Attack [ABC.COM] (MEDIUM)	Medium	Open
8616446	Security Misconfiguration and Public Exposure - SNMP Service and Banner are Observed on Default Ports [ABC.COM] (MEDIUM)	Medium	Open
8616430	DDoS Target - Host Participating in DDoS Reflected Attacks [ABC.COM] (MEDIUM)	Medium	Open
8616403	Internet Reputation Risk - Website Targeted for Site Leeching and Advertising Unauthorized Content [ABC.COM] (MEDIUM)	Medium	Open
8616401	Phishing Threat - Domain Spoofing and Domain Impersonation [ABC.COM] (MEDIUM)	Medium	Open
8616400	Shadow IT - Staging Website Exposed to Public [ABC.COM] (MEDIUM)	Medium	Open
8616397	Security Misconfiguration and Public Exposure - Direct IP Access Allowed [ABC.COM] (MEDIUM)	Medium	Open

2.0 Technical Findings and Recommendations

Ticket Number	Exposure Risk	Title	Description	Attack Surface	Affected Target / Asset	Recommendations	Status
8617191	Critical	User Credentials Leak - Leaked Employee Accounts [ABC.COM] (CRITICAL)	The exposure of your employee accounts and/or sensitive system information in the dark web that is 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. Affected Employee Record: 1	Email	1. abc.com	For paid subscribers only If you wish to subscribe, you may contact codered@provintell.com for quotation	Open
8617319	High	System Compromise - Host Attempted to Exploit Vulnerable Services on External Systems [ABC.COM] (HIGH)	A compromised host within your network is actively trying to exploit vulnerabilities in services hosted by external organizations over the internet, such as web servers, mail servers, or other services exposed online. Compromised systems can also be used to recruit additional hosts into botnets, which can be leveraged for various malicious purposes, including further exploitation, spam campaigns, or launching coordinated attacks against other targets. This unauthorized activity poses a grave threat to your organization's infrastructure and data integrity.	Infrastructure	1. forum.abc.com	For paid subscribers only If you wish to subscribe, you may contact codered@provintell.com for quotation	Open
8617197	High	System Compromise - Host Under Threat Actor Control for Bidding [ABC.COM] (HIGH)	Based on our observation, We have detected a host within the network is compromised and under the control of a threat actor. This compromise is linked to illicit bidding activities, commonly conducted through secure	Infrastructure	1. forum.abc.com	For paid subscribers only If you wish to subscribe, you may contact codered@provintell.com for quotation	Open

Ticket Number	Exposure Risk	Title	Description	Attack Surface	Affected Target / Asset	Recommendations	Status
			Communication channels like Telegram groups or specialized forums dedicated to criminal activities. This poses a grave risk to the integrity, confidentiality, and overall security stance of the organization.				
8616982	High	Vulnerable Attack Surface - High Risk Vulnerability in Public Domain [ABC.COM] (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. 1. digitalid.abc.com - PHP 7.4.32 - OpenSSL 1.1.1k	Web Application	1. digitalid.abc.com	For paid subscribers only If you wish to subscribe, you may contact codered@provintell.com for quotation	Open
8617114	High	User Credentials Leak - Leaked Corporate Accounts [ABC.COM] (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 exposure of your employee accounts in the dark web that is due to malware and password stealer that has infected your employees computer devices. 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	Email	1. abc.com	For paid subscribers only If you wish to subscribe, you may contact codered@provintell.com for quotation	Open

Ticket Number	Exposure Risk	Title	Description	Attack Surface	Affected Target / Asset	Recommendations	Status
			to sensitive data or other malicious activity. Emergency incident response and compromise assessment activities are required to contain and mitigate the active threat Affected Corporate Record: 55				
8616396	High	System Compromise - Website Redirecting Users to Malicious Site [ABC.COM] (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 Application	1. smpls.abc.com	For paid subscribers only If you wish to subscribe, you may contact codered@provintell.com for quotation	Open
8616402	High	Sensitive Data Leak - Sensitive Information Disclosure of Personal Identifiable Information [ABC.COM] (HIGH)	Based on our observation, we have discovered that one of the endpoint revealed a misconfiguration that lead to the unauthorized disclosure of Personal Identifiable Information (PII). This includes sensitive data such as names, addresses, passport number, contact details, and other personally identifiable details. The identified weakness poses a significant risk to the confidentiality and privacy of individuals associated with your organization. Such a breach can lead to reputational damage, eroding trust among stakeholders, and introducing increased security risks as	Storage	1. https://raidforums.com/Thread-SELLING-Malaysia-ABC-Delivery-Service-with-ABC-22-Millions%22,%22site%22:%22RaidForums%22,%22data%22:%22abc.com.my%22%4D	For paid subscribers only If you wish to subscribe, you may contact codered@provintell.com for quotation	Open

Ticket Number	Exposure Risk	Title	Description	Attack Surface	Affected Target / Asset	Recommendations	Status
			malicious actors exploit disclosed information.				
8616397	Medium	Security Misconfiguration and Public Exposure - Direct IP Access Allowed [ABC.COM] (MEDIUM)	The website can be accessed via public IP instead of domain name. It is possible for anyone to buy a domain name containing negative terms and binds your public IP to that domain. An attacker can carry out mass phishing attack to spoil to reputation of your company by binding site to any bad domain name thus resulting in loss of reputation of company.	Web Application	1. 11.11.123.124:80/tcp	For paid subscribers only If you wish to subscribe, you may contact codered@provintell.com for quotation	Open
8616401	Medium	Phishing Threat - Domain Spoofing and Domain Impersonation [ABC.COM] (MEDIUM)	Based on our observation, we have identified a phishing threat involving typosquatting, where the threat actor register misspelled variations of your domain name to divert traffic to malicious sites. The strategy involves registering all conceivable versions of your domain, including singular and plural forms, various domain extensions, and both hyphenated and non-hyphenated compound words. Typosquatted domains, also termed URL hijacking, present risks in spear phishing campaigns against company personnel or customers, as well as drive-by download incidents, and the inadvertent reception of misaddressed emails intended for the domain.	Web Application	1. abcc.com	For paid subscribers only If you wish to subscribe, you may contact codered@provintell.com for quotation	Open

Ticket Number	Exposure Risk	Title	Description	Attack Surface	Affected Target / Asset	Recommendations	Status
8616446	Medium	Security Misconfiguration and Public Exposure - SNMP Service and Banner are Observed on the Default Ports [ABC.COM] (MEDIUM)	Since SNMP is a UDP-based protocol, exposing it to the Internet will make you a likely participant in reflected DDoS attacks. In addition, the SNMP v3 interface will most likely expose sensitive information about your networks to anyone on the Internet.	Infrastructure	1. 11.11.123.123:161/udp	For paid subscribers only If you wish to subscribe, you may contact codered@provintell.com for quotation	Open
8616403	Medium	Internet Reputation Risk - Website Targeted for Site Leeching and Advertising Unauthorized Content [ABC.COM] (MEDIUM)	Based on our observation, your website is being exploited by malicious actors who are using it to promote unauthorized content, such as casino and pirate websites. This is happening because your website is running an improperly configured SharePoint application that allows anyone with internet access to submit survey forms. These survey forms are then indexed by search engines, making them appear as legitimate content on your website, which can negatively impact your SEO rankings, damage your website's reputation, and potentially expose you to legal liability.	Web Application	1. https://abc.com/question?/Lists/G00d%G00d%20Food%20Processing%20SurveyQuestionaire/DispForm.aspx?ID=123456	For paid subscribers only If you wish to subscribe, you may contact codered@provintell.com for quotation	Open
8616400	Medium	Shadow IT - Staging Website Exposed to Public [ABC.COM] (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	Web Application	1. staging-test.abc.com	For paid subscribers only If you wish to subscribe, you may contact codered@provintell.com for quotation	Open

Ticket Number	Exposure Risk	Title	Description	Attack Surface	Affected Target / Asset	Recommendations	Status
			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.				
8616430	Medium	DDoS Target - Host Participating in DDoS Reflected Attacks [ABC.COM] (MEDIUM)	Based on our observations, a host within your network has been identified as participating in a DDoS reflected attack. The affected host is serving as a reflector or amplifier for malicious traffic directed towards a target server or network. The host responds to requests from the attacker with larger responses, amplifying the volume of traffic directed towards the victim's server and contributing to the success of the DDoS attack. The involvement of the network's host in a DDoS reflected attack can tarnish the organization's reputation, as it reflects poorly on the organization's security posture and reliability of its services.	Infrastructure	1. stg-test.abc.com	For paid subscribers only If you wish to subscribe, you may contact codered@provintell.com for quotation	Open
8616430	Medium	DDoS Target - Exposed SNMP Service Vulnerable to UDP Reflection Attack [ABC.COM] (MEDIUM)	SNMP utilizes connectionless UDP transport for queries and responses, with no transport session or handshake required prior to data exchange. Exposing it to the Internet will make you a likely participant in reflected DDoS attacks. In addition, the SNMP v3 interface will most likely expose	Infrastructure	1. 23.123.213.12:161/udp 2. 23.123.213.14:161/udp 3. 23.123.213.13:161/udp	For paid subscribers only If you wish to subscribe, you may contact codered@provintell.com for quotation	Open

Ticket Number	Exposure Risk	Title	Description	Attack Surface	Affected Target / Asset	Recommendations	Status
			sensitive information about your networks to anyone on the Internet.				
8616430	Low	Security Misconfiguration and Public Exposure - Misconfiguration of DMARC Record [ABC.COM] (LOW)	DMARC is designed to give receivers of email better judgment control based on sending domain reputations. It provides a platform where the sending side can publish policies to improve effectiveness against spam and phishing, in effect building domain reputations.	Email	1. abc.com	For paid subscribers only If you wish to subscribe, you may contact codered@provintell.com for quotation	Open
8616399	Low	Security Misconfiguration and Public Exposure - Web Directory Listing Exposed to Public [ABC.COM] (LOW)	The system exhibits an exposed directory listing vulnerability, allowing the contents of directories to be displayed to anyone accessing the web server. Instead of a default welcome page, directories reveal their contents, potentially divulging sensitive information, such as file names, configurations, or system structures. This exposure provides a roadmap for attackers, aiding in reconnaissance and potential exploitation. Resolving this vulnerability is imperative to prevent unauthorized access to system details and enhance overall security.	Web Application	1. spla.abc.com	For paid subscribers only If you wish to subscribe, you may contact codered@provintell.com for quotation	Open
8616435	Low	User Credentials Leak - Leaked Consumer Accounts [ABC.COM] (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	Email	1. abc.com	For paid subscribers only If you wish to subscribe, you may contact codered@provintell.com for quotation	Open

Ticket Number	Exposure Risk	Title	Description	Attack Surface	Affected Target / Asset	Recommendations	Status
			under the control of an attacker. Attackers can use these devices to intercept login credentials, hijack user sessions, or perform other malicious activities. Affected Consumer Record: 642				

-- END OF REPORT --