SAMPLE COMPANY LLC

CST network security services Ltd.

Table of Contents

Table of Contents

Executive Summary

CST Network Security Services LTD has been contacted by SAMPLE COMPANY LLC to conduct a thorough, open source investigation on their website with the following scope(s):

- corp.local (AD)
- samplecorp.com
- any website utilizing SMAPLE COMPANY technology

The open source investigation (OSINT) was performed in such way in order to simulate and measure the **POSSIBLE** extend of the damages that a black hat hacker could achieve just through the reconnaissance and enumeration phase of a pentest on SAMPLE COMPANY LLC. The entire OSINT was performed using open source tools and no attempt was made to gain unauthorized access to any machine. The investigation was performed under controlled conditions and follow the NCSC guidelines.

High Level Outcomes

After having performed a thorough reconnaissance and enumeration as well as in depth fingerprinting on the targets in scope, we were able to identify key information that would aid a pentester in initiating engagement.

External: Several possible users were found on the domain 'CORP' as well as several insecure servers were found to harbor possible remote code execution vulnerabilities, as well as being prone to bruteforce attacks. A vast number of FTP servers appeared to be left in the open, with potential anonymous login and several primary mailing servers were exposed.

Overall, SAMPLE COMPANY LLC was found to have seemingly vulnerable attack surface which **may** allow a bad actor to gain full control of the 'CORP' domain and compromise all the machines.

Prioritized Recommendations

Based of the penetration test performed,we strongly urge the following changes to be made as soon as possible:

- Implement ACL functionality in OWA Panel and Tomcat server
- Update all backend software to latest stable releases
- Upgrade RoundCube to latest version to prevent SQLi
- Upgrade Grafana version 8.3.0 to latest to prevent Path Traversal

By following these guidelines, the websites in scope will have a strengthened surface, reducing attack vectors and would prevent the exact course of infiltration demonstrated in this report from being used in a real world scenario.

Appendix A: Vulnerability Detail & Mitigation

This section covers the possible primary vulnerabilities that seemed to persist across the SAMPLE COMPANY network, and would possibly allow a bad actor to gain unauthorized control over the network. Each key vulnerability is given an overall risk rating based off its individual impact on the website and its use in the exploitation phase. General guidelines on mitigation of the vulnerabilities will be highlighted in each section.

Overall Risk Rating

Rating:	Medium
Impact:	with the possible vulnerabilities and attack paths identified during the OSINT investigation on SAMPLE COMPANY LLC, it can be assumed that gaining an initial foothold on the 'CORP' network is highly possible, and the thorough fingerprinting performed would greatly aid in achieving that.

Exposed OWA Admin Panel

Rating:	High
Impact:	The CVE-2023-23397 vulnerability has a slight possibility of being present in the Outlook MX server on the IP [IP], although the panel primarily prone to bruteforce attacks on users with the domain 'CORP' as no rate limiter or ACL was put in place.
Remediation:	In order to resolve the potential CVE-2023-23397' issue, it is recommended to follow the patch issued by Microsoft through this link, and in order to resolve the bruteforce possibility, it is highly recommended to reconfigure the OWA Panel with a rate-limiter in place and to implement an Access Control List to only allow IPs within the company network to access the OWA Panel.

Grafana Directory Traversal

Rating:	High
Impact:	The CVE-2021-43798 Path Traversal vulnerability would allow for a bad actor to access potentially sensitive information stored on the machine hosting the grafana server by indexing the machines contents through the concatenation of the '../' operators.
Remediation:	In order to resolve the CVE-2021-43798 vulnerability present on the Grafana 8.3.0 instance, it is mandatory to follow the official patch notes released by Grafana through this link.

Potential RoundCube SQLi

Rating:	Medium
Impact:	The possible CVE-2021-44026 vulnerability present on the RoundCube login form on the IP [IP] suspected to belong to SAMPLE COMPANY LLC poses severe data breach threats and login bypass. It would imply that a bad actor could access and dump the contacts of the SQL database and access the RoundCube panel.
Remediation:	In order to resolve the possible CVE-2021-44026 vulnerability, its highly recommended to migrate to the latest stable release of RoundCube.

Exposed Tomcat

Rating:	Medium
Impact:	The exposed tomcat server may serve as a possible attack surface for a bad actor to attempt to infiltrate, and in the worst cases may allow for the complete takeover of the machine hosting it through the common vulnerable WAR file upload.
Remediation:	In order to better hide the tomcat server in question, it is highly recommended to implement an ACL of IPs that would only allow for machines within the companies network to access the server.

Leaked Users

Rating:	Medium
Impact:	The identified possible uses found through the OSINT investigation have a high likelihood of being present on the domain 'CORP', hence opening up doors to bruteforce attacks.
Remediation:	In order to better hide these users (root@dam1-mx1.samplecorp.com and c.john) it is recommended to hide these users from the public banners and instead keep communications through a safer, encrypted channel.

Findings and Enumeration

To begin the enumeration phase, we utilized powerful search engines and open source vulnerability scanners to identify all the possible attack vectors relevant to SAMPLE COMPANY LLC, and further search for any technologies originating from samplecorp.com around the web.

Hypothesized Attack Paths

After having completed the Open Source Investigation (OSINT) on SAMPLE COMPANY LLC, we have come up with a possible attack plan to gain a foothold on the network:

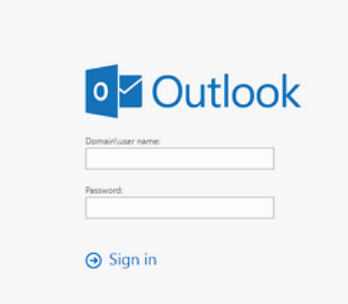
- Abuse the Grafana Directory Traversal for initial information.
- Bruteforce The Outlook Web Access (OWA) Panel with the 'c.john' user identified.
- Attempt to exploit the potential SQLi vulnerability on the RoundCube login form.
- Attempt to access the tomcat server through default credentials.

Exposed Admin Outlook Panel

In order to perform a better, more thorough pentest, it is mandatory to identify all the surface level access tools which are utilized by system administrators and can be infiltrated or abused by bad actors in order to receive local or system level shells on a given system.

Upon initial inspection, a hidden Outlook Panel was revealed on the IP [IP], which appears to be used to manage and automate emails via POP3 and IMAP (port 143).

```
device.corp.local Microsoft ESMTP MAIL Serv:
device.corp.local Hello [xxx.xxx.xxx.xxx]
SIZE 63424400
PIPELINING
DSN
ENHANCEDSTATUSCODES
AUTH LOGIN
```



The image above displays the SMTP banner, which shows the communication between the server and the user making the POST/GET requests. This reveals a new domain (corp.local) with a new set of subdomains (in this case devices) which seem to control the Microsoft ESMTP mail server. A preview of the outlook page on port 80 is present above. Possible users for this Outlook interface are also detailed and highlighted throughout this "Findings and Enumeration" section of the report.

In order to verify the authenticity of the domain identified through the banner, we have used the "scanner/http/owa_login" domain, which will perform further fingerprinting and fully expose the Active Directory domain responsible for hosting this Outlook MX server.

```
msf6 auxiliary(scanner/http/owa_login) > exploit

[*] XXX.XX.XXX.XX:443 OWA - Testing version OWA_2013
[+] Found target domain: CORP
[*] XXX.XX.XXX.XX:443 OWA - Trying user : pass
[+] server type: CORP-LOCAL
[!] No active DB -- Credential data will not be saved!
[*] XXX.XX.XXX.XX:443 OWA - FAILED LOGIN, BUT USERNAME IS VALID. 0.293672763 'CORP\user' : 'pass': SAVING TO CREDS
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/owa_login) >
```

Exposed Admin Outlook Panel

The screenshot above details the output generated by metasploit, revealing the Active Directory domain 'CORP'. Having found this, it can be safely concluded that an attacker may utilize this to perform bruteforce attacks with the following username syntax: 'CORP\USER'. Additionally, there appears to be no rate limiter implemented in the Outlook MX login interface, which further supports the bruteforce attack path as a viable route to exploit the exposed OWA Panel in question.

In order to perform additional fingerprinting to detect the exact version numbers of the OWA panel identified. This can be done through powerful search engine tools such as shodan.

```
* OK The Microsoft Exchange IMAP4 service is ready.
* CAPABILITY IMAP4 IMAP4rev1 AUTH=PLAIN AUTH=NTLM AUTH=GSSAPI STARTTLS SASL-IR UIDPLUS ID UNSELECT CHILDREN IDLE NAMESPACE LITERAL+
A001 OK CAPABILITY completed.
* ID ("name" "Microsoft.Exchange.Imap4.Imap4Server" "version" "15.1")
A002 OK ID completed
A003 BAD Command Error. 12
* BYE Microsoft Exchange Server 2016 IMAP4 server signing off.
A004 OK LOGOUT completed.
```

The screenshot above details the result of fingerprinting performed by shodan.io, which confirms the use of IMAPv4, as well as a Microsoft exchange server running on version 15.1 of 2016, which presents a variety of possible vulnerabilities.

After doing further research on the version of the Microsoft exchange server present on the IP in question, a few vulnerabilities with a CVSS score of 7.0 or higher appeared to be present on that specific version.

2	CVE-2021-37852	269		2022-02-09	2022-07-12	7.2	None	Local	Low	Not required	Complete	Complete	Complete

ESET products for Windows allows untrusted process to impersonate the client of a pipe, which can be leveraged by attacker to escalate privileges in the context of NT AUTHORITY\SYSTEM.

3	CVE-2021-37851	755		2022-05-11	2022-05-19	7.2	None	Local	Low	Not required	Complete	Complete	Complete

Local privilege escalation in Windows products of ESET allows user who is logged into the system to exploit repair feature of the installer to run malicious code with higher privileges. This issue affects: ESET, spol. s r.o. ESET NOD32 Antivirus 11.2 versions prior to 15.1.12.0. ESET, spol. s r.o. ESET Internet Security 11.2 versions prior to 15.1.12.0. ESET, spol. s r.o. ESET Smart Security Premium 11.2 versions prior to 15.1.12.0. ESET, spol. s r.o. ESET Endpoint Antivirus 6.0 versions prior to 9.0.2046.0; 6.0 versions prior to 8.1.2050.0; 6.0 versions prior to 8.0.2053.0. ESET, spol. s r.o. ESET Endpoint Security 6.0 versions prior to 9.0.2046.0; 6.0 versions prior to 8.1.2050.0; 6.0 versions prior to 8.0.2053.0. ESET, spol. s r.o. ESET Server Security for Microsoft Windows Server 8.0 versions prior to 9.0.12012.0. ESET, spol. s r.o. ESET File Security for Microsoft Windows Server 8.0.12013.0. ESET, spol. s r.o. ESET Mail Security for Microsoft Exchange Server 6.0 versions prior to 8.0.10020.0. ESET, spol. s r.o. ESET Mail Security for IBM Domino 6.0 versions prior to 8.0.14011.0. ESET, spol. s r.o. ESET Security for Microsoft SharePoint Server 6.0 versions prior to 8.0.15009.0.

Both of the identified **potential** vulnerabilities relate to privilege escalation, meaning they can be utilized to gain a shell with elevated privileges, specifically with the user NTAUTHORITY, only if a low level shell is acquired, therefore presents no surface level threat. This however means that a bad actor may find lateral movement easier to perform.

Exposed Admin Outlook Panel

Additional vulnerabilities appeared to be present after a more in-depth investigation with a powerful tool, ZoomEye.

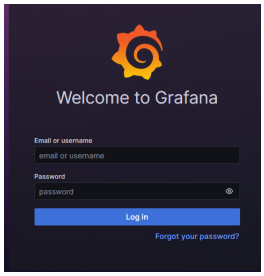
Serial number	Vulnerability number	Date of discovery	Vulnerability level	Vulnerability name
1	99659	2023-03-16	high	Microsoft Outlook 权限提升漏洞 (CVE-2023-23397)
2	99628	2023-01-09	high	Microsoft Exchange Server 权限提升漏洞 (CVE-2022-41080)
3	99610	2022-11-21	high	Microsoft Exchange Server 远程代码执行漏洞 (CVE-2022-41040 CVE-2022-41082)
4	99605	2022-11-17	high	Cisco ESA and Cisco Secure Email and Web Manager Next Generation Management SQL注入漏洞 (CVE-2022-20867)

These **possible** vulnerabilities pose more of a threat to the exchange server (if present), as they imply that a bad actor has the possibility of gaining unauthorized remote code execution, and a remote shell by abusing the Microsoft Outlook (CVE-2023-23397) and the Microsoft Exchange Server (CVE-2022-41080) vulnerabilities.

These high severity vulnerabilities persisted across multiple endpoints, including mailserv.samplecorp.com, and several of the other mailing related subdomains.

Exposed Grafana

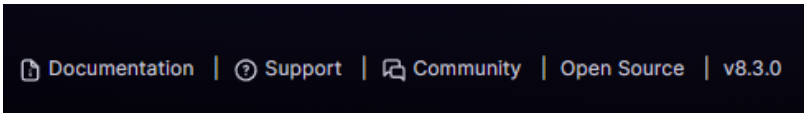
After further investigation, another attack surface was revealed on the 'CORP' network. This time it consisted of a Grafana login panel on the IP [IP], which acts as an administrative analytics panel to view data and metric which have been collected by Grafana.




```
HTTP/1.1 200 OK
Cache-Control: no-cache
Content-Type: text/html; charset=UTF-8
Expires: -1
Pragma: no-cache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Date: Fri, 12 May 2023 22:56:27 GMT
Transfer-Encoding: chunked
```

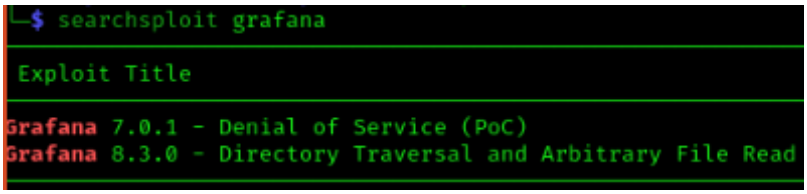
Exposed Grafana

The interface presented the expected login panel, and after further banner analysis and fingerprinting, we were able to identify the version of this specific panel. This turned out to be version '8.3.0', as attached below:



The specific Grafana version in question presents a high risk 'Local File Inclusion' vulnerability which was a discovered zero day under the CVE number CVE-2021-43798. This vulnerability allows an attacker to exploit a flaw in the application's code, enabling them to access and retrieve sensitive files from the targeted system. The LFI vulnerability in Grafana 8.3.0 poses a significant risk to SAMPLE COMPANY LLC, as it can lead to unauthorized disclosure of confidential data, system compromise, and potentially remote code execution. See "Appendix A" for further remediation advice.

In terms of exploitation, a script published under 'ExploitDB' can be found here. The script abuses the arbitrary file read and local file inclusion vulnerability by appending a string of characters which traverses the directories in order to reach the root directory, and from there appends the location of the file to read. It can be found through searchsploit like so:

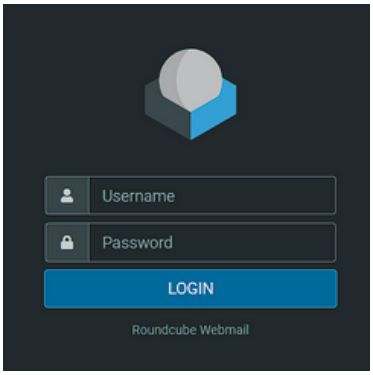


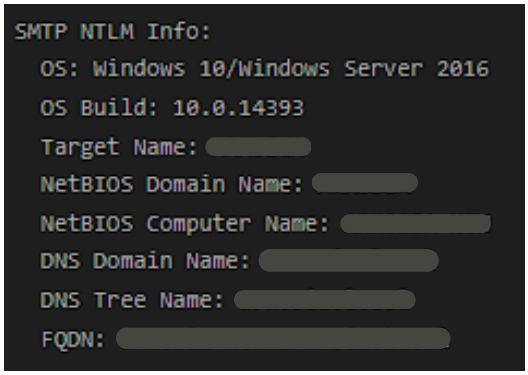
The exploit can also be performed manually by appending the chain of '../' to the URL and by sniffing the response through a proxy interception tool such as burpsuite. It is worth mentioning that no attempt was made to exploit or read files in the vulnerable grafana instance as is out of the scope of this pentest.

Vulnerable Roundcube

During the enumeration phase, another concerning attack surface was identified. This consisted of another mail related server, this time hosted on an EC2 bucket within AWS. The attack surface hosts a RoundCube login, an IMAP web-based client which works hand to hand with JavaScript and XLM (AJAX).

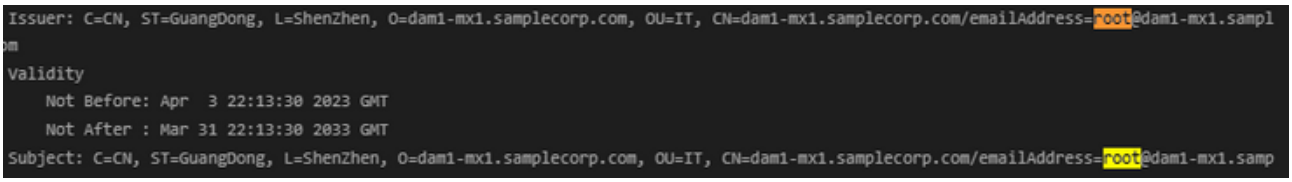
The identified attack surface has a high chance of belonging to SAMPLE COMPANY LLC on the IP [IP] and presents the following interface:





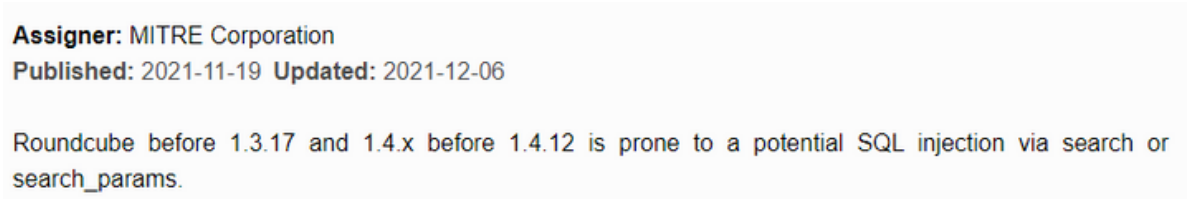
After successfully fingerprinting the web page, we can conclude that the attack vector does indeed link to Sample Business, and indicates the hosting server to be a Windows 10 2016 machine, which has a high likelihood of harboring high severity vulnerabilities on the CVSS scale. Given that the OS information supplied was too broad, we decided not to search for vulnerabilities as they may not be applicable in this scenario. The fingerprinting, has however led us to further understand the structure of the Sample Business network, and has added the possible domain corp.local to the scope list, and now confirms the initial belief that Sample Business runs on an Active Directory environment.

After further fingerprinting and enumeration of the banners, an account root@dam1-mx1.sampledomain.com has been identified as a possible account for the RoundCube login form, and as a possible administrative account in the corp.local network.



Vulnerable Roundcube

Taking into account all the backend software version numbers, and additional information gained from the enumeration of the RoundCube login form, we have identified a an outdated version of RoundCube (1.4.12), which relates to a high severity SQL Injection vulnerability, which would permit a bad actor to bypass the RoundCube login form and possibly dump the contents of the database connected to it.


Assigner: MITRE Corporation
Published: 2021-11-19 **Updated:** 2021-12-06

Roundcube before 1.3.17 and 1.4.x before 1.4.12 is prone to a potential SQL injection via search or search_params.

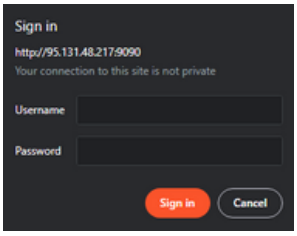
The screenshot above details a vulnerability highlighted by 'MITRE Corporation', which involves the **possibility** for a SQL Injection vulnerability (CVE-2021-44026) via the 'search_params', and appears to affect the identified version of RoundCube. Not only would this allow for a bad actor to fully access the contents of the RoundCube web mail at an administrative level, but also allow for full database dumps via a blind based SQL injection attack, which would further help a bad actor understand what users are present and gain potential password hashes for each user (if hashed). An attempt to perform this attack has not been made as it is out of the current scope for the Open Source Investigation.

Exposed Tomcat

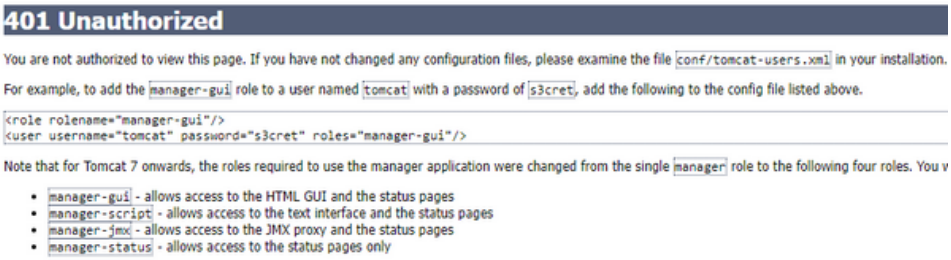
throughout the enumeration phase, another concerning attack surface was identified. An exposed Apache tomcat server was identified, which is a service that acts as a base to host all Java servlets. This also means that tomcat allows file upload, particularly with '.WAR' files, which may be used to check if the server has vulnerable file upload present, however no attempt was made to do so as it would require a successful login attempt to the identified login panel (detailed below) and is outside the scope of this pentest.

Exposed Tomcat

The identified attack surface was hosted on the IP [IP] and presents the following interface:



This interface reveals an unprotected login field, which does not appear to have any protection against bruteforce attacks with rate limiting, and would therefore pose as another possible attack surface for a bad actor to possibly infiltrate.



If no credentials are inputted, a static web page is returned with hints towards the use of the credentials 'tomcat' 's3cret', however no login attempt was made as it is out of the scope of this OSINT investigation.

Aside from that, tomcat servers are notorious for harboring high severity vulnerabilities, however none have been found as of yet for this specific version.

Appendix B: Disclaimers & Miscellaneous

The 'Appendix B' section has been reserved to include general disclaimers (including but not limited to the official CyberSanctus Terms of Service) which is lawfully required to protect the pentesters under CyberSanctus. Additional services will also be included in this secion.

Limitation of Liabilities

The information contained in this report is provided “as is” without warranty of any kind. CyberSanctus makes no representations or warranties of any kind, express or implied, as to the completeness, accuracy, reliability, suitability or availability with respect to the information, products, services, or related graphics contained in the report for any purpose. Any reliance you place on such information is therefore strictly at your own risk.

In no event will CyberSanctus be liable for any loss or damage including without limitation, indirect or consequential loss or damage, or any loss or damage whatsoever arising from loss of data or profits arising out of, or in connection with, the use of this report.
The report is intended for the recipient only and should not be shared or distributed without the express written consent of CyberSanctus. The recipient agrees to use the information contained in this report only for the purposes of evaluating the security of its own systems and networks and not for any other purpose.

This report is intended to provide information about vulnerabilities discovered during the scope of the engagement, but it should be understood that this report does not guarantee that all vulnerabilities have been identified. The client should also understand that the report does not guarantee the absence of any vulnerabilities that may exist on the client's systems.

This report is based on the information available at the time of the engagement, and the client should be aware that the security landscape changes over time. The client should therefore take the necessary steps to ensure that the vulnerabilities identified in this report are patched in a timely manner.

The client should also be aware that the vulnerabilities reported in this report may be dependent on other vulnerabilities or configurations that are not included in this report. Therefore, the client should not assume that the vulnerabilities reported in this report are the only vulnerabilities that exist on their systems.

Client Data Storage Policy

CyberSanctus is committed to protecting the privacy and security of our clients' data. As part of our security services, we may collect, store, and process client data, including but not limited to, personal information and documents submitted during the engagement process.

We understand that the confidentiality and integrity of our clients' data is of the utmost importance, and we take every precaution to ensure that it is protected and handled in compliance with applicable laws and regulations, including the General Data Protection Regulation (GDPR).

We will only retain client data for as long as is necessary to fulfill the purpose for which it was collected. Following the completion of the engagement, all client data, including pentesting reports, will be deleted from our databases within 30 days.

We will not share client data with any third parties without the express written consent of the client, except as required by law.

We have implemented appropriate technical and organizational measures to protect client data from unauthorized access, alteration, disclosure, or destruction. Our employees and contractors are required to sign a Non-Disclosure Agreement (NDA) and are trained on data protection best practices.

If you have any questions or concerns about our client data storage policy, please do not hesitate to contact us.

Please note that in case of any data breaches, CyberSanctus will follow all the GDPR requirements and will inform the clients and the regulating authorities within 72 hours of detection.

Emergency Response Team

CyberSanctus' ERT team is a group of experts who are trained and equipped to respond to cyber security incidents, such as data breaches, network intrusions, and other security-related incidents. Our ERT team is composed of security analysts, incident responders, forensic investigators and legal advisors who are experienced in handling a wide range of security incidents, and have the necessary tools and resources to quickly identify, contain, and resolve security incidents.

Our ERT team is designed to help organizations quickly and effectively respond to security incidents in order to minimize the impact to their systems, networks, and data. We understand that security incidents can happen at any time, and that quick action is crucial in order to contain and resolve the incident as soon as possible. When an incident occurs, our ERT team is activated immediately and works to understand the scope and impact of the incident, identify the cause, and implement the necessary countermeasures and mitigation steps to limit the damage.

Our ERT team will work with you to recover your systems and networks, and ensure that the incident is fully resolved and that your organization's systems are secure once again. Choosing CyberSanctus' ERT team will give you the peace of mind that comes with knowing that your organization has experts on hand to respond quickly and effectively to security incidents.

Our team is experienced, professional, and dedicated to helping you minimize the impact of security incidents, and to get your systems and networks back to normal operation as quickly as possible. With CyberSanctus' ERT team, you can trust that your organization's assets and sensitive data are in good hands.

In order to purchase this additional offering, please contact the business department via the contact information displayed in the website.