

C8N+FINITY

EMPOWERING YOUR BUSINESS, IS OUR BUSINESS



OUR CREDENTIALS



CYBER TRUST
Practitioner
Certified



ISO 9001



CYBERSECURITY SERVICES REGULATION OFFICE
Penetration Testing Service Licence
Licence No.: CS/PTS/C-2022-0266



CYBERSECURITY SERVICES REGULATION OFFICE
Managed Security Operations Centre (SOC) Monitoring Service Licence
Licence No.: CS/SOC/C-2022-0208

Who we are

Established in June 2021, Contfinity is an IT and cybersecurity managed services provider and cybersecurity consultancy provider. Contfinity partners class-leading established brand principals and distributors to offer customers innovative, reliable and good-value IT and cybersecurity solutions and services.



**Managed IT and
cybersecurity solutions**



***Appointed consultant for
Cyber Security Health Plan
Program***



**Pre-Approved
@SMEs GoDigital Vendor to
provide Cisco Meraki UTM**

WHAT WE DO ?

The aim is to make cybersecurity simpler and bring cybersecurity closer to our customers. We seek to share, to show the way, and to walk alongside our customers and partners in this exciting journey to make Singapore a more cyber-secure and cyber-resilient home for all.



Consultation

Solutioning

Commissioning,
Implementation &
project management

Managed
Services &
Cyber Watch

WHAT WE OFFER



Partner with us to start your cybersecurity journey, establishing basic cybersecurity best practices and earn the Cyber Essentials certification.



Partner with us to showcase your dedication in securing your digital assets and cybersecurity resilience to earn the Cyber Trust certification.



Partner us to be your CISO in your journey to cybersecurity health, enjoy funding support, and earn the Cyber Essentials



Cyber Watch is our specially-curated suite of managed security solutions that helps organization to meet proactively protects your organization from cyber threats and attacks, giving you 24x7 peace of mind.

CYBERSECURITY ROADMAP

Today

BASELINE APPROACH



RISK-BASED APPROACH



Cybersecurity Preparedness Tiers and Domains



INTERNATIONAL STANDARD



Cyber Essentials Mark

The **Cyber Essentials** mark is a cybersecurity certification for organisations that are embarking on their cybersecurity journey. It serves to recognise that your organisation has put in place good cyber hygiene practices to protect your operations and your customers against common cyber attacks.

Why should my organisation apply?

- Tailored to your organisation's cybersecurity needs
- Simplifies cybersecurity by prioritising the measures to focus on first
- Guides your organisation to implement cyber hygiene measures against common cyber attacks
- Provides recognition of your cybersecurity practices

Demonstrate that you have good cyber hygiene.

Scan to learn more:



What measures does my organisation need to implement?



ASSETS

People: Equip employees to be the first line of defence

Hardware and software: Know what hardware and software your organisation has, and protect them

Data: Know what kinds of data your organisation has, where they are stored, and secure them



SECURE/PROTECT

Virus/malware protection: Protect against malicious software like viruses and malware

Access control: Control access to your data and services

Secure configuration: Use secure settings for your organisation's hardware and software



UPDATE

Software updates: Update software on your devices and systems promptly



BACKUP

Back up essential data: Back up your essential data and store them offline



RESPOND

Incident response: Be ready to detect, respond to, and recover from cyber incidents



Cyber Essentials Self-Assessment

Assess your cyber hygiene



	Requirements ("shall" statements)						status	result
	total	yes	no	fail	pass			
A.1 Assets: People	2	2						Pass
A.2 Assets: Hardware and software	8	8						Pass
A.3 Assets: Data	4	4						Pass
A.4 Access: Virus and malware protection	9	9						Pass
A.5 Access: Access control	12	11	1					Fail
A.6 Access: Secure configuration	5	4	1					Fail
A.7 Update: Software updates	1	1						Pass
A.8 Backup: Backup essential data	6	6						Pass
A.9 Respond: Incident response	2	2						Pass
Overall Summary	49	47	2					Fail



CYBER TRUST

The Cyber Trust Mark aims to guide larger or more digitalized enterprises to adopt a risk-based approach by understanding their risk profiles and identifying relevant cybersecurity preparedness areas required to mitigate these risks.

Signifies a mark of distinction to recognize organizations as trusted partners with robust cybersecurity.

	Tier 1: Supporter	Tier 2: Practitioner	Tier 3: Promoter	Tier 4: Performer	Tier 5: Advocate
Cyber Governance and Oversight					
1. Governance			•	•	•
2. Policies and procedures			•	•	•
3. Risk management	•	•	•	•	•
4. Cyber strategy					•
5. Compliance	•	•	•	•	•
6. Audit				•	•
Cyber Education					
7. Training and awareness*	•	•	•	•	•
Information Asset Protection					
8. Asset management*	•	•	•	•	•
9. Data protection and privacy*	•	•	•	•	•
10. Backups*	•	•	•	•	•
11. Bring Your Own Device (BYOD)				•	•
12. System security*	•	•	•	•	•
13. Anti-virus/Anti-malware*	•	•	•	•	•
14. Secure Software Development Life Cycle (SDLC)					•
Secure Access and Environment					
15. Access control*	•	•	•	•	•
16. Cyber threat management				•	•
17. Third-party risk and oversight					•
18. Vulnerability assessment			•	•	•
19. Physical/environmental security		•	•	•	•
20. Network security		•	•	•	•
Cybersecurity Resilience					
21. Incident response*	•	•	•	•	•
22. Business continuity/disaster recovery		•	•	•	•
*Measures in Cyber Essentials Mark	10 DOMAINS	13 DOMAINS	16 DOMAINS	19 DOMAINS	22 DOMAINS

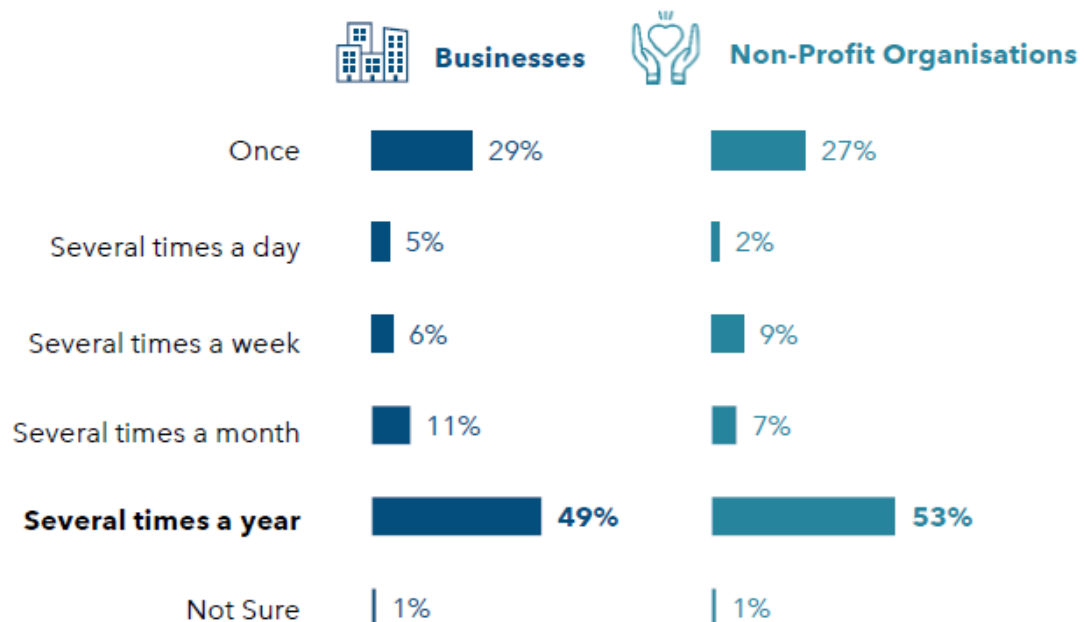
The cyber threat landscape is seeing increasingly sophisticated threats and more brazen threat actors

Threat Landscape

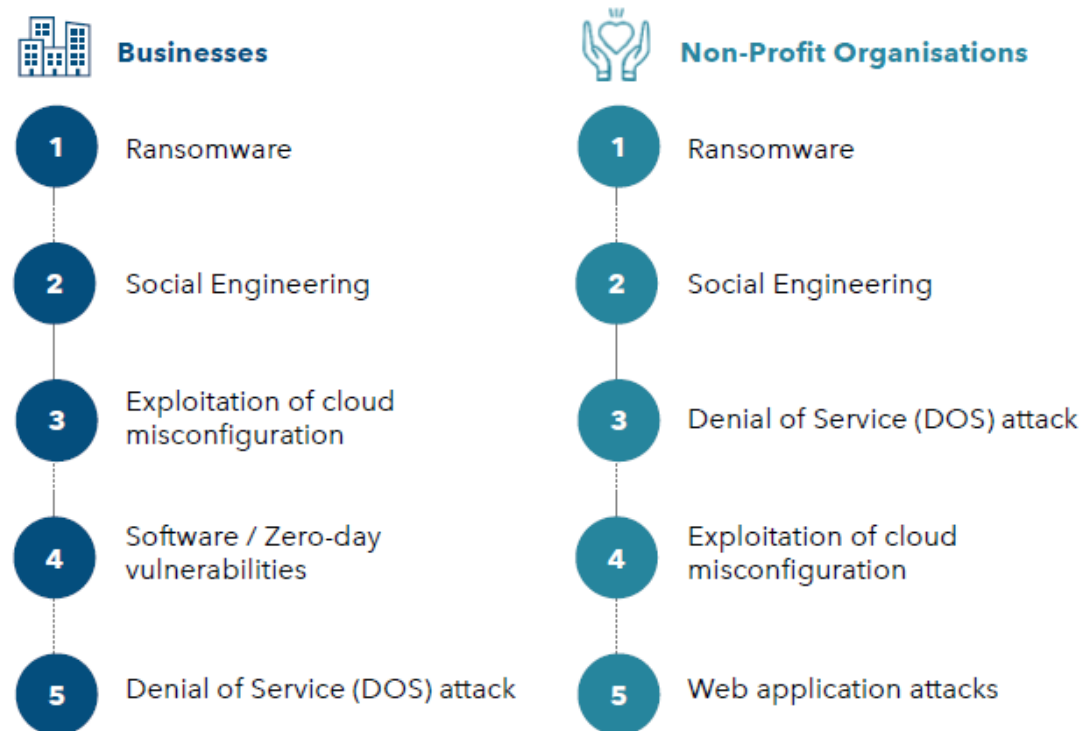


OVER 8 IN 10 organisations have encountered a cybersecurity incident in a year

Frequency of Incidents



Top 5 Incidents



As organisations go digital, cybersecurity incidents increasingly result in business impact

Business Impact



99% of these organisations suffered a business impact

Businesses



Business
Disruption



Data
Loss



Reputation
Damage



31%	Financial loss
27%	Incident response cost
26%	Regulatory implications

Non-Profit Organisations



Data
Loss



Business
Disruption



Reputation
Damage



34%	Financial loss
25%	IP and/or Trade Secret loss
24%	Incident Response cost

We recognise organisations face challenges in implementing cybersecurity

Cybersecurity
Challenges

Challenges in adopting cybersecurity



Businesses

- 59%** Lack of knowledge / experience
- 46%** Unlikely to be a target of cyber attacks
- 39%** Lack of manpower / resources
- 38%** Low priority for the organisation
- 36%** Low ROI for the business
- 31%** Lack of budget
- 20%** Lack of senior management support
- 7%** None



Non-Profit Organisations

- 56%** Lack of knowledge / experience
- 49%** Unlikely to be a target of cyber attacks
- 44%** Low priority for the organisation
- 37%** Lack of manpower / resources
- 31%** Low ROI for the business
- 27%** Lack of budget
- 19%** Lack of senior management support
- 11%** None

➔➔ A lot more needs to be done - CSA has various initiatives to help you ➔➔

MEASURE YOUR CYBERSECURITY HEALTH INDEX

- Identify your cyber hygiene gaps
 - Know where you are, compared with the industry benchmarks
-

IMPLEMENT CYBER ESSENTIALS

- Equip yourself with good cyber hygiene
 - Stay protected against common cyber attacks
-

IF YOU NEED HELP WITH YOUR CYBERSECURITY IMPLEMENTATION

- Approach the CISO as-a-Service cybersecurity consultants onboarded by CSA
- Funding support available for eligible organisations



CSA SG Cyber Safe programme supports organisations in this journey

<https://www.csa.gov.sg/sgcybersafe>



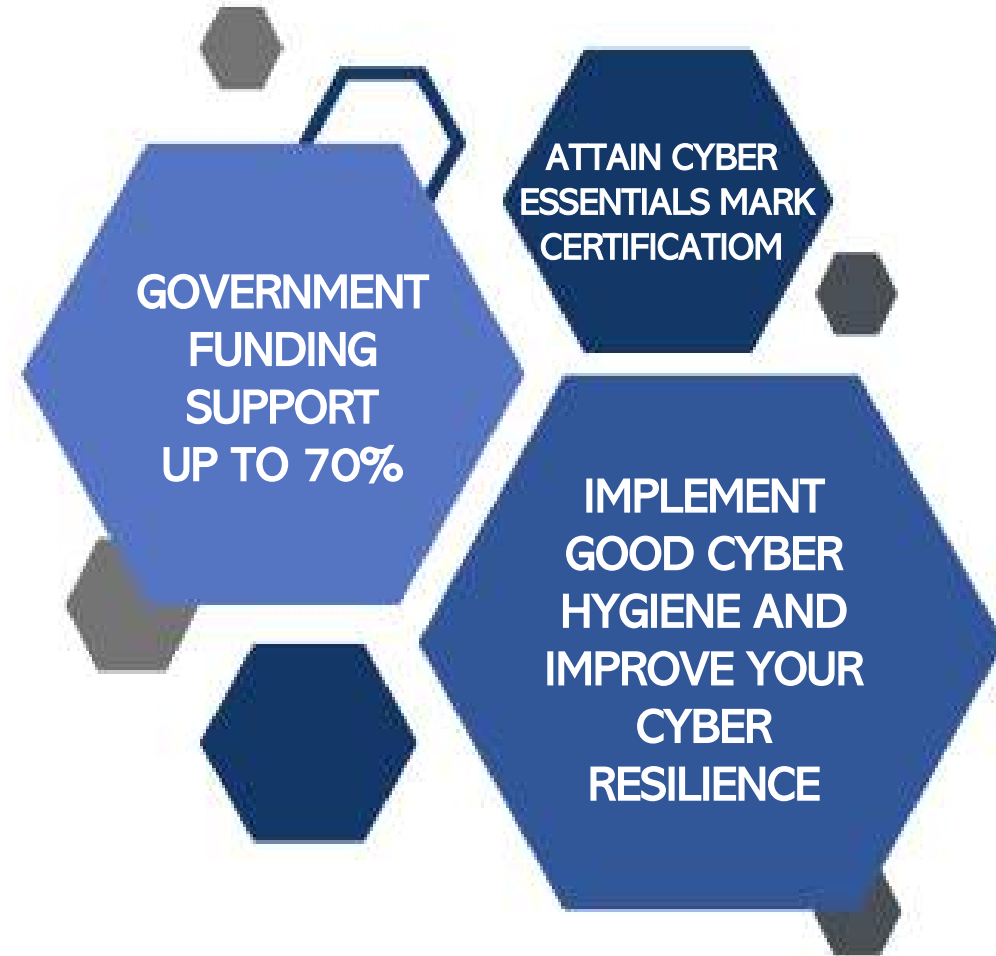
CYBERSECURITY HEALTHPLAN

Delivered by Contfinity as CISO as-a-Service (CiSOaaS) Consultants

Why organizations should apply

If you are just getting started in your cybersecurity journey, Contfinity will help you to improve your cyber resilience through cyber health “checkups”. We will develop a cybersecurity health plan tailored for your needs.

- Be cyber-resilience and aware of your cyber security posture.
- Tailored to your organization’s cybersecurity needs
- Simplifies cybersecurity by prioritizing the measures to focus on first
- Guides your organization to implement cyber hygiene measures against common cyber-attacks
- Provides recognition of your cybersecurity practices



Your Cybersecurity Health Plan Journey with Contfinity

Our consultants will help your organization successfully complete the Cybersecurity Health Plan journey and achieve Cyber Essentials mark certification.

1. Preliminary



- Understand customer's cybersecurity objectives and status
- Determine consultancy fees tier
- Apply for funding support and appoint certification body
- Required documents: ACRA, Network diagram, Org chart

2. Consulting



- Assess cybersecurity posture pre-CISOaaS and identify gaps
- Close gaps and assess cybersecurity posture post-CISOaaS
- Develop / enhance IT Security Policy

3. Submission & Certification

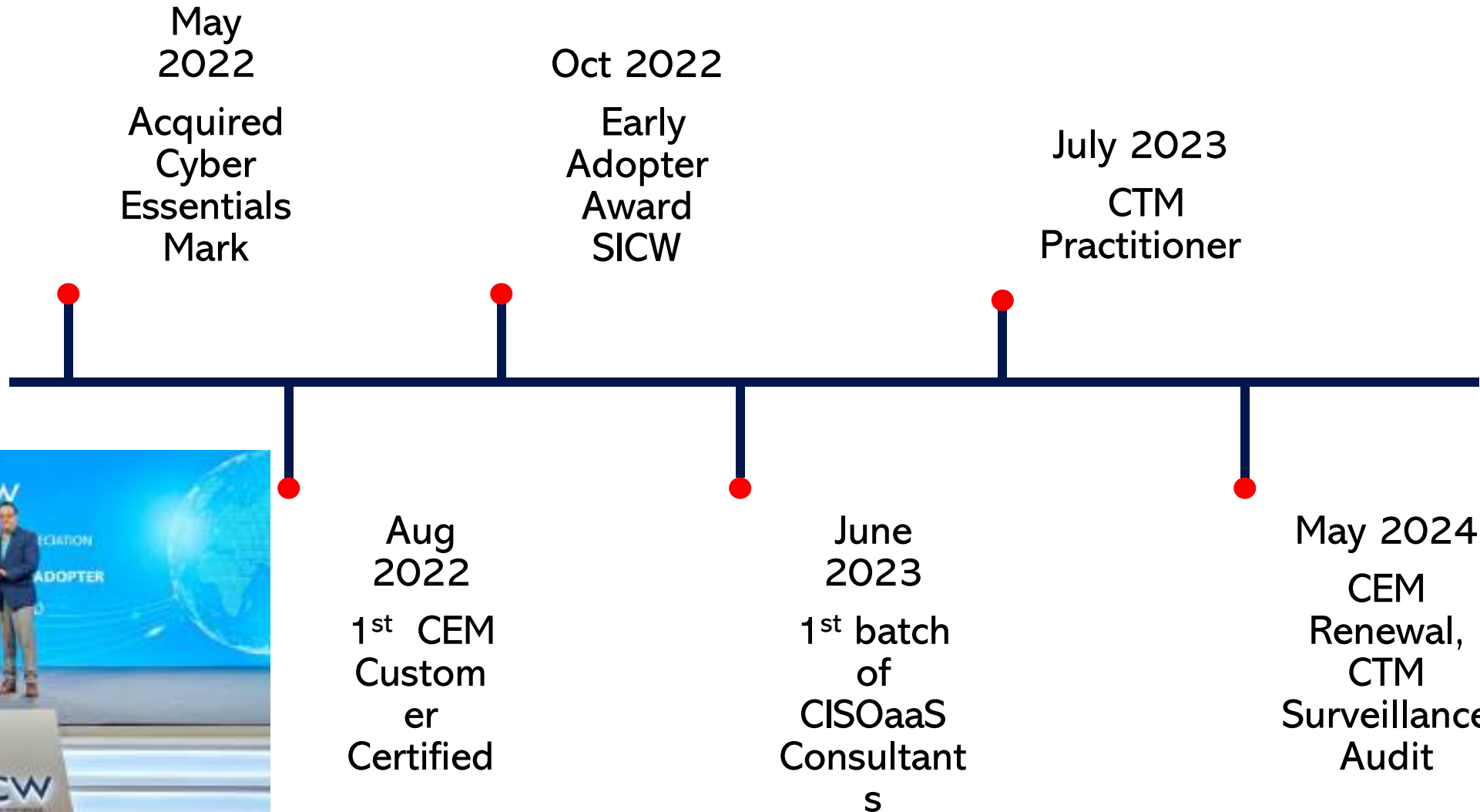


- Submit Schedule B Cybersecurity Health Plan
- Follow up on certification outcome
- Awarded Cyber Essentials Mark or Cyber Trust Mark

Contfinity SG CYBERSAFE Journey



CYBER TRUST
Practitioner
Certified



Contfinity CEM Consultancy Services



PROFESSIONAL SERVICES:



Information Gathering

To understand current CEM readiness



Cybersafe readiness

Guide and Review of IT Security Policies, Access Control, Security Solutions Config – FW, EDR etc to achieve Cybersafe and improve Cybersecurity Postures



Backup Strategy & Incident Response Plan

Implement / Review of Backup Strategy – RPO, RTO to improve Cyber Resillency



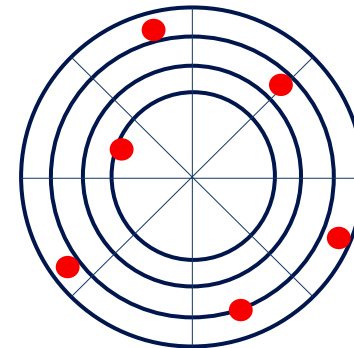
CEM Submission

Prepare and submit CEM documentation. Work with Appointed Certification Body for CEM audit

CYBER WA+CH

- **Monitoring and reporting of vulnerabilities** - Automated attack surface scanning of your environment to continuously identify areas of weaknesses.
- **Contextual threat intelligence** - real exploitation context as well as availability of exploit codes in the wild to show your actual exposure and cyber risks.
- **Automated Triage, Ticketing & Reporting** – Enabling operations to continue smoothly and maintain up time.

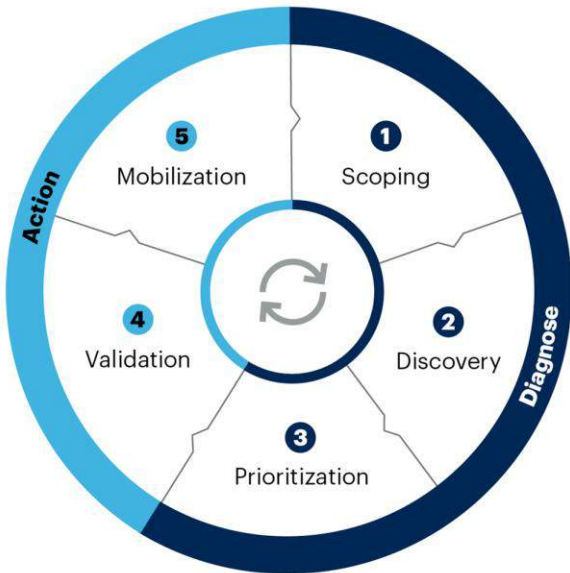
Attack Surface Monitoring & Vulnerability Assessment with



Radar

Globally Recognised Framework

5 Steps in the Cycle of Continuous Threat Exposure Management



gartner.com

Source: Gartner
© 2023 Gartner, Inc. All rights reserved. CM_GTS_2477201

Gartner.

“Continuous threat exposure management is a pragmatic and effective systemic approach to continuously **refine priorities** and walk the tightrope between two modern security realities.

Organisations **can't fix everything**, nor can they be completely sure what vulnerability remediation they can safely postpone.”⁴

⁴Gartner Article, *How to Manage Cybersecurity Threats, Not Episodes*, By Kasey Panetta

Assessing your posture with top of the line tools



CONFIDENTIAL

VULNERABILITIES SUMMARY

Vulnerability Priorities Breakdown

The following table summarises the count of vulnerabilities for each Priority, discovered and triaged during the timeframe selected:

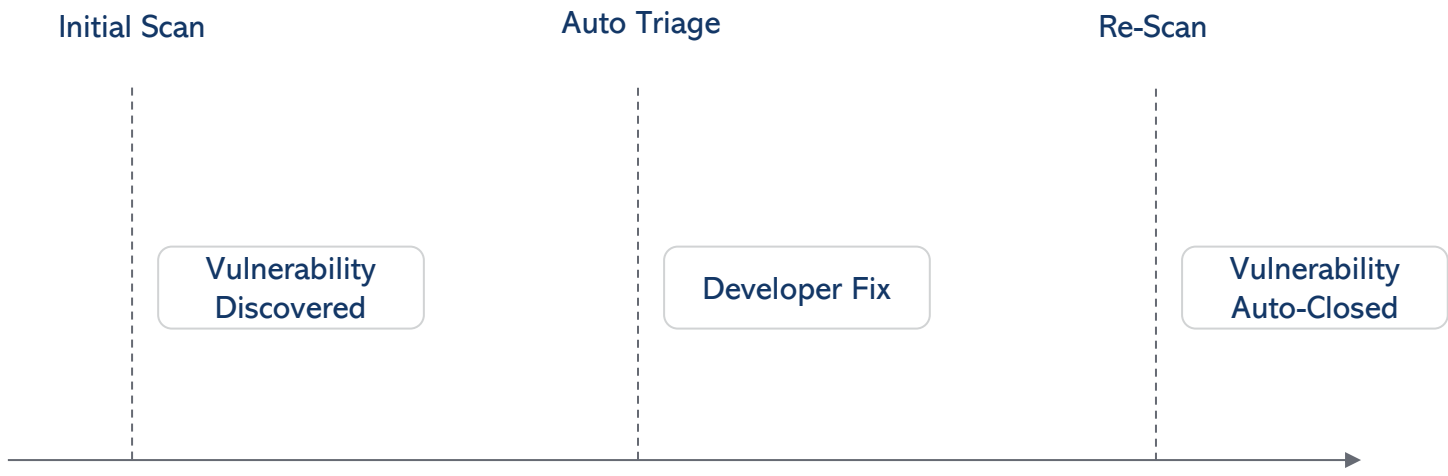
Critical	High	Medium	Low	Lowest
4	1	11	10	3

Vulnerability Table List

The following table lists the major details of vulnerabilities for each Priority, discovered and triaged during the timeframe selected. For further details including remediation advise, refer to the Detailed Report:

- **Identification and reporting of vulnerabilities** - Automated attack surface scanning of your environment to identify areas of weaknesses.
- **Contextual threat intelligence** - real exploitation context as well as availability of exploit codes in the wild to show your actual exposure and cyber risks.

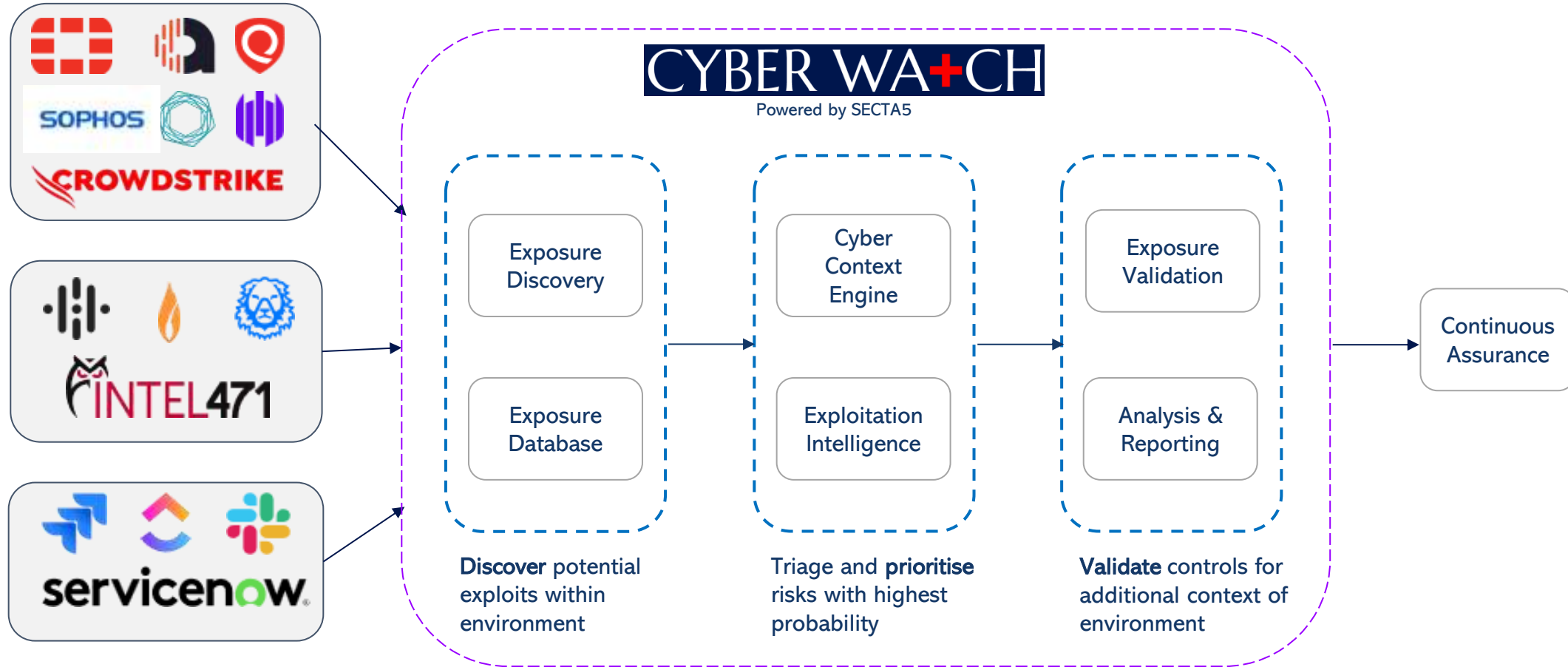
Seamless Workflow



Proven to reduce vulnerability triage and management workload by more than **90%**

- Automated attack surface scanning to continuously identify areas of weaknesses
- Match the identified vulnerabilities against real life exploitation intelligence to understand your risks
- Auto-triage based on your organisational context
- Prepare remediation based on advice provided within the platform
- Validate fixes via the next scanning window
- Auto-close issues upon valid resolution

High level architecture



Client Success Story

Problem Statement

10,000+

hosts within critical infrastructure needs to be resilient and up to date 24x7

Solution Deployed

5 pillars

of CTEM fully automated over the use of manual triage and response

Business Impact

S\$64.5M

enterprise and consumer users may lose communication access if breached

Business Outcome

3x

less likely to be compromised based on Gartner if CTEM is deployed

*"CyberWatch significantly optimised our vulnerability management operations and we managed to free up more than **95%** of our time from laborious manual efforts compared to the past."*

Daniel Tan, CEO

Client Success Story

Problem Statement

120

retail outlets that handles >a million client data requires exposure monitoring

Solution Deployed

7 days

exposure review cycle introduced to replace annual security testing

Business Impact

S\$64.5M

annual turnover business with high network clientele may be targeted

Business Outcome

52x

increase in security coverage with full security advisory with higher ROI

*"We are now able to identify our exposure **much quicker** now."*

Dave L.

Director, Group Technology

Why You Should Adopt

Current Approach	CYBER WA+CH
Manual scans to identify voluminous vulnerability loads	Automation of vulnerability scanning, ingestion and triage
Vulnerabilities typically lack context as-is	Auto-triaging and application of context to vulns allow reflection of true risk, without the use of 'proprietary' black box number generators
Manual tracking of assignments and remediations	Auto-close of vulnerabilities that have been resolved
Adversarial simulation in a point in time format	Continuous validation and enhancement of security posture

CYBER WA+CH



- Managed Security Training & Education services.
- Curated & gamified content
- Advanced reporting and metrics

Employees are every organization's first responders, that's why it's important to keep them educated, trained & aware. We aim to provide quality security training while also reducing the effort on your end.



Enabling your employees to be the first line of defense.

CYBER WA+CH

Data Loss through ransomware, data corruption and even theft are just some of the common ways organizations lose their **business-critical data**.

Developing a backup strategy and the appropriate solution in place to support that strategy is paramount in **ensuring data security**.

Plan B

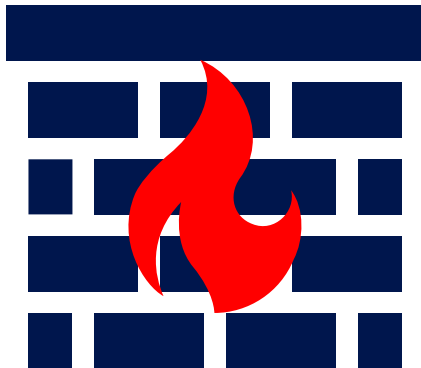
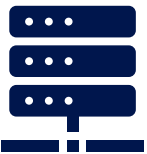


- One Drive, Teams, and mail backed up.
- Ensuring data availability at times of crisis.
- Develop your backup strategy with defined RTO and RPO's accordingly to suit your data strategy needs.

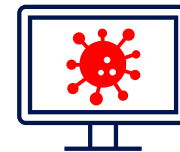
CYBER WA+CH

ProtectU

Your network infrastructure is one of the most critical assets you own. **ProtectU** Ensures that your digital ecosystem is protected against common threats like ransomware, backdoors, DDoS and spam.



ransomware



malware



DDoS

- Managed Firewall Services
- Enterprise Grade SD-Wan Ready
- NGFW with Layer 7 with identity-based Security Policies & Apps Management
- Integrated Intrusion and Detection.
- 24/7 Firewall Monitoring and Management
- Protected against ever-evolving Cyber Threats with Cisco Talos

CYBER WA+CH

Enabling you to carry on with business, worry free.

With next-generation firewalls(NGFW), we'll be able to help you remotely manage your security and help you safeguard your network infrastructure. You'd be able to stay secure while gaining control over network insights, real-time monitoring, and analytics.

- Cloud Managed Security
- Live Network Monitoring & Logging
- Comprehensive Application Visibility & Control
- Integrated Intrusion Detection & Prevention.
- 24/7 Incident Management, Technical Assistance & Support

Cisco Meraki Unified Threat Management

50% off for qualified SMEs for 1 year

MX75	MX85	MX95	MX105
Up to 200 users	Up to 250 users	Up to 500 users	Up to 650 users
\$5,000/year	\$5,700/year	\$8,900/year	\$13,000/year

Networks

Network tags

Devices

Tag ▾ Combine ▾ Delete Search... ▾ 3 networks Over the last week: 29 clients, 47.67 GB

<input type="checkbox"/>		Name	Usage	Clients	Tags	Network type	Devices	Offline devices
<input type="checkbox"/>		DC	1.36 GB	3		Appliance	1	0
<input type="checkbox"/>		609 Greenridge	11.67 GB	15	609_greenridge	Appliance	1	0
<input type="checkbox"/>		313 Upper Paya Lebar	34.64 GB	11	313_Upper_Paya_Lebar	Appliance	1	0

3 total



313 Upper Paya

Lebar_MX

MX8BCW-WW 88:3a:1e:45:45:bd



ADDRESS
165 Upper Paya Lebar Road 5534858

WARM SPARE

Configure warm spare

WLAN 1

Ready

Active

HOSTNAME

313-upper-paya-lebar-
z2dcgkjhcc.dynamic-m.com

313_upper_paya_lebar

NOTES

LEGAL & REGULATORY
Regulatory certification

FIRMWARE

Up to date
Current version: MX 16.16

Summary

Uplink

DHCP

Location

Tools

Ports



Live data

Current clients 0

There are no currently connected clients.

Utilization on current channels

802.11 Traffic non-802.11 Interference

Channel 1 (2.4 GHz): 17% (Acceptable)



Channel 44 (5 GHz): 1% (Acceptable)



Historical device data for the last month

Connectivity



Network usage



This website is blocked by your network operator.

If you feel you have received this message in error, please contact your network operator with the following information:

URL: <http://www.internetbadguys.com/>

Server: 146.112.255.155:80



Organization
Contnity Pte Ltd ▾

Network
Contnity Office ▾

Network-wide

Security & SD-WAN

Switch

Wireless

Cameras

Sensors

Organization

Event log for security appliances ▾

Client: Any Before: 08/10/2022 18:22 (+00)

Event type include:

- All security appliance events x
- Content filtering blocked URL x

Event type ignore:

None

Search [Reset filters](#)

Download as ▾

Time (UTC) ▾	Client	Event type	Details
Aug 10 18:11:37	CONT-NB-ROY	Content filtering blocked URL	url https://www.detrinityshop.com/..., server 172.67.184.38:443, categories
Aug 10 18:11:37	CONT-NB-ROY	Content filtering blocked URL	url https://www.detrinityshop.com/..., server 172.67.184.38:443, category Weapons
Aug 10 17:44:09	CONT-NB-JEREL	Content filtering blocked URL	url http://www.tekdefense.com/downloads/malware-samples/, server 198.385.159.177:80, category Hacking
Aug 10 17:39:49	CONT-NB-JEREL	Content filtering blocked URL	url http://www.internetbadguys.com/, server 146.112.255.155:80, categories
Aug 10 17:39:49	CONT-NB-JEREL	Content filtering blocked URL	url https://www.internetbadguys.com/..., server 146.112.255.155:443, categories
Aug 10 17:39:49	CONT-NB-JEREL	Content filtering blocked URL	url https://www.internetbadguys.com/..., server 146.112.255.155:443, category Phishing and Other Frauds
Aug 10 17:39:49	CONT-NB-JEREL	Content filtering blocked URL	url https://www.internetbadguys.com/..., server 146.112.255.155:443, category Phishing and Other Frauds
Aug 10 17:37:39	DESKTOP-HIMSGEJ	Content filtering blocked URL	url http://www.plyboy.com/, server 202.128.161.233:80, categories
Aug 10 17:36:29	DESKTOP-HIMSGEJ	Content filtering blocked URL	url http://www.plyboy.com/, server 202.128.161.233:80, category Adult and Pornography
Aug 10 17:34:28	CONT-NB-JEREL	Content filtering blocked URL	url http://2016.picar.org/85-O-Download.html, server 89.238.73.67:80, category Malware Sites

From: Cisco Meraki - No Reply <alerts-noreply@meraki.com>

Sent: Thursday, August 11, 2022 4:55:00 PM

To: simon.woo@ <simon.woo@>; TechSupport <techsupport@Contfinity.com>

Subject: Alert for [\[REDACTED\]](#) Cisco Warehouse [\[REDACTED\]](#) - Malware download blocked



Meraki

3 file downloads on your network 'DR01_ [\[REDACTED\]](#) Warehouse - appliance' were blocked in the last hour because they were determined to be malicious.

Investigate the impact [here](#).

- Cisco Meraki

This email was automatically generated; please do not reply.

You can change the [alert delivery settings](#) for this network.

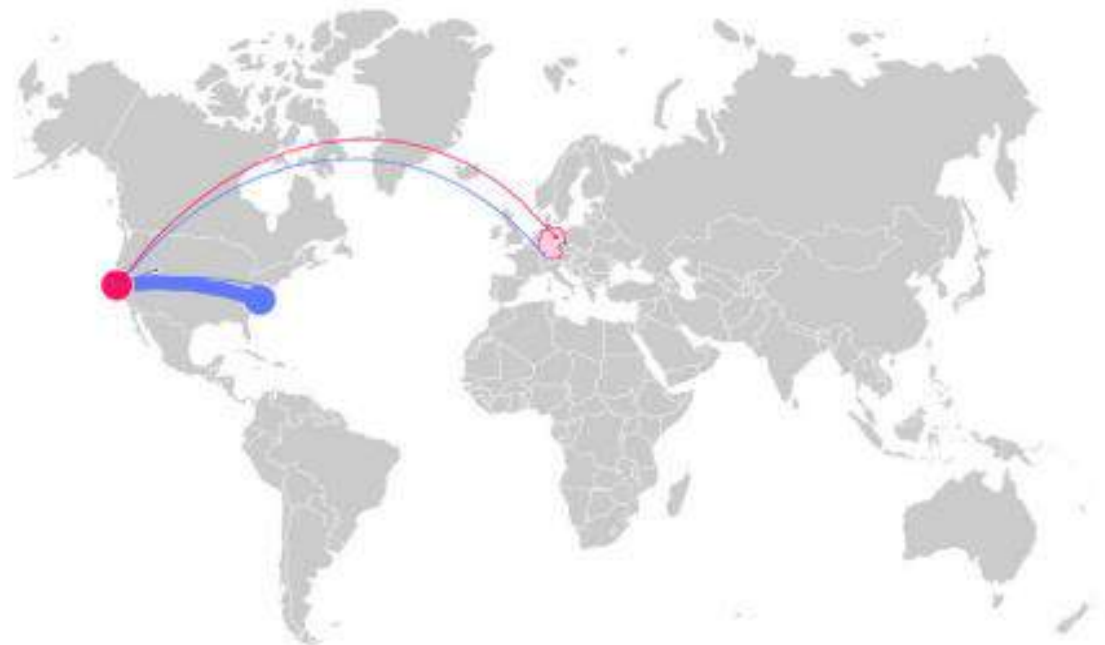
Events over time



Most affected clients

Client	Network	Last Affected	Events
MSWEATT-M-G039 <small>Mac OS X 10.12</small>	Meraki San Francisco - Security	Aug 9 13:42:48	16
10.92.105.8 <small>Apple iPad</small>	Meraki San Francisco - Security	Aug 13 14:28:57	11
CCHEN-X260 <small>Meraki Network OS</small>	Meraki San Francisco - Security	Aug 14 11:03:55	7
10.92.105.6 <small>Apple iPhone</small>	Meraki San Francisco - Security	Aug 16 0:32:14	5
YvonneSmariaMBP <small>Mac OS X 10.12</small>	Meraki San Francisco - Security	Aug 10 13:24:57	3
EVFLEISC-M-P131 <small>Mac OS X 10.12</small>	Meraki San Francisco - Security	Aug 8 14:16:09	3
10.92.105.160 <small>Apple iPhone</small>	Meraki San Francisco - Security	Aug 7 0:55:17	3
10.92.105.172 <small>Apple iPhone</small>	Meraki San Francisco - Security	Aug 18 16:21:02	3
SpencerMBP914 <small>Mac OS X 10.12</small>	Meraki San Francisco - Security	Aug 17 6:06:08	2
ABOLLINGER-X260 <small>Mac OS X 10.12</small>	Meraki San Francisco - Security	Aug 15 12:56:05	2

Top sources of threats






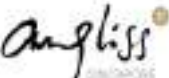
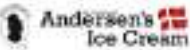



CERTIFIED ORGANISATIONS

List of Cyber Essentials Certified Organisations

Updated: 29.09.2023










 Charles Tan Surgery Expiry date: 02.01.2025	 Clarity Singapore Limited Expiry date: 21.12.2024	 Continuity Pte Ltd Expiry date: 19.05.2024	 Coverageous Pte Ltd Expiry date: 19.06.2024
 georges Expiry date: 01.06.2024	 Angliss Singapore Pte Ltd Expiry date: 20.08.2024	 Andersen's of Denmark Ice Cream Expiry date: 01.06.2024	 Dovechem Industries Pte Ltd Expiry date: 02.01.2025

List of Cyber Trust Certified Organisations

Updated: 29.09.2023



 Availilit Pte Ltd Expiry date: 12.06.2026	 Bass Aero Pte Ltd Expiry date: 14.03.2026	 Continuity Pte Ltd Expiry date: 26.07.2026	 CyberSafe Pte Ltd Expiry date: 14.11.2025
 Klobbi Pte Ltd Expiry date: 25.06.2026	 Life Planning Associates Pte Ltd Expiry date: 30.03.2026	 LINX Singapore Pte Ltd Expiry date: 30.01.2026	 Momentum Z Pte Ltd Expiry date: 15.01.2026

Our Partners

Acronis

 Barracuda.
Your journey, secured.

 **BLACKPANDA**

 **CHECK POINT**


CISCO

 **Meraki**

DELL

dedoco

druva

 **elastic**


**Hewlett Packard
Enterprise**

HPE **aruba**
networking

FORTINET.

JUNIPER.
NETWORKS

KnowBe4
Human error. Conquered.

 **Microsoft**

mimecast

Lenovo

 **paloalto**
NETWORKS

NUTANIX

SECTA5

veeam

 **TREND
MICRO**

vmware

ZYXEL
NETWORKS

Our Customers





scash

G L O B A L





CAPELLA



Our heartiest congratulations to **CAPELLA HOTEL GROUP** on being the first hotel group to achieve the highly recognized **CSA Cybersecurity Certification Cyber Essentials** mark.

Capella Hotels and Resorts was awarded as "#1 **Favourite Hotel Brand**" in the **Travel + Leisure World's Best Awards 2023**". The exceptional hospitality brand focuses on crafting authentic, cultural experiences for its guests, combining a legacy of thoughtful design with the highest level of personalised service.

On this special day, we have the honour to invite Ms [Veronica T.](#), Director, Safer Cyberspace ...see more

👍 11

1 comment

👍 Like 💬 Comment ↻ Repost ✈ Send



**CYBER
ESSENTIALS**

Certified

“We extend our heartfelt gratitude to Confinity’s exceptional support throughout our collaboration. Confinity understood our requirement to speed up the certification timeline. They has demonstrated unwavering dedication to our project from start and also continued with great support after sales service. Their responsiveness and ability to keep pace with our timeline have been remarkable, making them an indispensable partner in our project's success.”



CISOaaS consultant pricing (without solutioning)

Range of Endpoints	Professional Fees (before funding support)	Funding Support (based on 70% professional fees)	Net Professional Fees Charged
<u>1 – 10</u>	S\$ 4,380	S\$ 3,066	S\$ 1,314
<u>11 - 20</u>	S\$ 6,380	S\$ 4,466	S\$ 1,914
<u>21 – 50</u>	S\$ 10,880	S\$ 7,616	S\$ 3,264
<u>51 – 100</u>	S\$ 16,880	S\$ 11,816	S\$ 5,064
<u>101 - 200</u>	S\$26,880	S\$ 18,816	S\$ 8,064

C8N+FINITY

SECURING YOUR BUSINESS, IS OUR BUSINESS

CONTACT US:



sales@contfinity.com



+65-6871-8855



33 Ubi Avenue 3, #08-59 Vertex Tower A
Singapore, 408868



www.contfinity.com

