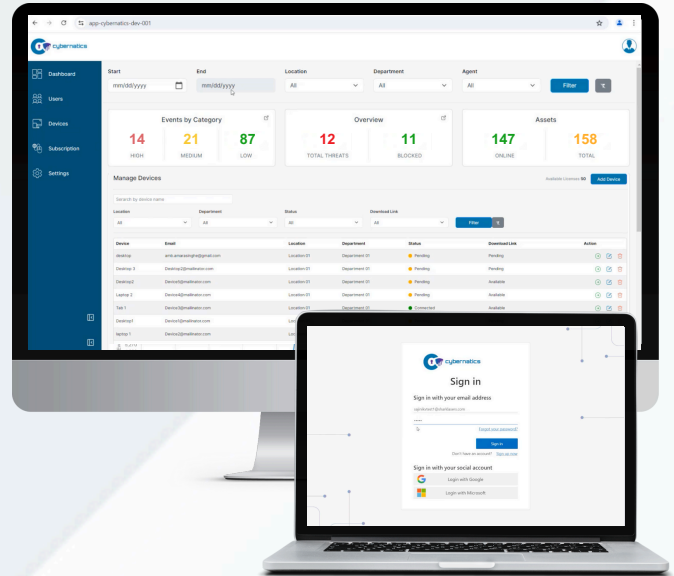


WE SEE WHAT YOU DON'T SEE

With over 80% of organizations encountering cybersecurity issues annually, Cybernatics is your business's primary defense. Cybernatics' SaaS Vulnerability Assessment and Compliance Report enhances your security without disrupting operations. We proactively identify vulnerabilities, reduce the attack surface, and optimize security policies. Our system automates essential processes, allowing your staff to focus on strategic goals rather than routine checks. **Secure your business's future with Cybernatics.**



START

- ✓ Malware & Ransomware Detection
- ✓ File Integrity Monitoring
- ✓ Log Analysis
- ✓ High Security Alerts
- ✓ Automated Response

SEE

- ✓ Vulnerability Visibility Report Enhances ROI
 - Reducing security incidents
 - Lowering remediation costs
 - Optimizing resource use
 - Protecting the organization from costly breaches and compliance penalties
- ✓ Security Configuration Assessment Report

COMPLY

- ✓ Comprehensive coverage on various framework or standards across industries:
 - PDPA, CYBER TRUST MARK, GDPR, PCI DSS, HIPAA, NIST, CIS, MAS TRM, RMIT AND MORE.

Why Cybernatics?

Businesses need powerful security solutions that grow with their digital transformation. Cybernatics enhances your security infrastructure without impacting operations. Our SaaS Vulnerability Assessment, Compliance Report, and Endpoint Security solutions seamlessly integrate into your systems to proactively identify weaknesses and strengthen security. Cybernatics provides IT operations with precise, easy-to-understand data that demonstrate ROI. Affordable, scalable, and easy to customize, the platform grows with your company. Cybernatics helps your IT staff concentrate on strategic projects while we manage cybersecurity.

Quotes:

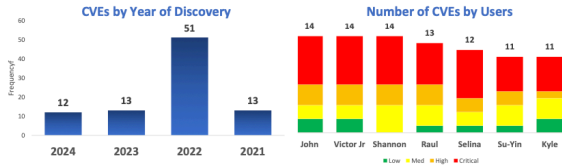
“ These incidents almost always result in a negative impact, **with 99% of the organisations which encountered an incident reporting that they suffered a business impact.** The top three business impacts cited were **business disruption** (48% for both businesses and non-profits), **data loss** (46% for businesses, 60% for non-profits) and **reputation damage** (43% for businesses, 44% for non-profits). Others included financial loss (31% for businesses, 34% for non-profits) and costs incurred from incident response measures (27% for businesses, 24% for non-profits). ”

VULNERABILITY VISIBILITY REPORT

Vulnerability Visibility Report



generated on 3 August 2024



CVSS	Frequency	CVE	Description
9.8	7	CVE-2022-34722	Windows Internet Key Exchange (IKE) Protocol Extensions Remote Code Execution Vulnerability
9.8	5	CVE-2022-21849	Windows Internet Key Exchange (IKE) Protocol Extensions Remote Code Execution Vulnerability
9.8	5	CVE-2022-29130	Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability
9.8	5	CVE-2022-21907	HTTP Protocol Stack Remote Code Execution Vulnerability
9.8	3	CVE-2022-24497	Windows Network File System Remote Code Execution Vulnerability
9.8	3	CVE-2022-34728	Windows TCP/IP Remote Code Execution Vulnerability
9.8	3	CVE-2022-34721	Windows Internet Key Exchange (IKE) Protocol Extensions Remote Code Execution Vulnerability
9.8	1	CVE-2022-22012	Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability
9.8	1	CVE-2022-24491	Windows Network File System Remote Code Execution Vulnerability
9.8	1	CVE-2023-30133	Windows Point-to-Point Protocol (PPP) Remote Code Execution Vulnerability
9.8	1	CVE-2022-26809	Remote Procedure Call Runtime Remote Code Execution Vulnerability
9.0	7	CVE-2021-26443	Microsoft Virtual Machine Bus (VMBus) Remote Code Execution Vulnerability
8.1	7	CVE-2021-43217	Windows Encrypting File System (EFS) Remote Code Execution Vulnerability
8.1	1	CVE-2024-22243	Spring Framework URL Parsing with Host Validation
7.8	7	CVE-2022-21874	Windows Security Center API Remote Code Execution Vulnerability
7.8	1	CVE-2024-21346	Win32k Elevation of Privilege Vulnerability
7.0	1	CVE-2024-25243	Windows USB Print Driver Elevation of Privilege Vulnerability
6.4	1	CVE-2023-23346	Use of a broken cryptographic algorithm affects HCL DRIVE MyCloud
5.5	1	CVE-2023-26443	CNA: Open-Xchange
4.9	1	CVE-2023-23546	Improper Certificate Validation

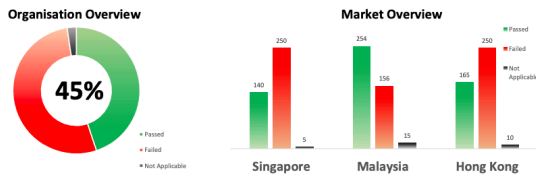


COMPLIANCE REPORT

Compliance Report for Personal Data Protection Act 2012



generated on 3 August 2024



Title	Result	Users Affected
Ensure 'Enforce password history' is set to '24 or more password(s)'.	Failed	94
Ensure 'Minimum password age' is set to '1 or more day(s)'.	Failed	84
Ensure 'Minimum password length' is set to '14 or more character(s)'.	Failed	81
Ensure 'Relax minimum password length limits' is set to 'Enabled'.	Failed	75
Ensure 'Account lockout duration' is set to '15 or more minute(s)'.	Failed	72
Ensure 'Account lockout threshold' is set to '5 or fewer invalid logon attempt(s), but not 0'.	Failed	64
Ensure 'Reset account lockout counter after' is set to '15 or more minute(s)'.	Failed	61
Ensure 'Accounts: Block Microsoft accounts' is set to 'Users can't add or log on with Microsoft accounts'.	Failed	58
Configure 'Accounts: Rename administrator account'.	Failed	55
Configure 'Accounts: Rename guest account'.	Failed	51
Ensure 'Devices: Allowed to format and eject removable media' is set to 'Administrators and Interactive Users'.	Failed	50
Ensure 'Devices: Prevent users from installing printer drivers' is set to 'Enabled'.	Failed	49
Ensure 'Domain member: Maximum machine account password age' is set to '36 or fewer days, but not 0'.	Failed	45
Ensure 'Interactive logon: Do not require CTRL+ALT+DEL' is set to 'Disabled'.	Failed	43
Ensure 'Interactive logon: Don't display last signed-in' is set to 'Enabled'.	Failed	40

Keeping Your Business Safe and Meeting Regulatory Compliance

- Provide regulatory-compliant cybersecurity solutions.
- Ensure that clients' cybersecurity practices align with industry guidelines and standards.



Talk To Our Experts

- Email: cassie.lee@cybernatics.io
- Contact: +65 6747 7855
- Website: www.cybernatics.io

Follow Us



COMMON ISSUES WE ADDRESS

Respond to Malware and Ransomware Attacks

Detect malware, block and quarantine malicious files and processes.



Vulnerability Visibility

Scan your network for the latest Common Vulnerabilities and Exposures (CVEs), highlighting the critical alerts.



File Integrity Monitoring

File Integrity Monitoring detects unauthorized changes, ensuring security, compliance, and system integrity.



Log Analysis

Monitor and analyze log data to identify security threats, detect anomalies, and provide actionable insights across your organisation.



High Security Alert

Detect and respond to critical security threats in real time, alerting teams to potential breaches and enabling swift action.



User Data Privacy

Ensure compliance with the Personal Data Protection Act (PDPA), safeguarding sensitive information and protecting individual privacy rights.



#WeSeeWhatYouDontSee

Top 7 Cybernetics High Alerts

Unauthorized Access

1	Scenario	Security Significance
	Multiple failed login attempts or unusual login behavior. Successful login from a suspicious or unknown location.	It could indicate someone is trying to break into a system. Shows that an unauthorized person might have gained access.



Malware Activity

2	Scenario	Security Significance
	Detection of known malicious software or suspicious file behavior. Execution of unexpected scripts or programs.	It could indicate someone is trying to break into a system. These might be signs of malware trying to run secretly.



System Vulnerabilities

3	Scenario	Security Significance
	Outdated software or unpatched systems. Use of weak or default passwords.	Hackers often exploit weaknesses in old software to gain access or cause harm. Weak passwords make it easier for hackers to break in.



Abnormal Network Traffic

4	Scenario	Security Significance
	Large or unexpected data transfers. Connections to known malicious websites or servers.	Could indicate sensitive information being stolen or unusual activity. Suggests a system might be communicating with hackers.



Privileged Account Misuse

5	Scenario	Security Significance
	Changes made by administrative accounts outside regular tasks. Creation of new, unexpected administrator accounts.	Misuse of high-level accounts can cause significant harm. A sign that someone is trying to gain control over critical systems.



Suspicious Behavior

6	Scenario	Security Significance
	Multiple files being deleted or modified rapidly. Unusual system restarts or shutdowns.	This could mean someone is trying to erase or alter important data. Can indicate an attacker covering their tracks or causing disruption.



Policy Violations

7	Scenario	Security Significance
	Installation of unauthorized software or tools. Use of personal or unapproved devices to access systems.	Unauthorized software can be risky and compromise security. These devices might introduce vulnerabilities or bypass security measures.



Customer Testimonials

5 STAR REVIEW



“Since partnering with Cybernatics, we’ve felt a significant boost in our cybersecurity confidence. Their SaaS platform is incredibly intuitive, and the real-time alerts for malware activity and unauthorized access have saved us from potential threats.”

Cybernatics has been an invaluable partner for us. Their ability to monitor and alert on suspicious behavior and abnormal network traffic has been a lifesaver. Their platform is user-friendly, and their team is always responsive.



Cybernatics made it so easy for us. Their SaaS platform monitors everything from system vulnerabilities to policy violations, giving us peace of mind. The alerts are timely, and the insights have helped us tighten our security measures.

As a tight-knit team in the fast-paced M&A world, cybersecurity used to keep us up at night. Cybernatics was a game-changer. Their easy-to-use, affordable platform integrated seamlessly and didn’t strain our budget.



As a small team, we don’t have the luxury of a dedicated IT security person, but Cybernatics makes it feel like we do. Now, we can focus on what we love building awesome websites for our clients without worrying about threats. Seriously, if you’re an SME, just get it!

As an MSP, we’re all about keeping businesses safe and running smoothly, and Cybernatics fits right into that mission. It’s like having an extra layer of security that just works, without the headaches. For any business serious about cybersecurity, this is a no-brainer. Highly recommend!”

