aqüta
data sciences

VIGILANTE
HumanFirewall

BUILD YOUR HUMAN FIREWALL WITH VIGILANTE

MINIMISING HUMAN RISK

Cybersecurity awareness training programs have little or no impact so far. Because 80% of cyber breaches is still due to hackers exploting human weaknesses mainly through social engineering and/or OSINT. Cheap tricks and tools are the favoured MO because they work! And giving the best return with lowest financial and exposure risk to hackers.

Why has cybersecurity awareness training failed in stopping hackers tricking your staff?

Because non-IT staff find it hard to internalise the threats when they do not understand how cyber space works. Our research shows 99% of people do not know how the Internet works! Few know how their personality/behaviors are exploitable by hackers. Even fewer know how the criminal mind works and the basic persuasion techniques they all use so effectively to trick your staff.

Our Human Firewall Program changes the odds against the hackers by training your staff to be Cyber Vigilantes monitoring their own behaviour risk as well as criminal attempts. Find out how below.

Why sign-up your organization?

If you are eager to train all your staff to be Cyber Vigilantes by learning how to keep data safe from hackers, or if any of the below describe you, enrolling your organization in the Human Firewall Program could help you create a hardened first line of defence against hackers:

Your general staff may be aware of cyber risks (from past awareness training workshops) but they have no visibility on what hackers are attempting in real time. Hence, there is unintended ignorance with little feedback on what hackers are up to in hoodwinking them.

Although 80% of cyber breaches is due to hackers exploiting human weak points cybersecurity remains in the remote care of the IT department. You believe that HR has equal responsibility to ensure every staff is fully engaged in threat awareness and monitoring.

You understand the growing need for cybersecurity to be a shared responsibility by all staff and not only the specialists in the IT department acting on breaches which could easily be avoided by staff.

Importantly, you have no idea of any hiddden threats that already exist in your organizations system!

Some of your staff unwittingly do any of the below exposing your organization to hackers?

1. Use public wifi e.g.in cafes, hotels, airports
2. Download cracks to save on paid software
3. Use simple passwords like Company2022
4. Use company emails in social media
5. Agree to T&C of apps without checking with IT Security
6. Forwarding emails to unauthorized addresses (gmail accounts etc) .. and more?

If you tick any of the above then the Vigilante Human Firewall Program may right for you now.

The skills & knowledge participants gain

The Human Firewall Program is an on-going cyber hardening practice by your staff. It is the only cyber hardening program that is human behaviour focused in self-awareness, criminal psychology and hands-on participation of threat monitoring of live data. What each staff will harden up:

Knowing oneself

- Who am I?
- How am I vulanerable to hackers?

Living inside the hacker's mind

- Persuasion techniques hackers use on me
- Cheap tricks to exploit my weaknesses

Real Immersion into the cyber space

- The virtual world of Internet, Deepnet, Darknet
- What is the Internet & how does it work?
- IPs, DNS servers, Routers gamified
- TOR and the Darknet
- Bash Bunnies, Rubber Duckies, Lan Turtles
- OSINT & my digital footprint

Hacking and Penetration Demo

- Kali Linux
- Metasploit
- Hashcat
- Burp Suite
- Web Vulnerabilities and Security

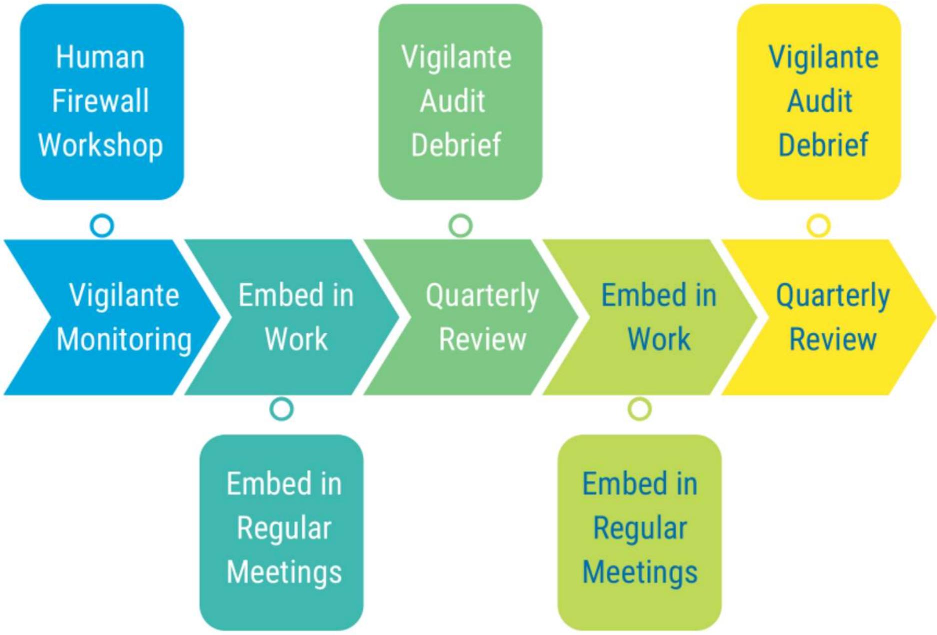
Becoming a practicing Cyber Vigilante

- How to use the Vigilante Dashboard
- What are indicators of Compromise (IOCs)
- Basic Threat detection & triaging
- Understanding Cyber Threat Audit Reports

On-going Role

- Embedding cyber montoring into team meetings
- Keeping updated by Quarterly Threat Reviews

Building on real-time engagement


Human Firewall Workshop

Vigilante Audit Debrief

Vigilante Audit Debrief

Vigilante Monitoring

Embed in Work

Quarterly Review

Embed in Work

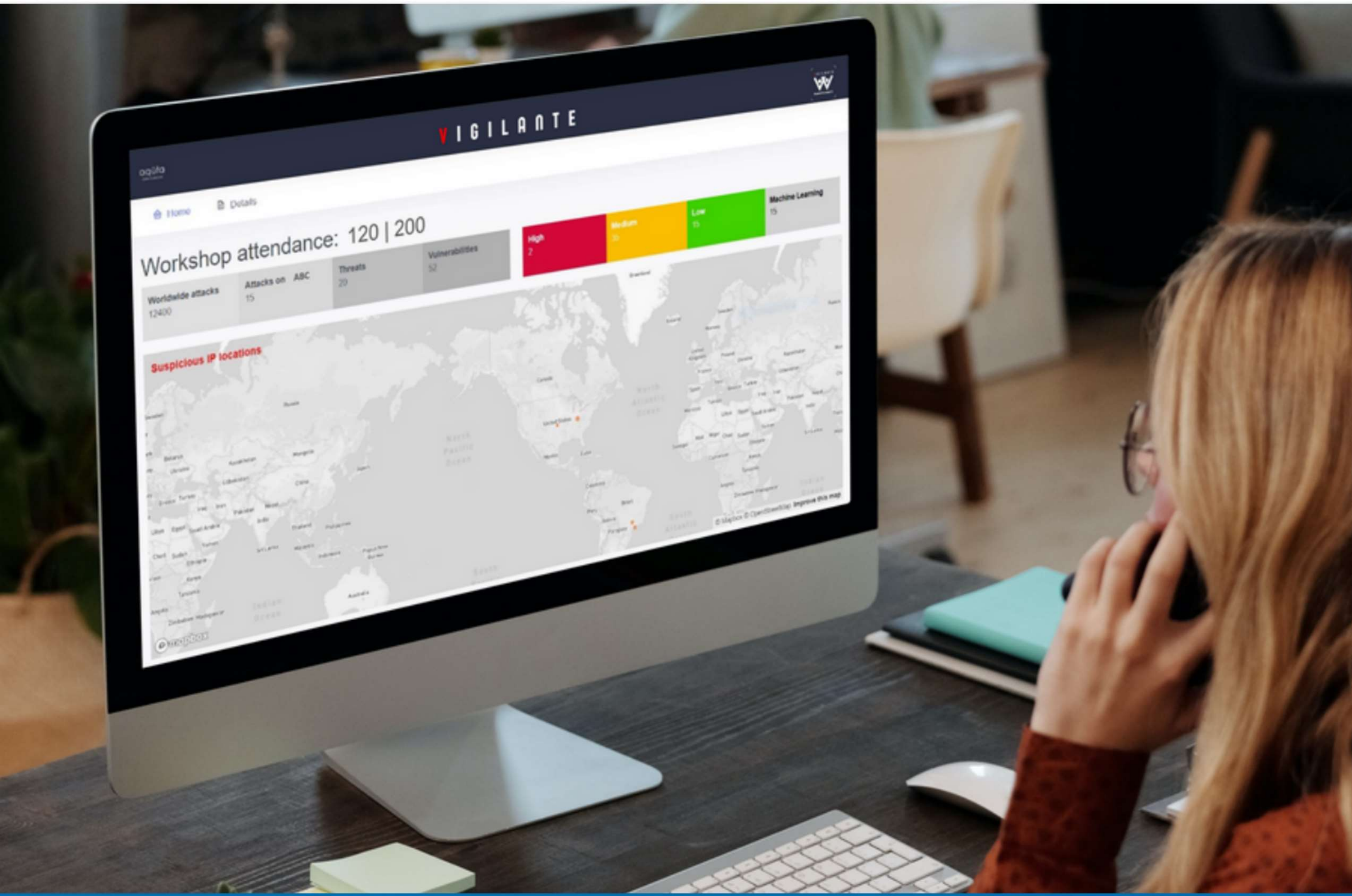
Quarterly Review

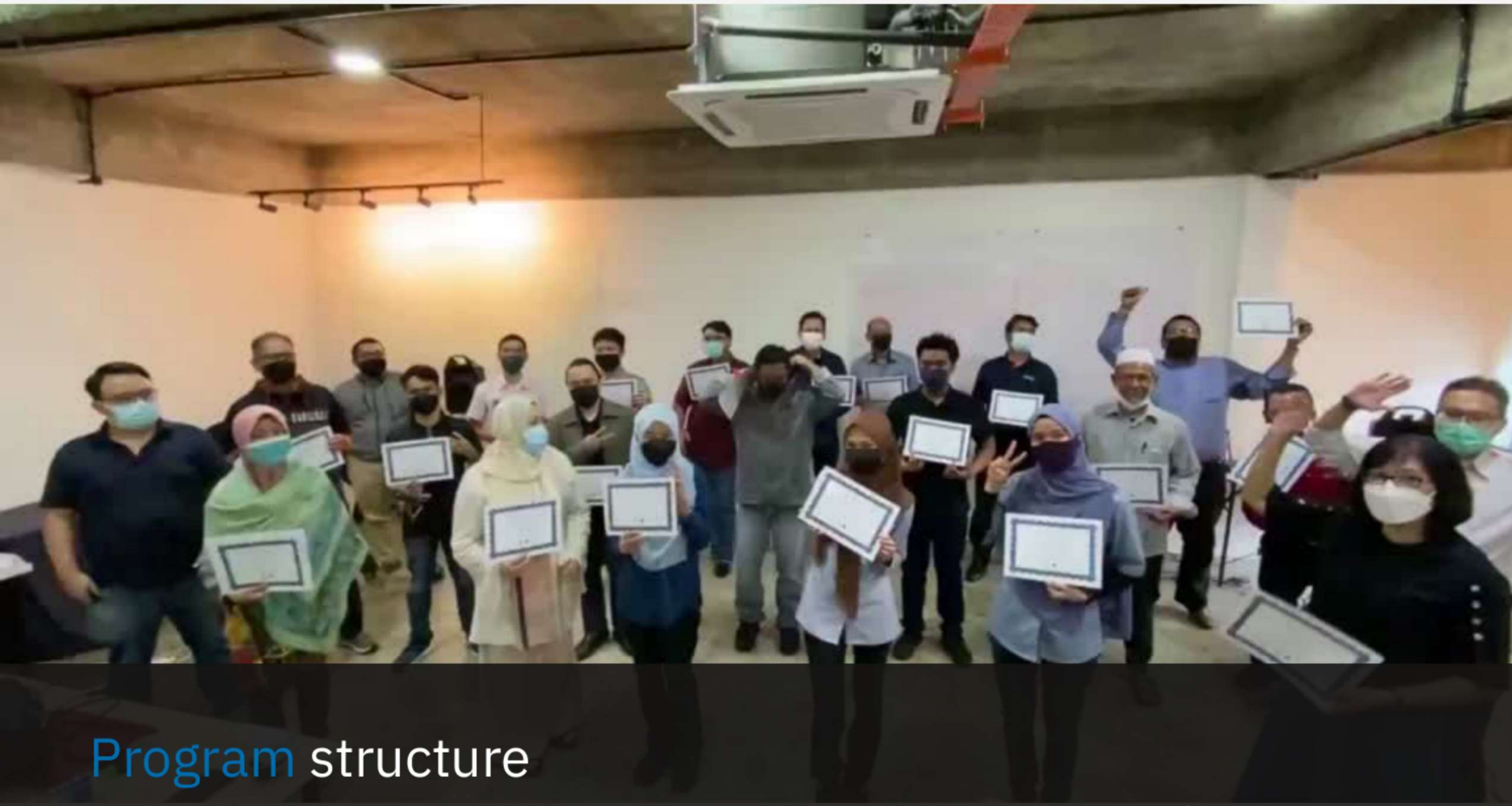
Embed in Regular Meetings

Embed in Regular Meetings

All Employees who are users of o365 are prepared for cyber safe behaviour and awareness through participating in the Human Firewall workshop.

Cyber safe behaviour and practice is embedded into the organizational culture by engaging staff in threat monitoring and triaging using the Vigilante Dashboard routinely.





Program structure

The Aquta Human Firewall Program is designed to engage all employees in adopting cyber safe mindset and behaviour. This is achieved through a unique combination of cyber-safe awareness workshops and hands-on real-time threat monitoring skills on our Vigilante Dashboard. The Vigilante System simplifies complex threat monitoring and triaging for general non-IT staff to do and create their human firewall.

Human Firewall Workshop

The Human Firewall Workshop transforms employees across the organization to be Cyber Vigilantes. This unique program truly engages the employees to become the Human Firewall for the organization. Your organization's Vigilante Threat Monitoring Dashboard is introduced and workshopped making the whole experience real.

Threat Training in Real Time

Post attendance of the Human Firewall Workshops our Cyber Safe Instructors will assist participants to begin monitoring threats in real-time and how to interprete and triage cases based on the Vigilante Dashboard signals. Our instructors will train the trainer (team leaders) on conducting weekly reviews with their teams.

Live Threat Monitoring

Team leaders embed 5-10min cyber threat reviews in their weekly meetings based on live monitoring using the Vigilante Dashboard. This is to engage every employee in adopting cyber-safe awareness and behaviours. Our instructors will conduct quarterly Audit Reporting & Analyis Debriefing and cyber threat updates via Teams.

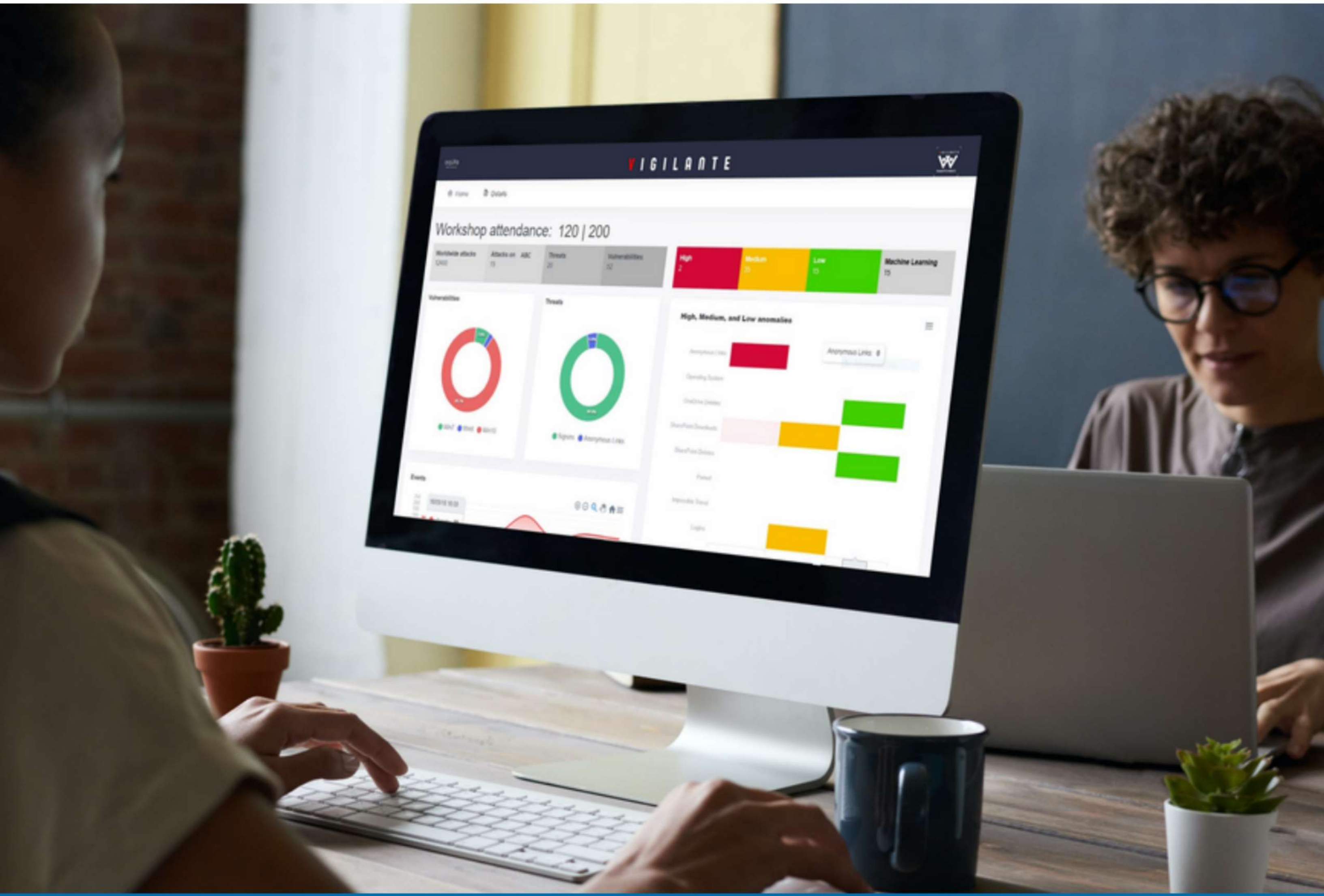
The Vigilante Threat Monitoring System

Vigilante is an automated solution that acts as an intelligent protective digital bubble, encasing your organisation’s o365 cloud I.T. attack surfaces. It provides real-time visualisation of critical indicators of compromise,of both internal and external sources, whilst leaving operations unaffected by its presence.
Vigilante's unique approach simplifies complex threat monitoring for the non-IT employee through its user friendly dashboard. This engages each employee to play an organizational role in building a human firewall against hackers. Implementation of the software is simple and installation is carried out remotely through an authorization link.

Vigilante is compromised of 2 parts:

Front End: This is a live dashboard of Indicators of Compromise (IOC's) designed for non-IT staff monitoring.

Back End: All the complexity of threat detection and prediction is handled by our proprietary software and simplified into visualization of IOC's on the dashboard. It also contains internal (o365 audit log) and external (darknet) data, AI algorithms, and behaviour modeling for threat hunting and prediction by our Cyber Analysts.



Vigilante Dashboard IOC's

Indicators	Description	What it is for
IOC 1 Worldwide Attacks (on country)	Asia accounts for 73% of the world's shortage of cybersecurtiy workforce resulting in attracting 80% of hacker focus. The indicator shows the number of attacks on the country of the client in real-time. This gives an appreciation of the enormity of the challenges organizations face every moment.	- Shows employees the enormity of the exposure to real-time hacking attacks every business faces in the country. It emphasises to all staff that cyber-safe knowledge and behaviour is not only crucial for your business but also for themselves whenever they go online
IOC 2 Attacks on Company	These are attempts to login to your business emails by bots and hackers. Over 50% of businesses in ASEAN faces an average of 5,000 attacks every day. Has selection of real-time and 90-day historical data visualization.	- Research shows 60% of alerts are not being investigated due to the sheer number of attacks per day. This indicator classifies atttacks into High, Medium and Low allowing the Team leaders/members and HR to help look out for malicious activities.
IOC 3 Operating Systems	Vigilante identifies operating systems and devices used for logins.	- End-of-support operating systems used for logins puts the business at high risk of malware compromise. Non white list logins using Linux OS are also likely threats.
IOC 4 Pwned	Alerts employee that email credentials have been breached.	- The employee can get further details of the breach at "have i being pwned" site and update their passwords if necessary.
IOC 5 Impossible Travel	Indicator will flag location logins within a 24 hr period of an employee that are physically impossible to do. Such as, numerous logins from different locations hours apart by travel in a day.	- It is highly likely that the employees login credentials have been compromised and password need to be reset. It will also alert IT security to perform a threat analysis to confirm there was no compromise on the business.
IOC 6 Malicious Downloads	Indicator will show harmful downloads of software by an employee.	- Hackers frequently inject malware into software downloads.

Vigilante Dashboard IOC's

Indicators	Description	What it is for
IOC 7 Mailbox Forwarding	Hackers frequently place mailbox forwarding rules to external accounts after a breach to exfiltrate data. During invoice fraud they may forward email correspondence into a hidden folder to avoid detection by a compromised employee (e.g. a CFO).	• Highlights suspicious mailbox forwarding of an employee's email account to unidentifed email accounts. Employee to confirm it is a malicous activity and triages this breach to the IT threat hunting team or vendor. Forwaring by the employee to unauthorised accounts will be discontinued by IT Security.
IOC 8 Account logins	The indicator shows all logins and attempted logins by employee account. It also alert account takeover (ATO) attacks such as brute-forcing, credential stuffing and password spraying. Suspicious logins are automatically checked for malicious IP's and alerted.	• Employee can confirm any suspicious login alerts from the date and time the event happened. Triage to IT Security as needed.
IOC 9 SharePoint Downloads	Alert employee of abnormal volume of file download activity from their accounts by suspicous IP.	• An employee's compromised acccount may result in files being exfiltrated by a hacker or an ex-employee who obtained account access of a current employee's login credentials. The employee can confirm and block.
IOC 10 SharePoint & OneDrive Deletes	Alert employee of unusual deletion of files from their accounts.	• The employee can confirm and report if it is a breach to mitigate further loss of data by the organization.
IOC 11 Anonymous Links	Indicator flags anonymous links and file sharing links from suspicious IP's.	• It is highly likely that the employees login credentials have been compromised. Upon confirmation by employee of a likely breach, IT security will begin investigation and prevention.
IOC 12 Anomalous Behaviour	Vigilante AI alerts the employee on any activities that seem out of the normal behaviours.	• The employee can confirm and report if the activities are not attributable to them to stop potential breach compromises

And More ..

We are here to help

As your staff move up the learning curve, you're likely to have questions around some of the more advanced concepts available in Vigilante such as threat hunting and prediction. We're here to help, through in-person and/or virtual office hours, as well as a dedicated MS Teams channel where you can get assistance from trainers, support staff and your team leaders. In addition, we provide:

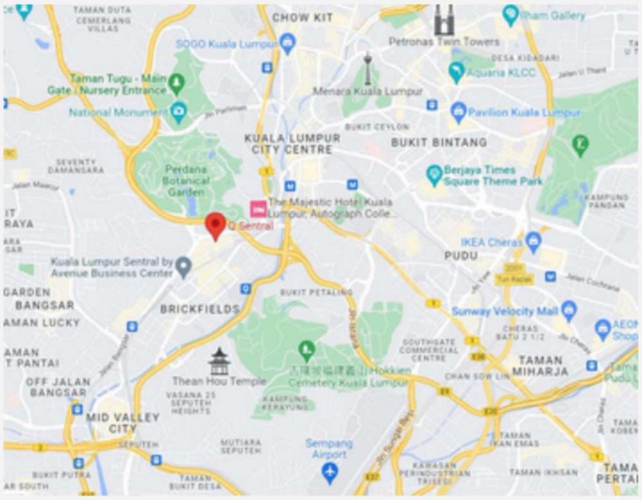
- Webinars on cybersecurity trends
- Refresher workshops
- Cyber-safe behaviour coaching
- Ethical hacking workshops
- Online digital awareness courses
- Threat hunting & prediction by our Cyber Analysts
- Board training - Digital Assurance
- Crises Management Simulation Stress Tests

aqüta

data sciences

Contact Us for a Demo

Aquta Data Sciences (M) Sdn Bhd
Suite 16-15, Lvl 16, Q Sentral
KL Sentral, Kuala Lumpur
Malaysia
+603 2776 3988
support@aquta.io



VIGILANTE
HumanFirewall