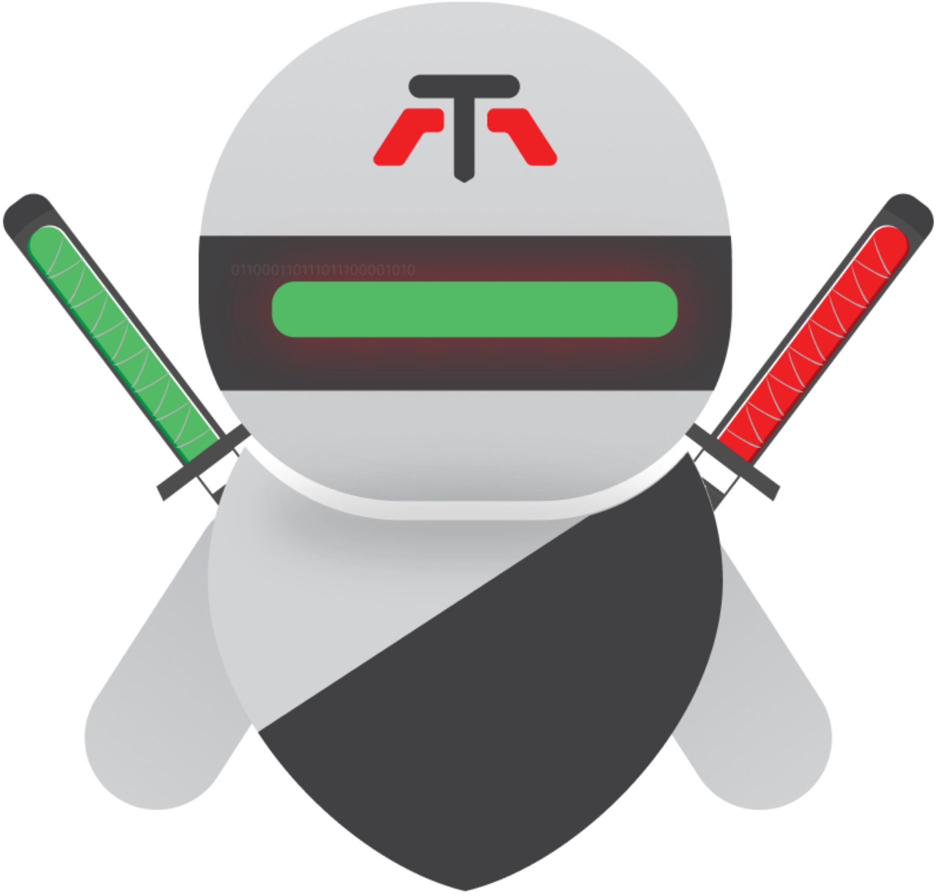
TekMonks



CYBERWARRIOR

Detect. Defend. Defeat.

DATA SHEET

Detect, Defend, Defeat

CyberWarrior is an AI expert security system for cyber defense designed to combat smart attacks. CyberWarrior AI Expert system, behaves like a human, using existing knowledge to detect the danger, then defend, and then defeat, using modern algorithms to protect the Enterprise.

AI Expert System
Built upon the BDI algorithm, we developed CyberWarrior, because the only way to combat AI cyberattacks is AI itself.

Integration
Integrates seamlessly with our other products as well as products from other organizations, such as Cisco's firewall.

Actively Fights Back
The only AI-powered active cyber defense solution capable of defeating the most intense cyberattacks.

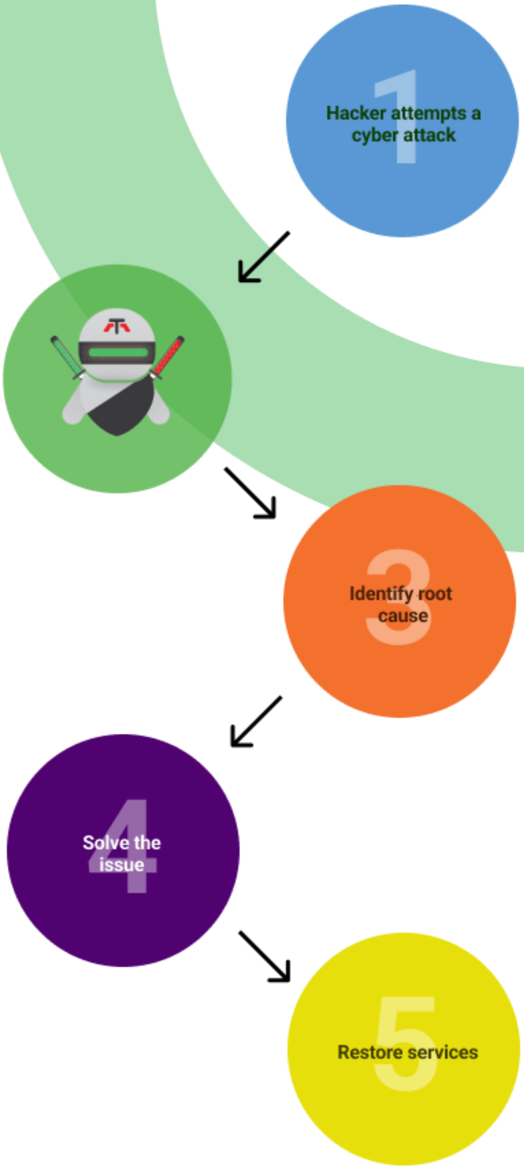
- AI Expert System - Developed with an expert knowledge base to detect and counter attacks.
- Monitors Servers, Applications and Firewall, and acts on attacks.
- Unified Solution - Detects and Prevents various cyberattacks in one unified solution.
- Realtime Attack Resolution - Monitors, analyses, and resolves attacks 24/7.
- Agentless - Monitors logs and remote connectivity to resolve attacks.
- Optional Dashboard: Provides information on network health and CyberWarrior Actions.

“The only way to combat Artificial Intelligence is AI itself. Hence, TekMonks conceived CyberWarrior – an AI expert system developed to counter cyberattacks”

Efficient Active Defense

Built to behave like a human, the strength and unique capability of CyberWarrior is its efficiency of carrying out commands to detect anomalies and prevent attacks. Instead of losing time by separating both monitoring and decision making between software and experts, Cyberwarrior boasts both aspects in parallel.

- Collects information
- Analyzes new threats
- Takes instantaneous course of action

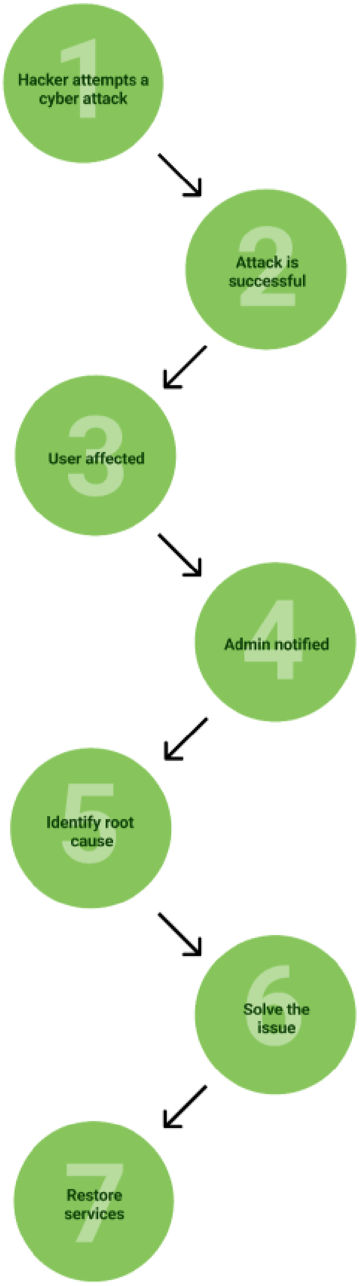


1 Hacker attempts a cyber attack

3 Identify root cause

4 Solve the issue

5 Restore services



1 Hacker attempts a cyber attack

2 Attack is successful

3 User affected

4 Admin notified

5 Identify root cause

6 Solve the issue

7 Restore services

"It resolves attacks in seconds if not milliseconds whenever a current threat arises"

Admin Solution Time	CyberWarrior solution time
Potentially, minutes to hours upon attack may occur. Valuable data may have been compromised.	Milliseconds to Seconds only

Detect. Defend. Defeat

Features and Benefits

Expert System

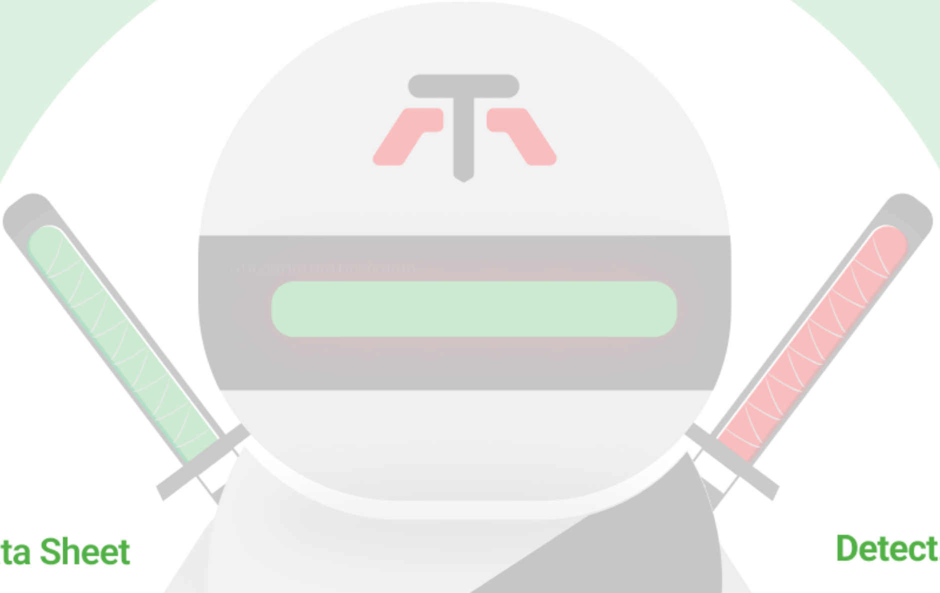
- Solves issues utilizing the “Belief, Desire, Intention” (BDI) algorithm as it checks its beliefs and executes plans in parallel.

- Knows what components and systems are dependent and related to each other in the network using complex dependency graphs.

- Gives priority to each element of the network when it starts to execute its plan.

  Solutions ranges from

  - Large (millions) IP blocks to Prevent a DDoS attack
  - Stopping application layer attacks
  - Removing application threats
  - Dropping paths from a router to prevent IP traffic from attacker to attacked machine.
  - Reconfiguring the network filters on the box
  - Reprogramming the application (e.g., http server) to drop malevolent traffic and even take down a server if all else fails.
  - Ensuring the Malicious Hacker never wins, and your data will not be stolen.



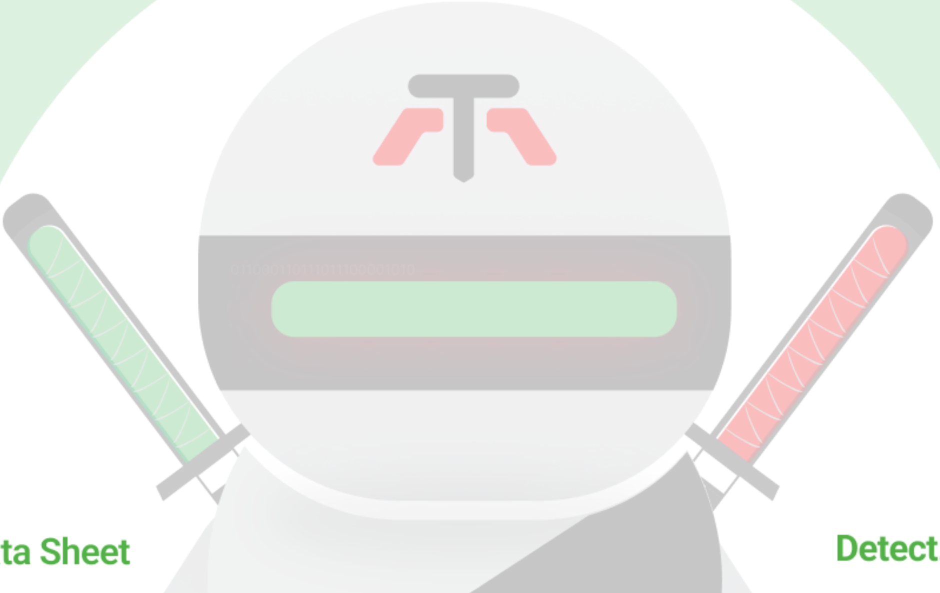
Features and Benefits

Monitors servers, desktop, and firewall

- Security information and security event management.
- Turns pre-existing components within the network into their smart devices.
- Strengthens all layers of the network.
- Add levels of speed and consistency to network security monitoring and defense.
- Does not rest as it continuously provides instructions to the network devices to repel attacks in real-time.

One Solution

- Software installed in a virtual appliance within the network.
- Architecture involves individual components that act on their own.
- Designed to be flexible and able to accommodate any additional specific or special component that the client needs.



Features and Benefits

Real time attack resolution

- The most important way that Cyberwarrior can monitor information is through Cyberwarrior components.
- Components can perform remote monitoring and resolution at a very high frequency.
- Incremental log checks - only need to watch what happened in the previous interval leading to a very fast check and response time.

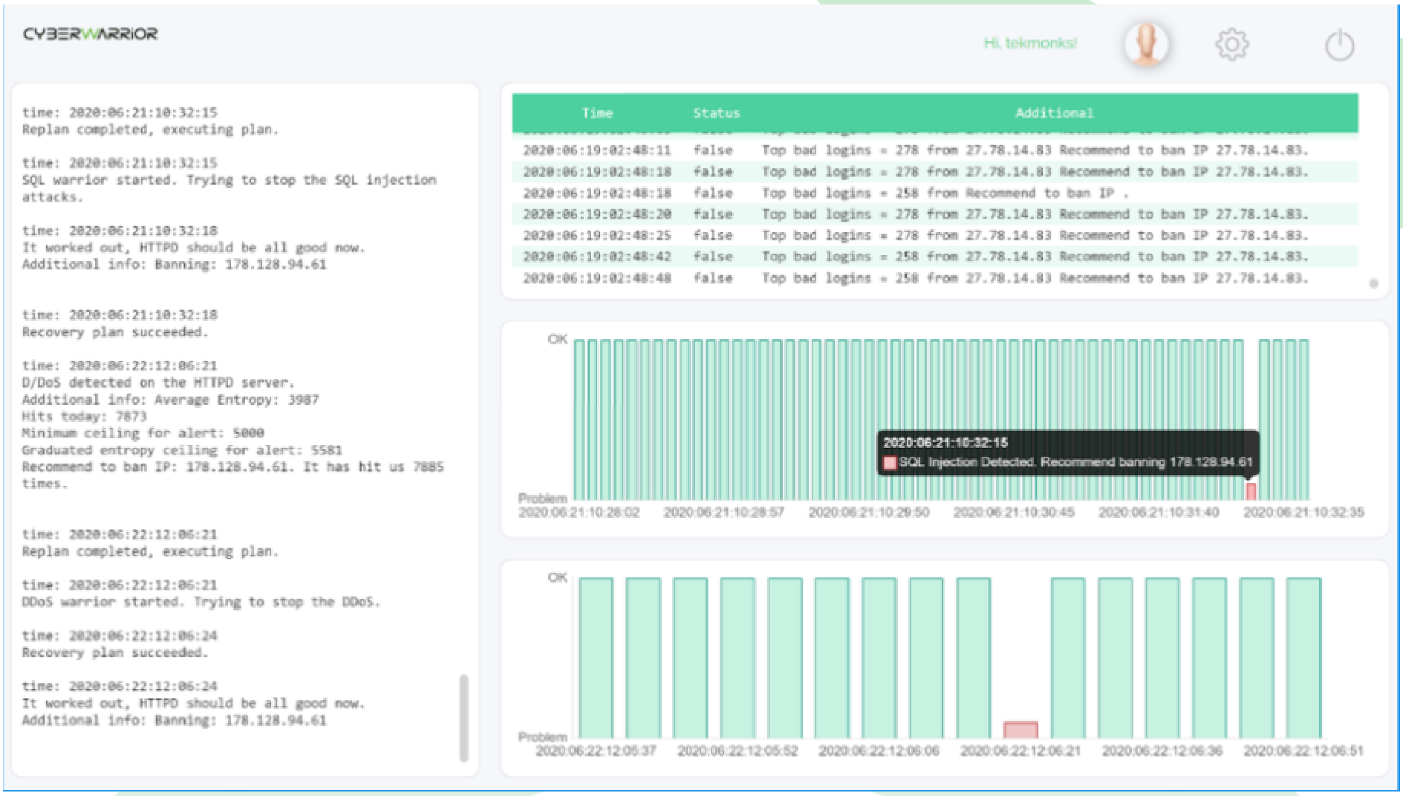
Agentless Monitoring

- Most modern systems ship with capability to send monitoring and alert data remotely.
- For network devices, either SSH or remote admin via APIs is used.
- Capable to automatically discover, monitor, and administer system security:
  - Uses the capabilities built into the products that are being managed.
  - Just as any human system administrator would.
  - No agent installation is required.

Features and Benefits

Optional dashboard

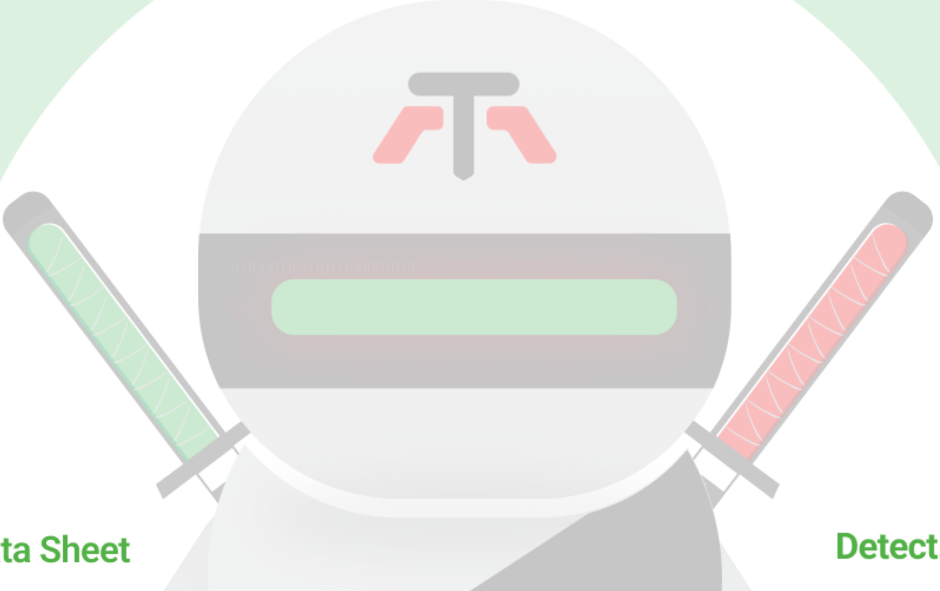
- Notifies incoming attacks based on priority of severity, and information on actions CyberWarrior has taken to stop them.
- Provides the administrator with clear information on network health.
- Fix problems after detection in mere seconds and informs the admin.
- Can be integrated into pre-existing dashboards hence, it is optional.



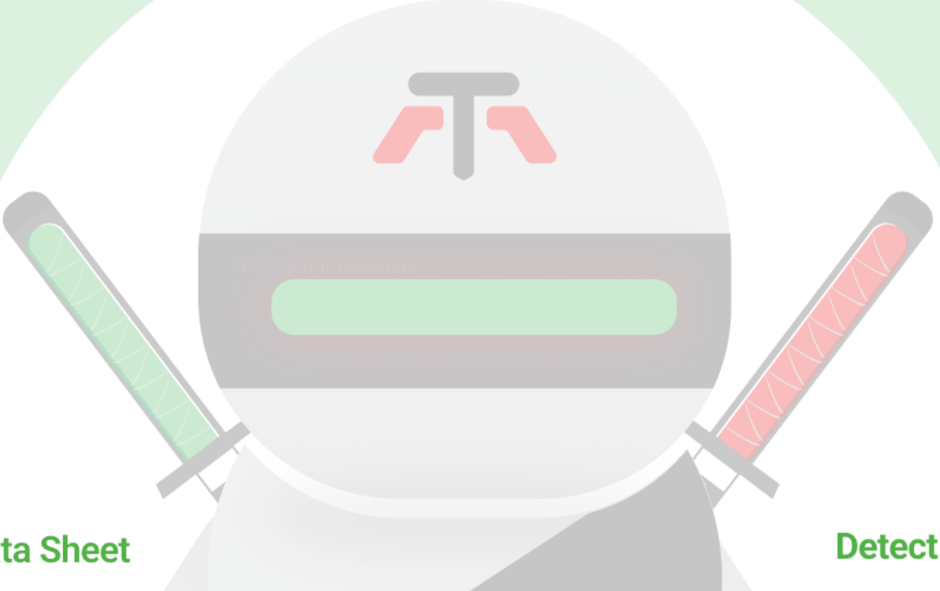
```
time: 2020:06:21:10:32:15
Replan completed, executing plan.

time: 2020:06:21:10:32:15
SQL warrior started. Trying to stop the SQL injection
attacks.

time: 2020:06:21:10:32:18
It worked out, HTTPD should be all good now.
Additional info: Banning: 178.128.94.61


time: 2020:06:21:10:32:18
Recovery plan succeeded.

time: 2020:06:22:12:06:21
D/DoS detected on the HTTPD server.
Additional info: Average Entropy: 3987
Hits today: 7873
Minimum ceiling for alert: 5000
Graduated entropy ceiling for alert: 5581
Recommend to ban IP: 178.128.94.61. It has hit us 7885
times.


time: 2020:06:22:12:06:21
Replan completed, executing plan.

time: 2020:06:22:12:06:21
DDoS warrior started. Trying to stop the DDoS.

time: 2020:06:22:12:06:24
Recovery plan succeeded.

time: 2020:06:22:12:06:24
It worked out, HTTPD should be all good now.
Additional info: Banning: 178.128.94.61
```

Time	Status	Additional
2020:06:19:02:48:11	false	Top bad logins = 278 from 27.78.14.83 Recommend to ban IP 27.78.14.83.
2020:06:19:02:48:18	false	Top bad logins = 278 from 27.78.14.83 Recommend to ban IP 27.78.14.83.
2020:06:19:02:48:18	false	Top bad logins = 258 from Recommend to ban IP .
2020:06:19:02:48:20	false	Top bad logins = 278 from 27.78.14.83 Recommend to ban IP 27.78.14.83.
2020:06:19:02:48:25	false	Top bad logins = 278 from 27.78.14.83 Recommend to ban IP 27.78.14.83.
2020:06:19:02:48:42	false	Top bad logins = 258 from 27.78.14.83 Recommend to ban IP 27.78.14.83.
2020:06:19:02:48:48	false	Top bad logins = 258 from 27.78.14.83 Recommend to ban IP 27.78.14.83.

2020:06:21:10:32:15
🟥 SQL Injection Detected. Recommend banning 178.128.94.61



Specifications	
Supported OS	Linux, Redhat Enterprise and Ubuntu
Compliance	ISO 27001
System Requirements	4 cores and 12 GB RAM and 250 GB Disk
Product Model	SaaS Software
Installation Methodology	Delivered as Saas or Prebuilt VMs
Integration	Windows, Linux, Network via SNMP
Support	[Click for Support Documentation]

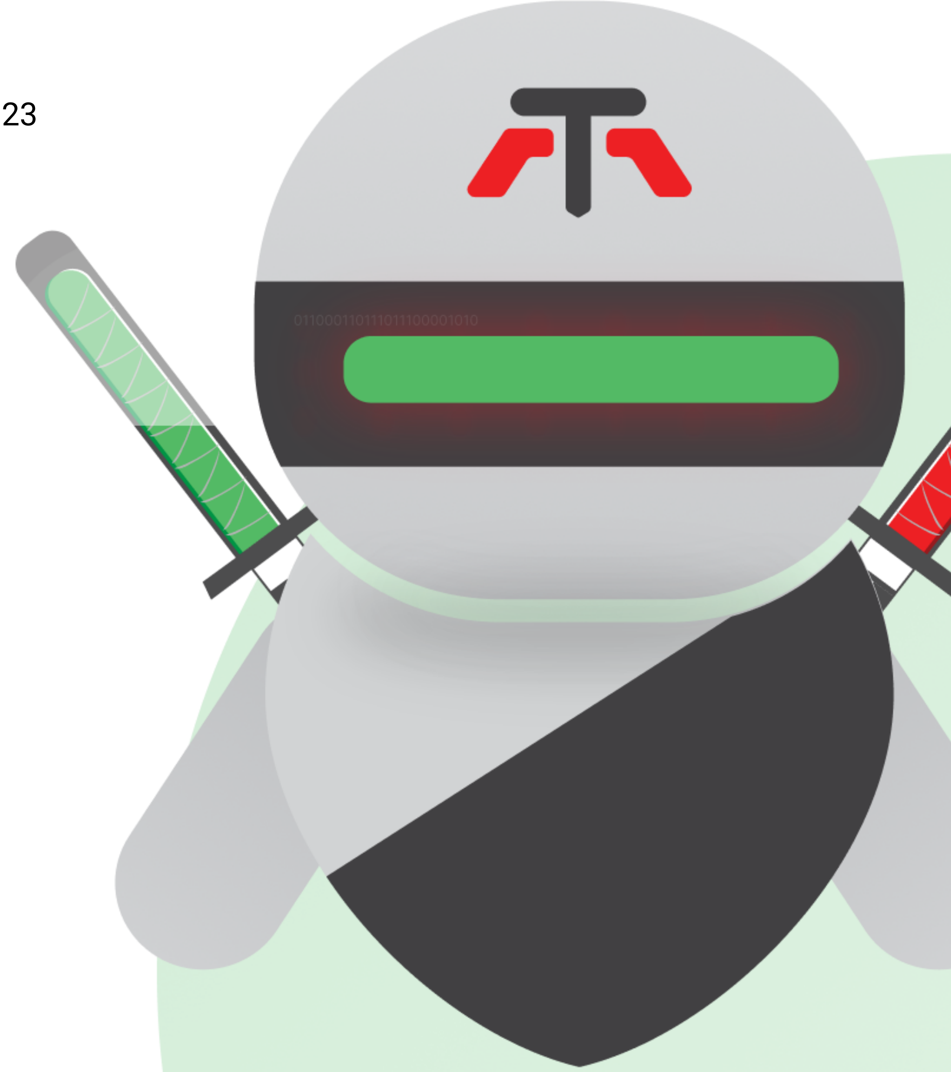


Produced/Printed in the UK 02/2023

IMPORTANT PRIVACY INFORMATION: If you would like to request access to or correction of your details, or if you would prefer you or your organization not to receive further information on Tekmonks products and services please contact us at: privacy@tekmonks.com

Tekmonks Ltd.

Kemp House, 152 City Road
London. EC1V 2NX. UK.



Tekmonks