

The SecQube AI-driven Cyber Security Portal. Powered by Harvey.

Achieve more. Spend less.

Revolutionising SOC performance on Microsoft's Sentinel SIEM Platform.



At SecQube, Data Security is designed in.

Our AI-powered SOC assistant, Harvey, will speed up triaging and support remediation whatever the size of your SOC. What is more, we deploy into your jurisdiction – whether a public or private Azure instance, ensuring your Data Residency is respected and maintained.



Immediate ROI

Savings will massively outweigh the cost of the portal, meaning return on investment begins on Day 1.



Ongoing Compliance

Data residency is crucial in the security world. We don't move or store your data – it stays in your Sentinel instance.



Improved customer service

We reduce triage & resolution times down from minutes to seconds. Service Providers respond to customer issues instantly.



Public or Private cloud

As a SaaS solution we can deploy in any Azure instance. If you want your own version, we can deploy to your private instance – only access then is to deploy updates.



Addressing the global skills shortage in Cyber Security

As the threat landscape grows continuously, so too does the demand for skilled security Analysts. Combine that with growing demand for SOC services built on the Microsoft Sentinel SIEM platform and you have a perfect storm.



Primary challenge

Enterprises and service providers (MSPs, MSSPs & others) compete for a limited workforce supply which, itself, is also constantly moving and evolving, resulting in retention, training, cost and quality issues.



Ideal solution

Reduce that dependency on the skills shortage through automation. Our AI-powered solution, 'Harvey', will perform the work of multiple junior Analysts in a fraction of the time and at a fraction of the cost.



Desired outcomes

Reduced costs, increased speed, improved accuracy and greater consistency / efficiency. Harvey handles ~80% of your activity in a fraction of the time. Analysts work on more interesting issues – improving job satisfaction and reducing churn.

SecQube. Delivering value. Immediately.

Addressing the cyber security skills shortage through our AI-powered SOC assistant, Harvey. Driving value for all Microsoft Sentinel users through reduced costs and risk combined with enhanced speed, accuracy and effectiveness



Reduced Costs

Triage large volumes of Alerts without the need for a large team of Analysts.



Reduced Risk

Avoid manual errors through automation leveraging AI to support or even replace Analysts when triaging.



Reduced Diagnostic Time

In today's security world, time is critical. We reduce triage & resolution times down from minutes to seconds.



Ease of Setup

A SaaS solution, deployable in minutes and providing value immediately thereafter, connecting via lighthouse.

Who should use SecQube's Cyber Security Portal?

Anyone needing a SOC with a combination of people and tooling will benefit from using the SecQube Security Portal. Ideally already on Microsoft Sentinel. If not, we can still help.

Everyone looking to reduce SOC costs and improve accuracy & efficiency will benefit from using the Portal.



The SecQube Security Portal for Enterprises

Typically run their own SOC. Looking to reduce costs and improve efficiency. Maybe have outsourced their SOC service to a 3rd party and just want to keep an eye on their effectiveness...

The SecQube Security Portal for MSPs

Already provide IT services to customers and want to add SOC security solutions to protect them further but don't have the in-house capability and don't want to partner externally, e.g. with an MSSP.

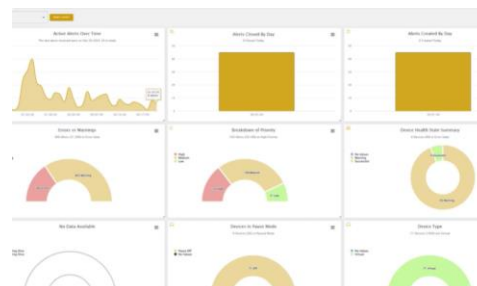
The SecQube Security Portal for MSSPs

Already provide SOC services and want to scale the business. Maybe want to switch to (or add) Sentinel as a solution. Face the skills shortage daily including rising people costs.

Portal Highlights

A 100% Azure Application

Azure



Live Responsive Dashboard

Monitor resource utilisation, identify bottlenecks, and optimize operations for a seamless user experience and enhanced output through our user-tailorable Dashboard.

Harvey: Our conversational AI bot

Powered by Microsoft OpenAI, Harvey constantly analyses cyberthreats. It instantly identifies potential risks and then provides customised action points for analysts to follow, ensuring proactive defence at all times.



Alert ID	Alert Name	Severity	Category	Source	Target	Status	Assigned To	Created At	Updated At	Resolved At	Resolution Time
SEC-2023-001	Malware Detected	High	Malware	Windows Defender	10.10.10.10	Open	John Doe	2023-01-01 10:00	2023-01-01 10:05		5 min
SEC-2023-002	Phishing Attempt	Medium	Phishing	Outlook	10.10.10.10	Open	Jane Smith	2023-01-01 11:00	2023-01-01 11:05		5 min
SEC-2023-003	Brute Force Attack	High	Brute Force	SSH	10.10.10.10	Open	John Doe	2023-01-01 12:00	2023-01-01 12:05		5 min
SEC-2023-004	SQL Injection Attempt	High	SQL Injection	Web Server	10.10.10.10	Open	Jane Smith	2023-01-01 13:00	2023-01-01 13:05		5 min
SEC-2023-005	Denial of Service Attack	High	Denial of Service	Web Server	10.10.10.10	Open	John Doe	2023-01-01 14:00	2023-01-01 14:05		5 min

Be on top of Incidents

Harvey provides your analysts with alerts that have already been analysed, saving critical triage time & with clear steps to resolve each alert. The severity of alerts ensures that the most important incidents are addressed first.

Centralise your Microsoft Sentinel



Self-Service, quick & easy setup



Multi-Tenant



Deployable to any region



Global Reach

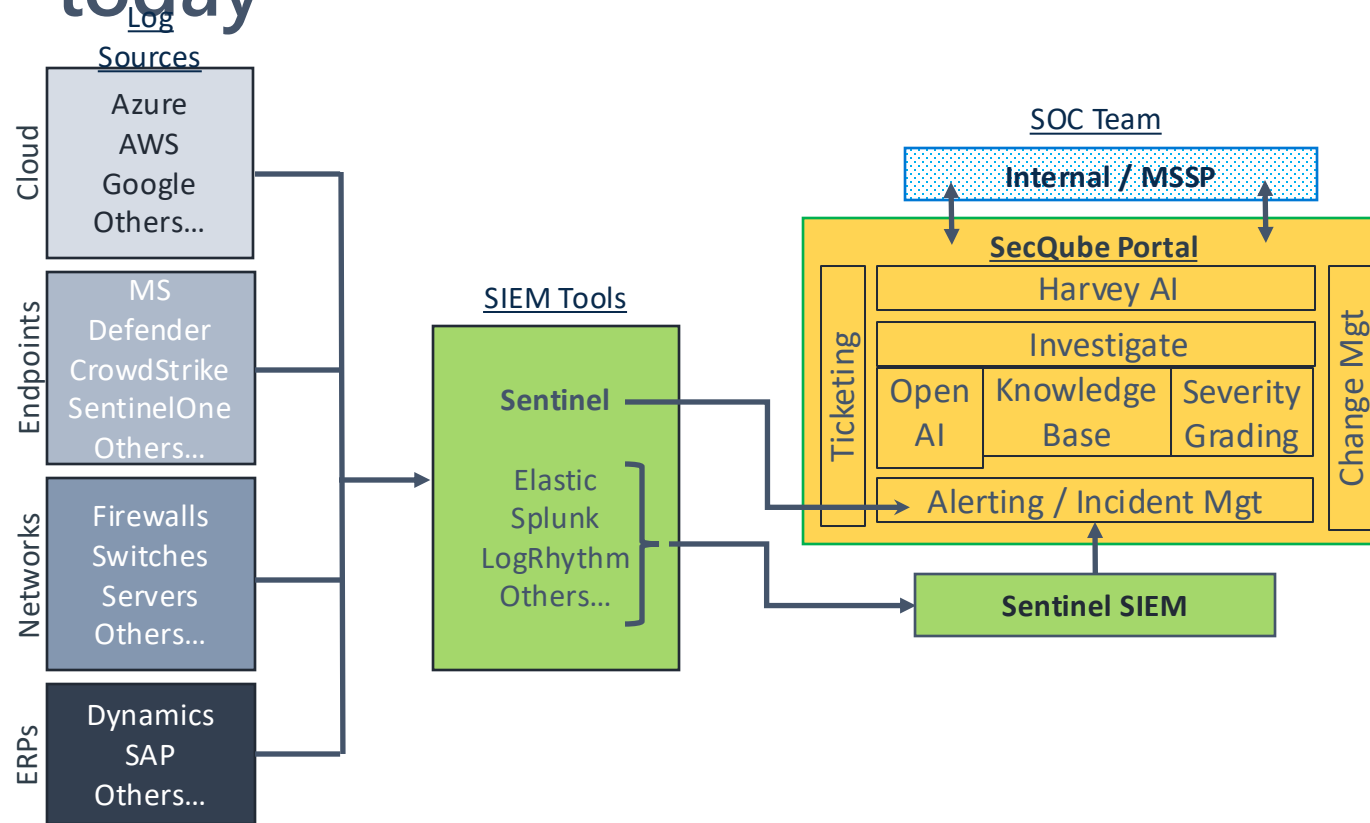


AI Knowledge Base



24/7 AI Support

Use Case Explainer – in the market today



Don't know Sentinel?

No problem! The SecQube Portal sits above Microsoft Sentinel. You don't need to know Sentinel as our portal becomes your alert and incident management interface.



Not heard of Sentinel?

No problem! Microsoft Sentinel is a top SIEM platform according to the leading independent analysts Gartner, IDC and Forrester.



Using other non-Microsoft tools?

No Problem! Sentinel has the ability to collect logs and data from a range of sources including various EDRs, XDRs, MDRs, ERPs, Cloud Services and network devices.

Why Microsoft and what value does SecQube offer?

Microsoft Sentinel is seen by leading independent Analysts as a 'Leader' in the SIEM category and, as such, is creating ever-increasing demand for the solution. This, in turn, exacerbates the challenge caused by a lack of skilled labour.



Skills Shortage

More Sentinel customers means more skilled resources needed. SecQube's Portal bridges that gap, supporting Analysts of all skills levels to be more effective and efficient.



Adoption

More and more businesses are looking to rapidly deploy and benefit from using Sentinel.



Retention / Churn

As businesses sign up in volume they need to see value rapidly and consistently to ensure they will continue to use Sentinel.

As a result SecQube have.....

- ✓ Been invited to join the Microsoft ISV program as a native Azure App developer (and have now done so)
- ✓ Received technology funding support from Microsoft to support platform costs
- ✓ Signed up to the MS Azure App Marketplace, making the portal available to all Microsoft partners
- ✓ Signed up to the Microsoft Co-sell program, enabling MS sales teams to sell our solution





In Summary, everyone running a SOC service needs to reduce costs, increase security and speed up detection and resolution times while improving accuracy and consistency.

SecQube's Portal helps deliver these outcomes.