About QMasters

- QMasters, founded in 2015, provides **best of breed** security technology with professional **delivery** services.
- QMasters is a market-leader in end-to-end cyber solution delivery services - meaning we provide our customers with consulting, best practices and with the best-suited solution to meet their requirements.
- Innovation is the key principle representing our top-tier standard of cybersecurity, servicing over 300 leading medium and enterprise-sized customers from all different fields - national defense forces, financial institutes, medical institutes, insurance companies, manufacturing companies, governments and more.
- QMasters has established itself as a leading information security company both locally in Israel and globally.

- Our commitment to quality and service excellence is why our customers view us as value added partners and trust us with their network and data security.
- Our in-depth knowledge, expertise and experience enables us to be trusted cybersecurity advisors and meet all our customer cybersecurity needs.

- In 2019 as a vision of being able to provide customed software Qmasters had developed its own development services who provide Agile software development services for a variety of security requirements such as Security Orchestration, Automation and Response (SOAR) technologies, security API addons to support current tools and extend functionalities. Extensive experience building unique security applications for Splunk ,IBM QRadar™, Palo Alto Networks™, SentinelOne™, Radiflow™, IntSights™, Watchguard™ and more.

Expert Cyber Security Consulting

Custom Development of Security capabilities & Automation

Customized Cyber Integration

Technology Implementation

MCSS – Managed Cyber Security Services

StrongHold MCSS – Managed Cyber Security Services

StrongHold Services are made to protect organizations of all sizes against data breaches, to reduce attacker dwell-time and to negate the impact of any malicious activity on your business operations.

providing a complete portfolio of threat detection and response capabilities that organizations can take advantage of to protect their on-premises, hybrid, and cloud environments and reduce and mitigate their risk exposure.
To make this happen, we have made it our business to collect the right data at the right time – with no compromises.

24 x 7 x 365 monitoring, detection, response, and remediation services are provided in response to alerts that are ingested and correlated from the organizations' Endpoint Detection and Response (EDR) / Endpoint Protection Platform (EPP), SIEM, or XDR platforms. Appropriate response capabilities are taken on behalf of the client based on previously agreed upon response plans as part of onboarding process .

Key metrics that are often reported to the board, such as mean time to detect and mean time to respond, are easier to report on as StrongHold offers service-level agreements (SLAs) with one hour or less time to detect (TTD) and real time live customer portal.

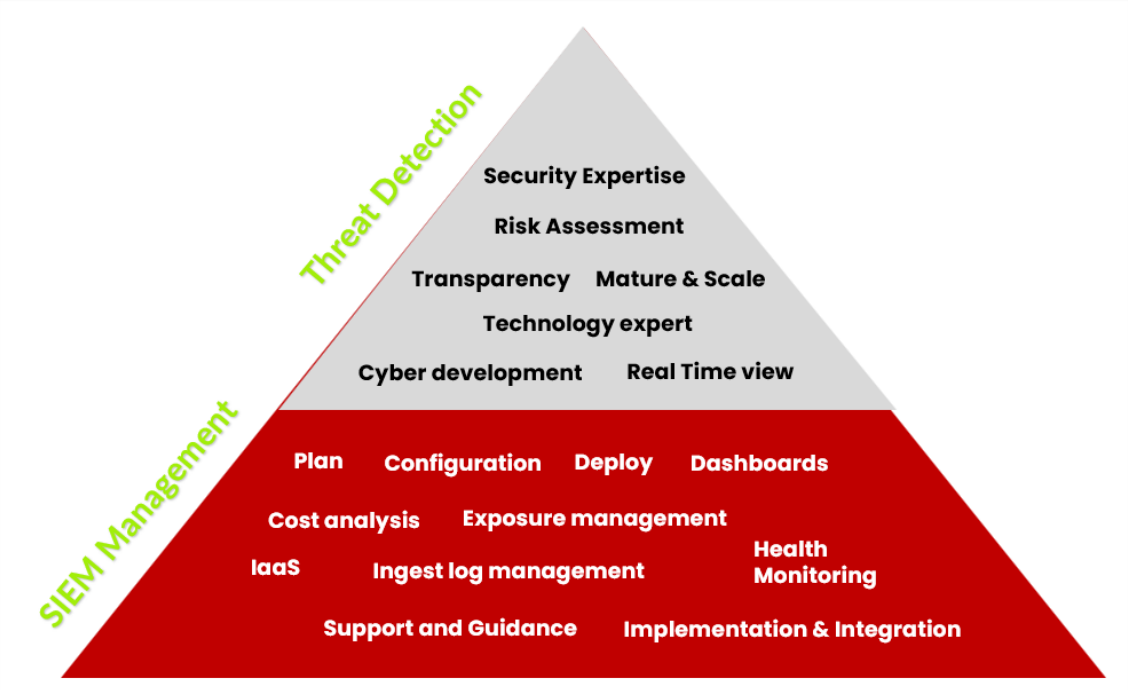
StrongHold MCSS takes all of the alerts generated — regardless of data source — and quickly identifies and resolves favorable outcome. Using our customer portal and MobileSOC both SOC and Customer can make sure all relevant alert are being investigated and responded to by expert security analysts.

During this whole process, customers can obtain 100% visibility to every action and every data point that is looked at by the StrongHold team. MOBILESOC — a mobile application — which goes beyond notification and ticketing functions to allow users to perform response actions or communicate with the SOC to take the appropriate response action.

StrongHold blue team defenders are leveraging the knowledge and wisdom of the Detection Engineering and Cyber Threat Intelligence services & technologies to gain insights into the tactics, techniques, and procedures (TTPs) that the cyber adversary is likely to use during an attack. The Cyber Research Unit also manages, maintains, and curates out-of-the-box detections and IOCs .

CONCLUSION

Using a risk-based approach, Stronghold provides comprehensive services backed by industry-leading methodologies, processes and technologies.
By assisting in advancing organizational cybersecurity capabilities over time (based on risk profile), we empower organizations to balance cost and risk mitigation to achieve desired maturity level. We are passionate about our work, committed to organization success and proud to provide you with results backed by our transparency, expertise and Service Level Agreements (SLAs) and enhanced by the our MOBILESOC approach .



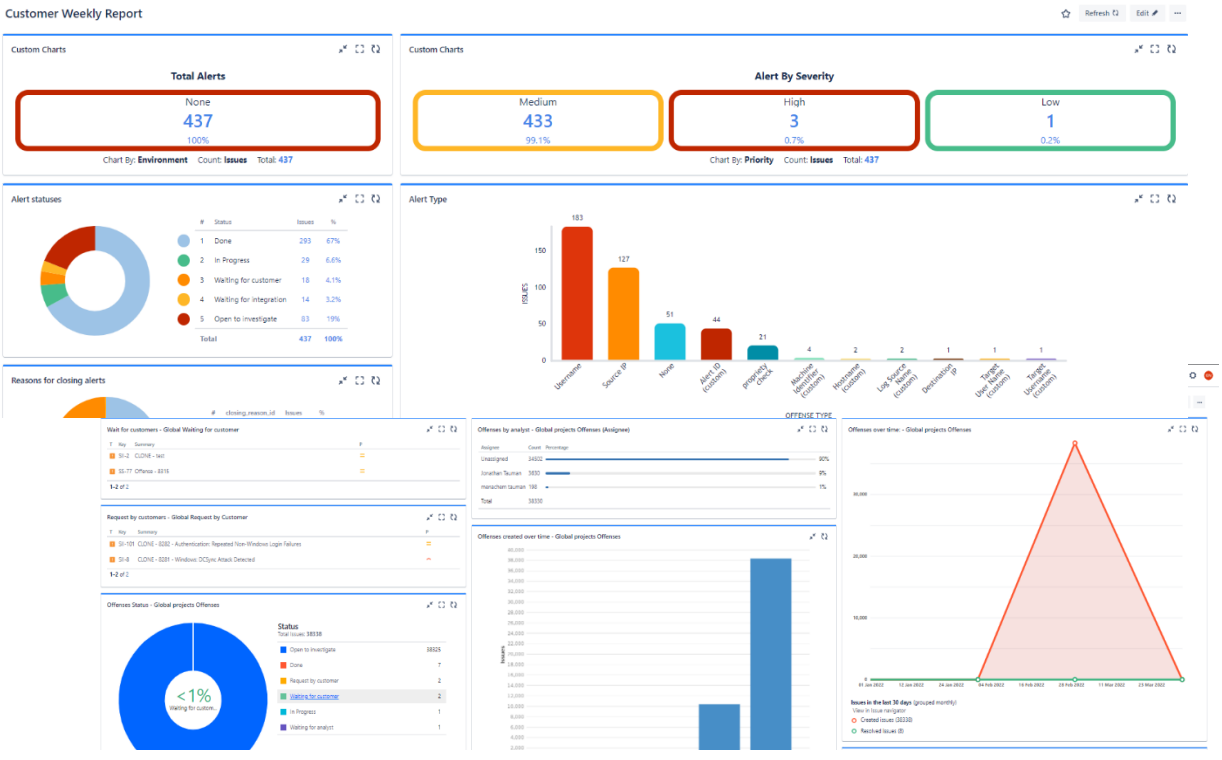
Why QMasters ?

Managed Cyber Security Services

- A new approach for providing managed security services
- Customer portal management – full visibility at all time!
- Quick and efficient onboarding process including complete gap analysis and critical framework mapping
- Connectors with Splunk and Qradar

Customer Portal & Mobile SOC

- Enables real-time overview of security status
- Intuitive and easy to use
- Full visibility of every alert including details of each investigation
- Complete view of all tickets, current status, ability to reassign any task as needed at any time
- Quick response from anywhere



StrongHold MCSS – Managed SIEM value added services

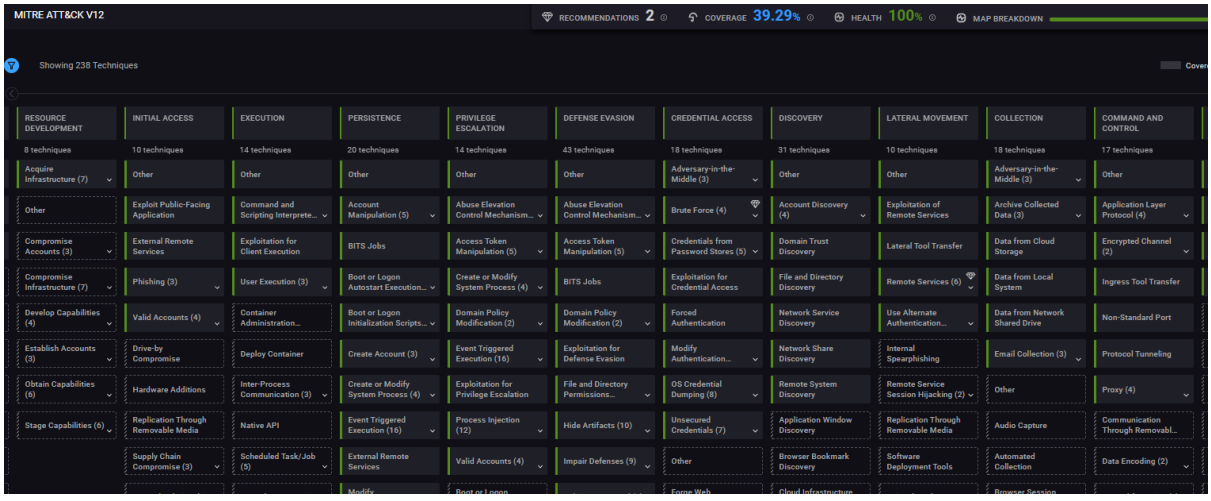
StrongHold Managed SIEM meets and exceeds all the requirements and best practices for Managed SIEM Services and includes a dedicated team of security experts to help you derive maximum value from your SIEM investment. Our experts identifies and continuously analyzes log sources to ensure they are of the highest fidelity, reducing your risk acceptance and optimizing your breach protection.

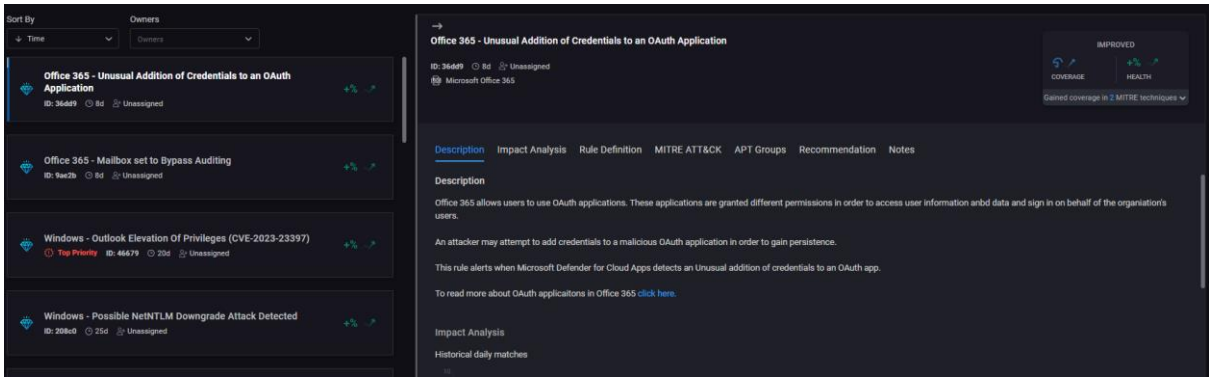
Configuration and customization: Improve team productivity and increase efficiency with custom development for dashboards, reports and log sources to support your security, risk, compliance and audit use cases.

Quarterly service review: Maximize your total cost of ownership and increase your security outcomes with visibility into how your SIEM is performing.

Health monitoring: Keep your SIEM running at optimal capacity with log source performance, availability and capacity monitoring to identify potential issues with log ingestion.

Risk reduction reviews: Keep up with new threats and compliance requirements by ensuring that your data is being properly ingested. Our experts help prevent misconfigurations by analyzing the potential impact of adding log sources and detection content on your coverage under the industry-standard MITRE ATT&CK® Framework.





We Work with the Best

StrongHold services integrate with leading security technologies to detect every alert, resolve every alert and respond to breaches

Tailor-Made Managed Services – Pick Your Package:

- SIEM as a Service – we provide you with the SIEM platform only.
- Bring your SIEM solution – you own the SIEM platform, we manage and monitor.
- SOAR as a Service – Orchestration and Automation.
- Data Protection as a Service – DLP solution as an external service.
- EDR & MDR – Full MDR & EDR solutions, expert service or full management.
- On-demand sandbox – via API or portal
- Cyber intelligence – Exposure / brand protection / Darkweb / IOC services.
- Automated penetration testing – network / web / lateral movement etc
- CPSM (Cloud Posture Security Management) as a Service
- Incident Response team - crisis management
- Vulnerability Management – Detection & response – internal and External .

What Differs QMasters from the Competition?

- We provied mixed SOC & MDR services tailored to organizational security operation's unique needs , detect the right threats and help make faster, more accurate decisions on which response actions to take.
- Our solution is **based on a fixed amount of EPS without a specific limit**. We want to connect as many critical and relevant data-sources in order to get a holistic and complete state-view of your cyber security posture.
- We don't do **fines** , we **do not charge** for excess EPS!
- Unlike other companies , we do **not charge for additional APM** (Alerts Per Month) the alerts are our responsibility and if the number of events grows, it is in our best interest to continuously improve and tweak the system.
- **12-month contract term**: we know the service level we provide our customers with will keep them satisfied, and that why they will choose to renew the contract.
- We offer an initial response team, a specialized IR team to help with understanding of a cyber incident and prepare a an active mitigation response.
- Our client portal allows you full visibility of every incident and every investigation, at any time from any place via real-time web and mobile access (MobileSOC).
- Our comprehensive, all-inclusive onboarding process provides you with a full gap analysis and clear understanding of your current security-state.
- Constant improvement – the more we learn about your organization, the more accurate we make the rules in the system, the better we can adjust them and tailor-make them to fit your exact use-cases.
- We help you define your critical framework (business impact) , and monitor your most valuable business processes and services ("crown jewels").

Partial List of Qmasters MCSS Customers Already Enjoying StronghHold Services:

We Work with all industries providing Managed Security and cyber technologies :

- Financial industry , Fintech companies
- Health sector , Cloud and IT infrastructure ,
- Energy Industry , Real state companies , manufacturers
- Cloud technology company , hi-tech and low tech companies
- Consumer retailer , retailer