

Managed Detection and Response (MDR)

Because you need more than just Endpoint Security

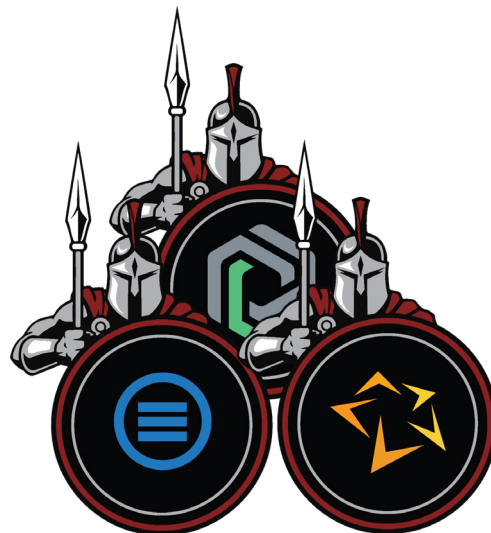
Managed Detection and Response (MDR) is a comprehensive service that includes 24/7 threat monitoring, threat hunting, and detection response. We leverage a combination of hand-picked and vetted technologies deployed at the host using advanced analytics, threat intelligence, and human expertise to deliver sophisticated and thorough incident investigation and response. We also offer incident validation and remote response services such as threat containment as needed.

“

Solutions Granted's SOC detected strange activity on a client's server at 2 a.m. We were able to contain the breach at an early stage. I sleep better at night knowing Solutions Granted is watching over my clients' networks.

— Dan Browne, CEO DMB networks.

”



MANAGED SERVICE

On-demand support from experienced threat hunters, malware analysts, and incident responders

FORENSIC STATE ANALYSIS

Independent deep host inspection across every node on your network - physical and virtual

INCIDENT RESPONSE

Identify patient zero with Activity Trace and respond to threats with automated timelines and triage

EASY IMPLEMENTATION

From configuration to deployment and response, our experts will guide you and support your need

Find out what a true partnership with a security provider is like

with an MDR solution that is not only built for MSP's - but priced for MSP's with a true consumption model

To learn just how good partnering with Solutions Granted can be, contact us today!

sales@solutionsgranted.com – 703.565-2395

AGENT-BASED DEPLOYMENT

Lightweight agents are installed on the endpoints to provide persistent, continuous access. This enables real-time monitoring and collection capabilities.

ANOMALY-BASED DETECTION

Utilizing heuristics, statistical analysis, and machine learning, ARR highlights atypical events or features of an artifact/file which aids in detection of advanced and zero-day threats.

Key Features:

- Real-time Process and Script Monitoring
- Continuous Live Memory Analysis
- Powershell and other "Living-off-the-Land" adversary techniques
- Abuse of legitimate administrative tools
- Lateral movement
- User Account Misuse

BEHAVIOR-BASED DETECTION

The behavioral analytics engine identifies suspicious behaviors of legitimate processes and events and maps them to known attacker tactics, techniques and procedures (TTPs) as described by the MITRE ATT&CK framework. We concentrate defenses against the Top 20 most commonly observed ATT&CK techniques that are also achievable to monitor. These allow us to be more effective and catch adversaries actions more often.

FORENSIC STATE ANALYSIS

The agent has the ability to collect and analyze live forensic data from your endpoints, including from both volatile and non-volatile memory. This capability enables proactive inspection of thousands of hosts for current and historical compromise as well as aiding in the root cause identification of detected attacks. This analysis can be conducted agentlessly or via the ARR agent.

Forensic Collection and Analysis includes:

- Active Processes & Scripts
- Triage of Live Volatile Memory
- Registry and Autoruns (Run Keys, Startup Folders, Lnk Files, Schtasks/Cron, etc.)
- Execution Artifacts (shimcache, amcache, prefetch)
- OS Subversion (API hooks, disabled controls)
- Local Event Log Triage
- Privileged Accounts
- Installed Applications & Vulnerabilities
- Active Host Connections & Listeners

CONTINUOUS ENDPOINT MONITORING, RESPONSE AND FORENSICS

ARR's advanced threat hunting and monitoring adds another layer of security focused on identifying key behaviors observed during and following an attack. In addition, automated forensic analysis enables our analysts to proactively verify integrity of endpoints or quickly determine root cause once a breach is found. MDR simplifies and accelerates the identification, investigation and response to sophisticated cyber attacks.



703.565.2395

Toll Free: 800.619.8481

solutionsgranted.com

sales@solutionsgranted.com

POWERED BY:

