DGS ATT&CK Detection&Response powered by Microsoft

A Smart roadmap to a comprehensive Cyber Security efficiency

Security leaders are seeking event management solutions with capabilities that support early attack detection, investigation and response.

Minimize attack remediation leveraging on Detection & Response Technique according to MITRE ATT&CK Framework exploiting the Microsoft Azure Security Platform capabilities. The solution boost the synergy of MS Defender ATP, Sentinel and Azure Security Center and Azure Network Watcher to enable an Attack Automated Response.

Why customers use solution

This at-a-glance box

- Limited visibility of incident
- Long time between attack & recovery
- Complex operations activities

Attack Visibility

- Kill chain comprehension
- Alert triage
- ATT&CK Mapping

gain visibility for faster and more effective response

Fast Containment

- Fast Response
- Lateral movement containment
- Data exfiltration containment

minimizing mean time to detect

Automated Remediation

- Automated check & act
- Boost SOC capabilities
- Reduce incident cost

reduce and accelerate recovery time