DGS ATT&CK Detection&Response powered by Microsoft

DGS

Industry Situation – the evolving market of Cybersecurity tools and the advent of standardization best practices

Challenges

- Attacks are becoming more and more complex
- SecOps teams are overwhelmed by volume of alerts and can't respond quickly enough
- Single vertical technologies are unable to cope: they need integrations & orchestration

- Significant shortage of IT Security resources[1]
- Security Orchestration & Automation is the top investment priority[1]
- Mean Time to Detect is becoming the primary KPI[1]

[1]source: Gartner Mkt Guide Y19; Wipro Report Y20

Ideal Solution

- Early visibility of security events coupled with efficient tools to reduce false positives and accelerate remediation with minimum effort
- Optimal solution should provide synergy between a standard attack framework (MITRE) and EDR, SIEM and SOAR tools

- This approach would help to improve processes and provide customers with further clarity and context to the threats they face.

Desired Outcomes

Customers, even those who have already some of the Microsoft components, could provide a better Cybersecurity response with the help of an integration layer and a best practice framework (i.e. MITRE ATT&CK). This would give them the full benefit of Microsoft leading-edge security portfolio.

- Full visibility of attack kill-chain
- Data enrichment enable better detection and simplify threat hunting and remediation
- Operational and technological synergies granted by a Microsoft full-stack solution

DGS ATT&CK Detection&Response powered by Microsoft

Increase the response capabilities leveraging visibility and performance through Microsoft solutions aligned on MITRE ATT&CK framework

EDR in ATT&CK

EDR value visibility & performance

- EDR behavior in MITRE ATT&CK framework context
- EDR capabilities mapping to ATT&CK framework

SIEM in ATT&CK

SIEM value visibility & performance

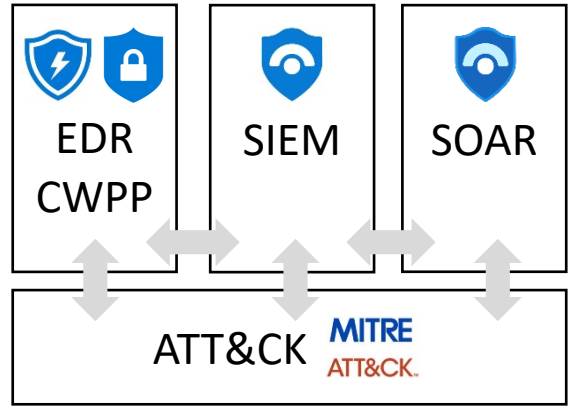
- SIEM added value in MITRE ATT&CK framework context
- SIEM capabilities mapping to ATT&CK framework

SOAR in ATT&CK

SOAR value visibility & performance

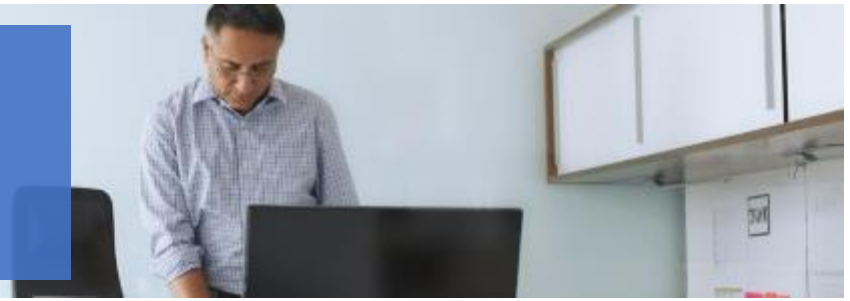
- SOAR remediation in MITRE ATT&CK framework context
- SOAR capabilities mapping to ATT&CK framework

Logical Architecture



Integration, orchestration and standardization are the key values for an efficient approach to a Cyber Security protection

DGS ATT&CK Detection&Response powered by Microsoft



Minimize attack remediation leveraging on Detection & Response Technique according to MITRE ATT&CK Framework exploiting the Microsoft Azure Security Platform capabilities.

Solution Alignment

Cyber Security expertise and market leader solution in APT

- From reactive to proactive approach
- Maximize results improving visibility and protection

Cyber Security expertise and Microsoft SIEM

- Data aggregation
- Correlation and enrichment capabilities powered by AI

Cyber Security expertise and Microsoft SOAR

- Effective orchestration and automation
- Faster incident response and remediation