SAPPHIRE™

Deception Services

Service Description

Classification: Public

Registered office as shown, registered in England no. 3183935, VAT reg no. 664874881.
Sapphire is the trading name of Sapphire Technologies Ltd.

Contents

Proprietary Notice

Deception Services

Gathering threat intelligence before cyber-attacks and being able to take preventative action is vital for mature organisations that have the ability to consume or act on this data. Typically, these are organisations that have a SOC/MXDR service. Deception technology is a key next step for customers who have embraced MXDR/SOC technology. They can not only provide proactive detection capabilities but also tripwires and intelligence on attacker activity as well as providing a possible delay into the attackers plans against your critical systems.

Deception is a service provided by Sapphire and delivered by our UK-based Security Operations Centre (SOC). It uses Honey nets and decoys. Decoys are used to detect/find an attacker and can be used internally or externally i.e. internal networks or on the internet. Active deception allows you to lead the adversaries away from your crown jewels by deploying a deceptive campaign within minutes.

While the adversary is engaged, with the decoys, deception technology allows you to mount an effective response, while adversaries focus on targets that have no operational value for you.

This service provides a deception service deployment with potentially several decoys deployed with a secure manner and configured to send alerts whenever unusual traffic is detected. As soon as any traffic arrives at the decoy, the service raises an alert, the traffic is captured and logged and made available for analysis via a web browser.

The challenge with decoy is that it attracts criminal activity and so needs to be hardened and monitored to avoid being a route of compromise into the organisation or SOC monitoring service.

Alerts can be managed or sent to the customer via email or via integrations with the customer's SIEM or Sapphire MXDR/SOC service.

The baseline service is designed to be 'drop in' – quick and easy to deploy and fully managed with minimal intervention. It is also configured to not cause an impact on existing customer networks.

The service can be extended to include more complex and integrated decoys as well as canary tokens and cloud-based services.

Why is it needed?

- Assume breach approach - i.e. this service aligns with assume breach mentality.
- Detect internal threats and attackers in the network.
- Assume they will get in or have already breeched your network.

- Ability to catch adversaries inside the network is key and helps to defend against insider threat.
- Augments customers SIEMs such as Sentinel and Exabeam, and augments SOC operations and fully integrates into SIEMs.

This deception service is designed to be used within the customers network (on premise, data centre or cloud).

Service Features

- Provided as a managed decoy environment for on prem/data centre and/or cloud.
- Enriched integration with MS Sentinel and Exabeam
- Alerts can also go to a customer's SIEM.
- Standalone service or an additional service to our SOC service.

Service Benefits

- Detects both internal threats and external attackers in the network.
- Designed to be used within customer's network.
- Benefit of SOC threat hunting experience.
- Assumed breach approach = zero trust.

Service Options

- Cloud-based deception (deployed as VM)
- Canary tokens / decoys deployment and consultation (on prem/data centre, cloud, web, email, db, device, user, etc.)
- More advanced decoy configuration/deployment to make them more authentic and detect wider range of attacks.
- High availability service options.

Sapphire's Certifications and Associations