Singtel Business

Product Brochure
Managed Deception & Detection Service

Delivering adaptive defence with Singtel's Managed Deception & Detection Service

Managed Deception & Detection Service introduces game-changing adaptive defence capabilities for heightened threat detection and accelerated incident response, enabling enterprises to address the challenges presented by advanced persistent threats and other attacks in an increasingly dynamic and volatile threat landscape.

Singtel

Managed Deception & Detection Service

Enterprise Challenges

One of the main cyber security challenges facing businesses today is that of advanced persistent threats (APTs) where an unauthorised user gains access to the enterprise network, avoids detection and stealthily carries out nefarious activities such as the exfiltration of corporate data.

Given the covert nature of APTs, businesses are often hampered by poor visibility when they attempt to address these threats - whether they originate from outside the organisation or are perpetrated from within. The lack of visibility and knowledge about these threats leads to delayed or inaccurate threat mitigation, and also makes it difficult to automate incident handling and response.

To address these cyber security challenges, enterprises have started moving away from prevention-only approaches to cyber security to focus more on detection and response. According to research firm Gartner, enhancing detection and response capabilities will be a key priority for security buyers through 2020.

One way to achieve heightened detection and response is through the use of deception technology. Deception leverages the knowledge that defenders have of their organisation's environment, its key assets and where they are kept, in order to mislead and get an upper hand over attackers.

The deception technology market sector is poised to grow at a CAGR of about **10.3%** to reach **US$2.59 billion** by 2025[1].

Gartner Says **Detection and Response** is **Top Security Priority** for Organisations in 2017[2].

Attivo Networks® Proves **Deception Fools Attackers**[3]

Managed Deception & Detection Service

Singtel's Managed Deception & Detection Service uses deception technology to create a '**hall of mirrors**' environment which lures, confuses and misdirects attackers into revealing themselves. This is done through the use of decoys in both the **information technology (IT) and operational technology (OT) network environments**.

The Managed Deception & Detection Service is part of the Singtel Managed Security Services (MSS) suite which consists of **Threat Monitoring, Managed Security Device and Threat Mitigation**. When the decoys are compromised, they immediately send out a strong indicator of threat presence which is picked up by the Threat Monitoring Platform, reducing time-to-detection and eliminating false positives.

The threats are directed to a controlled sinkhole environment where they are "detonated", allowing security experts from Singtel's Advanced Security Operations Centre (ASOC) to conduct a **forensic analysis** of the attacks. At the same time, automated incident handling is triggered according to pre-defined playbook rules to provide rapid threat mitigation. The Managed Deception & Detection Service thus elevates managed security services by introducing game-changing adaptive defence capabilities for heightened detection and accelerated incident response.

The service is available as an on-premise model with deception-based adaptive defence, orchestration and response automation customised for each customer.

[1] Global Deception Technology market report, 2016
[2] Gartner Newsroom, 2017
[3] Nasdaq GlobeNewswire, 2017

Features

Deception and real-time detection

- Network and endpoint decoys are deployed dynamically to misdirect attackers.
- The entire network is turned into a trap using deception breadcrumbs to lure attackers.
- Decoys and traps enable detection of threats as they move laterally across the network.
- Provides assessment of vulnerable attack paths that an attacker takes to reach important business assets.

Monitoring and management

- Provides 24/7 real-time monitoring with intelligence capabilities.
- Security Information and Event Management Platform (SIEM) delivers visibility into the network and potential threats via a user-friendly customer portal.
- Supports enterprises in security policy and configuration management.
- Includes performance, availability and fault management with on-site hardware replacement.

Mitigation and response

- Takes a multi-vector approach for threat correlation and investigation, enabling prioritised escalation and more informed recommendations for mitigation.
- Incident response can be automated using a playbook customised to any security environment.
- Relevant playbook policy rules and indicators of compromise (IOC) can be configured to detect, block and hunt threats depending on the capabilities of the enterprise's managed security device.

Reporting and analysis

- Collates logs across diverse platforms for a holistic view of the networking and threats landscape.
- Provides incident reporting with context analysis for improved decision making.
- Includes a wide range of reports from ad-hoc fault incident reports to monthly summaries for performance and availability as well as top security events.

Benefits

Increases effectiveness in threat detection

- Zero false positives because real users will never wander into the fake environment.
- Threats such as ransomware and advanced persistent threats can be detected in real time by tracking lateral movement of malware across the network.

Reduces incident response time

- Accelerated incident handling with automation of response.
- Response is orchestrated via a playbook tailored to the customer's environment.
- Sinkhole environment prevents attackers from propagating throughout the network.

Adapts dynamically to a volatile threat environment

- Through intelligent traffic monitoring, the service is able to detect what hackers are targeting at.
- Decoys are generated to obfuscate the environment and confuse the attackers.
- Induces attackers to expend resources targeting fake assets and reveal themselves in the process.

Improves visibility

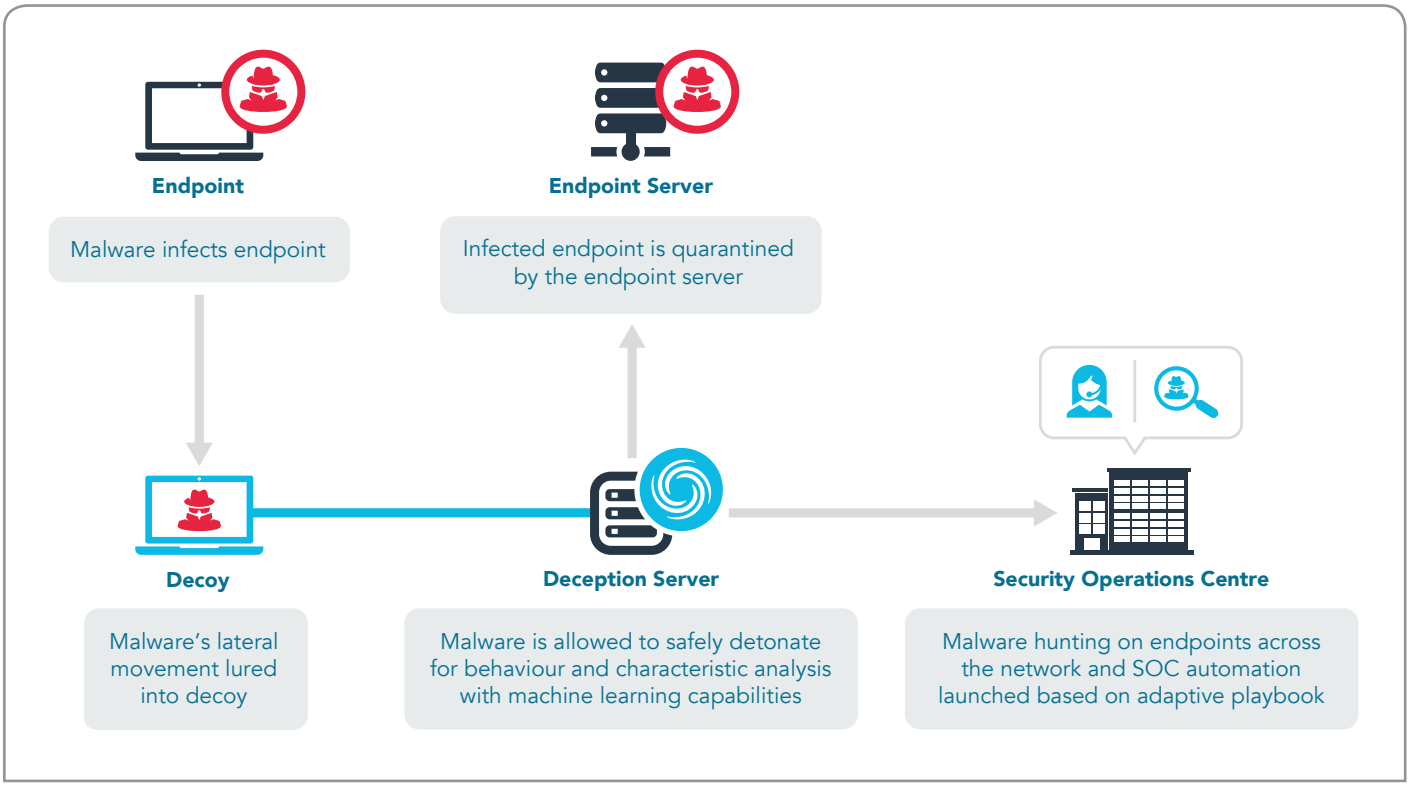
- Round-the-clock monitoring and a user-friendly customer portal provides improved visibility into the network and security environment.
- Delivers a more holistic view of threats with log collation across diverse platforms, as well as incident reporting with context analysis.

How It Works

Scenario 1: External threats

When an external attacker attempts to infiltrate the network:

- The deception server identifies the infected endpoint by using decoys and traps to trace the attack path.
- The IP address of the infected endpoint is pushed to the endpoint security server which blocks/quarantines the endpoint.
- The firewall protecting the network perimeter will be updated to block subsequent incoming attacks.
- Concurrently, the endpoint security server initiates malware hunting across the entire network.
- Event details are also pushed to the SIEM platform which applies machine learning to analyse the threat for incident handling/response.

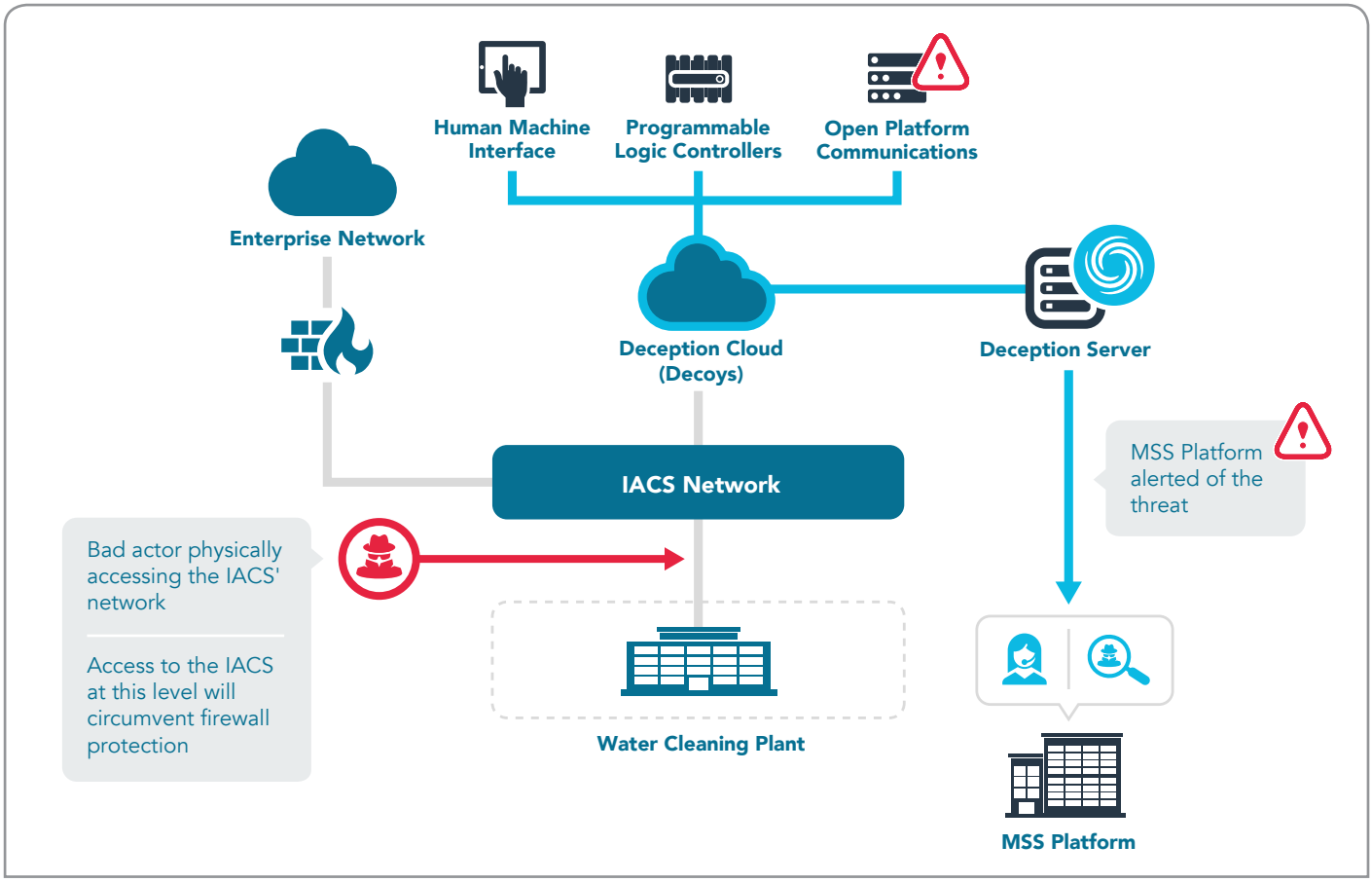


How It Works (continued)

Scenario 2: Insider threats

Insider threats are amongst the most difficult to counter because they are perpetrated by "trusted" internal parties. In an insider breach involving Supervisory Control and Data Acquisition (SCADA) and Industrial Automation and Control Systems (IACS):

- The insider is able to access the IACS' network, circumventing firewall protection.
- Deception technologies detect abnormal lateral movements, indicating the presence of a threat.
- The deception server identifies the threat and routes it to the sinkhole.
- The SIEM platform is alerted of the threat and applies machine learning to analyse it for incident handling/response.



Why Singtel

Backed by 10 audit-ready Singtel Security Operations Centres (SOCs) - 4 in North America, 4 in Asia Pacific and 2 in EMEA – and SpiderLabs' global leading intelligence research team.

Access to a team of security-cleared and experienced professionals with deep domain knowledge and professional certification[4].

End-to-end capabilities in deploying enterprise-wide, mission-critical security systems, trusted security advisory services, and independent security reviews to determine compliance gaps and propose remediation measures.

[4] CISSP, SABSA, CISM, CISA, GCIA, GCIH, GCFA, CEH, ECSA, CHFI, Mile2 and more.

About Singtel

Singtel is Asia's leading communications technology group, providing a portfolio of services from next-generation communication, technology services to infotainment to both consumers and businesses. For consumers, Singtel delivers a complete and integrated suite of services, including mobile, broadband and TV. For businesses, Singtel offers a complementary array of workforce mobility solutions, data hosting, cloud, network infrastructure, analytics and cybersecurity capabilities. The Group has presence in Asia, Australia and Africa and reaches over 685 million mobile customers in 22 countries. Its infrastructure and technology services for businesses span 21 countries, with more than 428 direct points of presence in 362 cities. For more information, visit www.singtel.com.

Awards

Gartner's Magic Quadrant for MSS, Worldwide
Leaders' Quadrant (Trustwave) (2018)

Frost & Sullivan APAC Best Practices Awards
Singapore Managed Security Service Provider of the Year (2016 - 2017)

NetworkWorld Asia Information Management Awards
Security-as-a-Service (2012 - 2017)
Regional Security Operations Center (2017)

Telecom Asia Awards
Most Innovative Approach to Mobile Security (2017)

SC Awards
Best Managed Security Service (Trustwave) (2017)

NetworkWorld Asia Information Management Awards
Disaster Recovery & Business Continuity (2014 - 2017)

March 2018

For more information g-security@singtel.com www.singtel.com/cybersecurity