Enhancing Cybersecurity with secure+ from ramsac: case studies

ramsac
the secure choice

Cyber threats are becoming increasingly sophisticated and require robust cybersecurity solutions. secure+ is a comprehensive cybersecurity monitoring tool designed to enhance an organisation's cyber resilience. Through proactive detection, intelligent classification, and rapid response to security incidents, secure+ safeguards against cyber attacks. This factsheet outlines how secure+ addresses different cybersecurity challenges through real-world case studies.

Adversary-in-the-Middle (AiTM) Attack Bypassing MFA

Scenario:

A victim received a phishing email mimicking a SharePoint file sharing link. Upon clicking the link and entering their credentials and MFA code, a cybercriminal stole their session data and accessed SharePoint as the victim.

How secure+ protects:

secure+ detected simultaneous logins from different IP addresses, generating a high-severity alert. The ramsac cybersecurity team quickly identified the malicious activity, locked the account, and cleared session data, preventing any data breach. secure+ intelligently assesses login activities and can automate lockouts based on suspicious behaviours.

Data Exfiltration from Insider Threat

Scenario:

A disgruntled employee attempted to transfer data from the company's file server to an external USB stick.

How secure+ protects:

secure+ detected the bulk data download and raised a high-severity alert. The ramsac cybersecurity team investigated and provided detailed evidence to the legal and HR teams, leading to immediate account lockdown. secure+ can block data transfers to external devices and automate responses to prevent further data loss.

Account Breach Using Leaked Credentials

Scenario:

A victim's credentials, leaked in a data breach, were used by a cybercriminal to access the victim's Microsoft account after the victim carelessly accepted an MFA request.

How secure+ protects:

secure+ detected the suspicious login from a different IP address and automatically locked the account, preventing data access. The ramsac cybersecurity team reset the victim's password and recommended further security awareness training. secure+ offers customisable automated responses to secure compromised accounts swiftly.

Brute-force Login Attempt on Company Firewall

Scenario:

A cybercriminal attempted to brute-force login credentials for a client's office firewall.

How secure+ protects:

secure+ detected the brute-force attempt, blocked the cybercriminal's IP address, and worked with the client to restrict management console access to specific IP addresses. This significantly reduced the attack surface and prevented further login attempts.

Preventing a Breach Following Compromised Credentials

Scenario:

A victim's credentials were stolen in a phishing attack, and the cybercriminal spammed multiple MFA requests.

How secure+ protects:

Secure+ detected the denied MFA attempts and sent an alert to the Cybersecurity Team. The team blocked the malicious IP, reset the victim's password, and provided guidance on avoiding similar attacks in the future. Secure+ can automatically send verification emails and escalate incidents for investigation.

ramsac
the secure choice

Stolen or Lost Laptop

Scenario:

A laptop containing sensitive data was stolen from a victim's car.

How secure+ protects:

Secure+ confirmed BitLocker encryption, initiated a remote-wipe command, and set up monitoring for any attempted device connections. The Cybersecurity Team maintained vigilance over the victim's account, ensuring no data compromise occurred. Organizations are reminded to report such incidents to the ICO if necessary.

secure+
from ramsac

What is secure+?

secure+ is a 24/7 eye on your IT security, helping you to protect your data and prevent cyber breaches. secure+ uses Microsoft Sentinel, which is a security monitoring and management tool created by Microsoft specifically for the analysis and investigation of security events. Sentinel ingests millions of events a day across an organisation's IT estate, and using artificial intelligence looks for signs and behaviours that seem unusual, risky or potentially malicious.

Sentinel then highlights these to the ramsac Cybersecurity team, who manually investigate them and determine what action may be required to safeguard your organisation. Sentinel can also ingest event data from other systems, such as Anti-Virus, firewall, and physical, virtual, or cloud servers. We continuously review and tweak the monitors we use in Sentinel to improve our effectiveness at detecting suspicious events.

Find out more

Contact us for more information on how secure+ from ramsac can help your organisation mitigate cybersecurity risks.

Tel: **01483 412 040** email **info@ramsac.com**

ramsac
the secure choice