Pondurance Managed Detection and Response (MDR) for Healthcare

PONDURANCE

CASE STUDY

THE CHALLENGE

A U.S.-based healthcare organization experienced a business email compromise (BEC) on its shared human resources account. The threat actors gained entry due to compromised weak user credentials and attempted to access organizational files. They also prepared to send emails to internal addresses, most likely in an attempt to gain further access.

OUR SOLUTION

As a Pondurance MDR customer, this organization is monitored 24 x 7 by our Security Operations Center (SOC). We were able to detect initial access through real-time log analysis and take immediate action. Our SOC reported the suspicious activity to the client's security team. We were able to track the threat actor within their Office 365 environment and guide the client on how to remove it. We were able to validate if any files were accessed and activate our Incident Response (IR) team to ensure no backdoors or nefarious inbox rules were created.

OUR RECOMMENDATIONS

- Monitor your infrastructure 24/7 to quickly identify suspicious activity across cloud, network, logs, and endpoints.
- Have an IR plan in place to be able to act immediately.
- Perform a security assessment and conduct tests.
- Perform a vulnerability audit to identify weak passwords and patches needed.
- Enable multi-factor authentication to make it more difficult for cybercriminals to access accounts.
- Regularly audit shared and service accounts for password strength and complexity.

Like our healthcare client, you should focus on quickly detecting threats and knowing who to call when you need help!

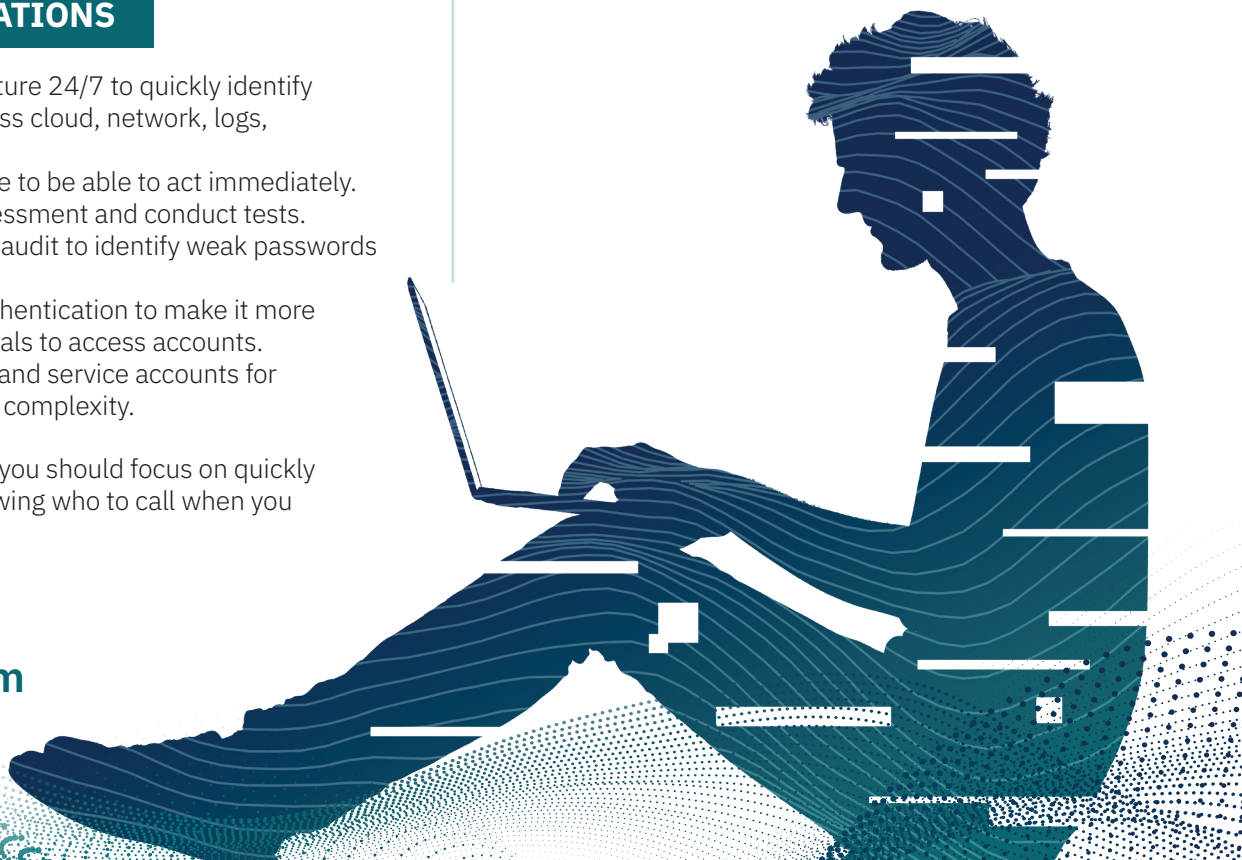
BENEFITS OF PONDURANCE MDR

- Stop security incidents through 24/7 detection and response.
- Maximize internal resources and security investments.
- Improve compliance through reporting.
- Rapidly accelerate security program maturity.
- Lower total cost of ownership (TCO).

ABOUT PONDURANCE

Pondurance delivers world-class MDR services to industries facing pressing and dynamic cybersecurity challenges including ransomware, complex compliance requirements, and digital transformation.

Our advanced platform with our experienced team of analysts continuously hunts, investigates, validates, and contains threats so your team can focus on what matters most.



pondurance.com

500 N. Meridian St., Suite 500,
Indianapolis, IN 46204