‘Extortion is a well-established approach for cyber criminals and is used through tactics that include threatening denial of service, doxing, and ransomware. In the reported case of the city of Johannesburg, the 4 Bitcoin ransom (circa $30K USD / £23.3 GBP / €26.8 EUR) is meaningful but not particularly high and so may be pitched at that level to encourage a decision to pay. Cyber criminals are increasingly making rational economic decisions around targeting organisations and demand ransom levels that they believe will have a higher likelihood of payment. Cybersecurity teams supporting the city will undoubtedly be working flat out to confirm the extent of any attack to aid officials in deciding if they should pay. The same learning needs to be applied to their future risk mitigation of any techniques the attackers used. All too often we are reminded that defensive controls are imperfect, and the ability to quickly detect and respond to live attacks that have successfully penetrated an organisation can make the difference between a contained incident and damaging breach.’