Captura de trafico para detección de Ransonware

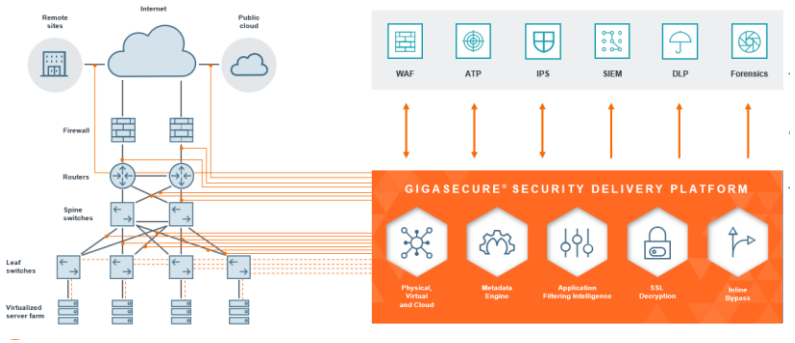
Problema

En la actualidad uno de los ataques mas temidos por todas las organizaciones es el Ransomware. Se trata de un problema muy complejo y difícil de atajar, ya que un simple descuido de cualquier usuario de la organización que acceda a un correo malicioso que contenga un ataque de phishing puede desencadenar una catástrofe para la organización que acabe paralizando su actividad por completo. No existe una única solución tecnológica capaz de resolver este problema, sino que es necesario contar con varias herramientas de seguridad y continuidad de negocio que ayuden a detectar y paliar el ataque cuanto antes, además de un equipo profesional que sea capaz de utilizarlas y reaccionar rápidamente ante un ataque. Entre estas soluciones podemos destacar loas de EDR, NDR, RBI, Web Proxies, Email Gateways, Detonadores de Malware//Sandbxing, Securizacion de Backups, Segmentación, Asignación de privilegios en directorios...

Solución

La plataforma de visibilidad de Gigamon permite capturar todo el trafico de la red, tanto de entornos físicos como virtuales, para filtrarlo, adecuarlo, y enviarlo a la plataforma de detección adecuada
Siendo el Ransomware un problema tan complejo de detectar y detener, Gigamon va a tener que alimentar a diferentes herramientas de detección, como pueden ser los NDR, IDS, IPS, Proxies, email Gateways, Sanbox...
Es también muy importante poder romper los túneles de SSL/TLS para tener visibilidad en el trafico cifrado, incluso en línea si se utilizan protocolos de clave segura PFS, como ocurre con TLS1.3. Aquí la plataforma de Gigamon puede también ayudar llegando a descifrar tanto el trafico entrante como el saliente

Esquema



Metadata
Generation
SSL Decryption
Map Rules

LINK