GravityZone XDR Network Sensor

Test GravityZone Network Sensor

1. login ssh sulla VA del Network Sensor
2. tail -f /opt/bitdefender/var/log/bdxdrd.log | grep Alert
3. con un endpoint di una delle reti monitorate,
   accedere con il browser a
   http://ghostr.bitdefender-testing.com/ghostr/html.html/763fdvf
4. Sulla console SSH della VA vediamo apparire nel log un alert simile a
   questo:https://nimb.ws/PCWmjqi
5. In GravityZone Cloud Console
   Incidents --> Search, tab HISTORICAL
   digitare una query come
   alert.type:ghoster
   oppure
   other.sensor_name:network
   + <RUN QUERY>
   Deve apparire una entry così: https://nimb.ws/GFKyA5L

Test Vulnerability Scan

1. Ci assicuriamo che sia disponibile una NIC sulla rete da scansionare (dove risiedono gli endpoint protetti)
2. login ssh sulla VA del Network Sensor
3. tail -f /opt/bitdefender/var/log/bdxdrd.log | grep VAScanner
4. In GravityZone Cloud Console
   Risk Management → Vulnerabilities
   Filtro Company: [company cliente da testare]
   <SCAN>
   O Endpoint scan
   V Network scan
   <SCAN>
5. Sulla console SSH della VA vediamo apparire nel log un alert simile a questo:
   https://nimb.ws/3zaZAPI

AVANGATE SECURITY