IBM QRADAR USE CASES

➢ Multiple Login Failures Followed by Success- Single Username

Rule Actions

Force the detected Event to create a NEW offense, select the offense using Username
Annotate this offense with: Multiple Login Failures Followed by Success - Single Username

Rule Responses

Dispatch New Event
Event Name: Multiple Login Failures Followed by Success - Single Username
Event Description: This rule is designed to detected when a successful login is observed after a brute force attempt. This activity could indicate that an attacker has successful enumerated the account credentials.
Severity: 1 Credibility: 0 Relevance: 0
High-Level Category: Authentication
Low-Level Category: User Login Success
Annotate the offense with Multiple Login Failures Followed by Success - Single Username
Force the dispatched event to create a NEW offense, select the offense using Username

Rule Condition

Apply Multiple Login Failures Followed by Suc on events which are detected by the Local system
and when a subset of at least 1 of these Attempted Password Guessing - Single Username, in any order, with the same username followed by a subset of at least 1 of these BB:Category Definition: Authentication Success in any order to the same username from the previous sequence, within 15 minutes

➢ Synology Log Cleared

Rule Actions

Force the detected Event to create a NEW offense, select the offense using Source IP
Annotate this offense with: Synology Log Cleared

Rule Responses

Dispatch New Event
Event Name: Synology Log Cleared
Event Description: This rule will detect when an audit log on a Synology NAS has been cleared. This could indicate an attacker who is attempting to cover their tracks.
Severity: 5 Credibility: 10 Relevance: 10
High-Level Category: System
Low-Level Category: Information
Annotate the offense with Synology Log Cleared
Force the dispatched event to create a NEW offense, select the offense using Source IP

Rule Condition

Apply Synology Log Cleared on events which are detected by the Local system
and when the event(s) were detected by one or more of SynologyDSM
and when the event QID is one of the following (1003000082) System Log Cleared

➢ Internal Port Sweep

Rule Actions

Force the detected Flow to create a NEW offense, select the offense using Source IP
Annotate this offense with: Internal Port Sweep

Rule Responses

Dispatch New Event
Event Name: Internal Port Sweep
Event Description: This rule will detect when a single host attempts to scan the same destination port to 6 different destination hosts over a 2 minutes span. This type of activity could indicate a possible port sweep in the network.
Severity: 5 Credibility: 10 Relevance: 10
High-Level Category: Recon
Low-Level Category: Network Sweep
Annotate the offense with Internal Port Sweep
Force the dispatched event to create a NEW offense, select the offense using Source IP

Rule Condition

Apply Internal Port Sweep and when the context is Local to Local on events or flows which are detected by the Local system
and when at least 6 events or flows are seen with the same Source IP, Destination Port and different Destination IP in 2 minutes
and NOT when the destination port is one of the following 0, 80, 443, 22, 445

➢ Inbound Traffic Allowed from X-Force Risky IP

Rule Actions

Force the detected Event to create a NEW offense, select the offense using Destination IP

Rule Responses

Dispatch New Event
Event Name: Inbound Traffic Allowed from X-Force Risky IP
Event Description: This rule detects when traffic from an X-Force watchlist is allowed through the firewall to an internal device. This activity could indicate that a device has been compromised.
Severity: 5 Credibility: 10 Relevance: 10
High-Level Category: Potential Exploit
Low-Level Category: Potential Misc Exploit
Annotate the offense with Inbound Traffic Allowed from X-Force Risky IPQRCE - 002 - Inbound Traffic Allowed from X-Force Risky IP
Force the dispatched event to create a NEW offense, select the offense using Destination IP

Rule Condition

Apply Inbound Traffic Allowed from X-Force R on events which are detected by the Local system
and when the event(s) were detected by one or more of Firewall
and when the event category for the event is one of the following Access.ACL Permit, Access Access Permitted, Access. Firewall Permit, Access.Firewall Session Opened
and when the source IP is a part of any of the following XForce Premium

➢ Unknown MAC Address

Rule Actions

Force the detected Event to create a NEW offense, select the offense using Destination MAC Address

Rule Responses

Dispatch New Event
Event Name: Unknown MAC Address
Event Description: This rule detects a MAC address that has not been seen on the network for over 30 days. When this happens the new MAC address is added to the known MAC address list but an event is created for the new device.
Severity: 1 Credibility: 10 Relevance: 10
High-Level Category: Control System
Low-Level Category: Device Information
Annotate the offense with Unknown MAC Address
Force the dispatched event to create a NEW offense, select the offense using Destination MAC Address
Add Destination MAC to Reference Set: Known Mac Addresses

Rule Condition

and when the event(s) were detected by one or more of OPNSense
and when the event category for the event is one of the following Application DHCP Session In Progress. Application.DHCP Success. Application DHCP Session Opened, Application.DHCP Failure, Application DHCP Session Denied, Application.DHCP Session Closed

and NOT when any of Destination MAC are contained in any of Known Mac Addresses - AlphaNumeric (Ignore Case) and NOT when the event QID is one of the following (1002250010) DHCP Reuse Existing Lease

➢ Successful VPN Connection Outside the US

Rule Actions

Force the detected Event to create a NEW offense, select the offense using Source IP

Rule Responses

Dispatch New Event
Event Name: QRCE - 001 - Successful VPN Connection Outside the US
Event Description: This rule will create an event when a Successful VPN connection outside of the United States. This should never happen on this network as the only users are US based.
Severity: 5 Credibility: 10 Relevance: 10
High-Level Category: Application
Low-Level Category: VPN In Progress
Annotate the offense with QRCE - 001 - Successful VPN Connection Outside the US
Force the dispatched event to create a NEW offense, select the offense using Source IP

Rule Condition

Apply Successful VPN Connection Outside the on events which are detected by the Local system
and when the event(s) were detected by one or more of OpenVPN @ OPNsense
and when the source is Remote
and NOT when the source IP is a part of any of the following North America. United States
and when the event QID is one of the following (1002750013) VPN Internal Address Assigned. (1002750007) Attempting to Send VPN Connection Settings

➢ Internal Vulnerability Scan

Rule Actions

Force the detected Event to create a NEW offense, select the offense using Source IP

Rule Responses

Dispatch New Event
Event Name: QRCE - 002 - Internal Vulnerability Scan
Event Description: This rule will look for 10 unique snort signatures (QIDs) in a 10 minute span from the same source IP. This type of activity is typically associated with a an attempted vulnerability scan.
Severity: 5 Credibility: 10 Relevance: 10
High-Level Category: Recon
Low-Level Category: Misc Recon Event
Annotate the offense with QRCE - 002 - Internal Vulnerability Scan
Force the dispatched event to create a NEW offense, select the offense using Source IP

Rule Condition

Apply Internal Vulnerability Scan on events which are detected by the Local system
and when the event(s) were detected by one or more of Snort Open Source IDS
and when the event context is Local to Local
and when at least 5 events are seen with the same Source IP and different QID in 3 minutes

➢ Unauthorized DNS Server

Rule Actions

Force the detected Flow to create a NEW offense, select the offense using Source IP

Rule Responses

Dispatch New Event
Event Name: QRCE - 003 - Unauthorized DNS Server
Event Description: This event will trigger when an unauthorized DNS server is detected on the network. This rule will compare the DNS servers included in the DNS Servers reference set and if a match is not found an event will be created.
Severity: 5 Credibility: 10 Relevance: 10
High-Level Category: Application
Low-Level Category: DNS In Progress
Annotate the offense with QRCE - 003 - Unauthorized DNS Server
Force the dispatched event to create a NEW offense, select the offense using Source IP

Rule Condition

Apply Unauthorized DNS Server on events or flows which are detected by the Local system
and when the destination port is one of the following 53
and NOT when the context is Local to Local
and NOT when any of Source IP. Destination IP are contained in any of DNS Servers - IP
and NOT when a flow or an event matches any of the following Authorized DNS Exceptions
and NOT when the source IP is one of the following 10.0.30.20

➢ TOR Traffic - ET_TOR

Rule Actions

Force the detected Flow to create a NEW offense, select the offense using Destination IP
Annotate this offense with: QRCE - 001 - TOR Traffic - ET_TOR

Rule Responses

Dispatch New Event
Event Name: QRCE - 001 - TOR Traffic - ET_TOR
Event Description: This event will trigger when traffic is observed to or from a known TOR IP address that is contained on the reference set (ET_Tor). This activity could possibly indicate that TOR traffic is occurring on the network.
Severity: 5 Credibility: 10 Relevance: 10
High-Level Category: Policy
Low-Level Category: Compliance Policy Violation
Annotate the offense with QRCE - 001 - TOR Traffic - ET_TOR
Force the dispatched event to create a NEW offense, select the offense using Destination IP

Rule Condition

Apply TOR Traffic-ET_TOR on events or flows which are detected by the Local system
and NOT when the context is Local to Local, Remote to Remote
and when any of Destination IP, Source IP are contained in any of ET Tor - IP
and NOT when the destination network is DMZ.WAN External IP, DMZ.T-Pot Docker Containers-VLAN30
and NOT when the source network is DMZ.WAN External IP

➢ Excessive OTP Fails from an IP Address for Several Usernames

Rule Condition

Apply Credential Access - Excessive OTP Fails from an IP Address for Several Usernames
and when the event matches Event Name is OTP Incorrect
and when at least 3 events are seen with the same Source IP and different Username in 12 hour(s)