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)

➢ Network Running on UPS

Rule Actions

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

Rule Responses

Dispatch New Event
Event Name: Network Running on UPS
Event Description: This rule looks for any UPS events indicating that the local network is running on a UPS. This is an indicating that the System was lost power and is utilizing the battery backup.
Severity: 3 Credibility: 10 Relevance: 10
High-Level Category: System
Low-Level Category: Warning
Annotate the offense with Network Running on UPS
Force the dispatched event to create a NEW offense, select the offense using Source IP

Rule Condition

Apply Network Running on UPS on events which are detected by the Local system
and when the event(s) were detected by one or more of Synology @ Spiderman
and when the event QID is one of the following (1003000032) Running on UPS

➢ Outbound 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: Outbound 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 Outbound Vulnerability Scan
Force the dispatched event to create a NEW offense, select the offense using Source IP

Rule Condition

Apply Outbound 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 Remote
and when at least 5 events are seen with the same Source IP and different QID in 3 minutes

➢ VPN Connection from Multiple IPs

Rule Actions

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

Rule Responses

Dispatch New Event
Event Name: VPN Connection from Multiple IPs
Event Description: This event will trigger when the same username is observed successfully authenticating from 2 unique source IPs in a 4 hour time span. This activity could indicate that credentials are being shared or that the account is compromised.
Severity: 1 Credibility: 10 Relevance: 10
High-Level Category: Application
Low-Level Category: VPN In Progress
Annotate the offense with VPN Connection from Multiple IPs
Force the dispatched event to create a NEW offense, select the offense using Username

Rule Condition

Apply VPN Connection from Multiple IPs on events which are detected by the Local system
and when Successful VPN Authentication match at least 2 times with the same Username and different Source IP in 4 hour(s)

➢ Internal Port Scan

Rule Actions

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

Rule Responses

Dispatch New Event
Event Name: Internal Port Scan
Event Description: This rule will detect when a single IP has attempted to access 10 unique ports from the port range 1-10000 in a 2 minute span to the same destination IP. This activity could possibly indicate a local port scan attempt.
Severity: 1 Credibility: 10 Relevance: 10
High-Level Category: Recon
Low-Level Category: NMAP Reconnaissance
Annotate the offense with Internal Port Scan

Rule Condition

Apply Internal Port Scan on events or flows which are detected by the Local system
and when the context is Local to Local
and when Port Scan Activity match at least 10 times with the same Source IP, Destination IP and different Destination Port in 2 minutes

➢ Outbound Port Scan

Rule Actions

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

Rule Responses

Dispatch New Event
Event Name: Outbound Port Scan
Event Description: This rule will detect when a single IP has attempted to access 10 unique ports from the port range 1-10000 in a 10 minute span to the same destination IP. This activity could possibly indicate a port scan attempt.
Severity: 1 Credibility: 10 Relevance: 10
High-Level Category: Recon
Low-Level Category: NMAP Reconnaissance
Annotate the offense with Outbound Port Scan
Force the dispatched event to create a NEW offense, select the offense using Destination IP

Rule Condition

Apply Outbound Port Scan on events or flows which are detected by the Local system
and when the context is Local to Remote
and when Port Scan Activity, match at least 10 times with the same Source IP. Destination IP and different Destination Port in 3 minutes
and NOT when the source network is DMZ WAN External IP

➢ Outbound Traffic to X-Force Risky IP

Rule Actions

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

Rule Responses

Dispatch New Event
Event Name: Outbound Traffic to X-Force Risky IP
Event Description: This rule detects when an internal host is reaching out to a Risky IP classified by the X-Force remote networks list. When this activity is observed this could potentially indicate that the internal endpoint is compromised.
Severity: 5 Credibility: 10 Relevance: 10
High-Level Category: Potential Exploit
Low-Level Category: Potential Misc Exploit
Annotate the offense with Outbound Traffic to X-Force Risky IP
Force the dispatched event to create a NEW offense, select the offense using Source IP

Rule Condition

Apply Outbound Traffic to X-Force Risky IP on events or flows which are detected by the Local system
and when the destination IP is a part of any of the following XForce Premium
and NOT when the destination network is DMZ.T-Pot Docker Containers-VLAN30
and NOT when the destination port is one of the following 123
and NOT when the source network is DMZ.WAN External IP

➢ MS Audit Log Cleared

Rule Actions

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

Rule Responses

Dispatch New Event
Event Name: MS Audit Log Cleared
Event Description: This rule will detect when an audit log on a windows device 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 MS Audit Log Cleared
Force the dispatched event to create a NEW offense, select the offense using Source IP

Rule Condition

Apply MS Audit Log Cleared on events which are detected by the Local system
and when the event(s) were detected by one or more of Microsoft Windows Security Event Log
and when the event QID is one of the following (5000006) The audit log was cleared, (5001535) Audit Log Cleared, (5000178) Audit log cleared, (5001534) Audit Log Cleared

➢ Synology USB Exfiltration

Rule Actions

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

Rule Responses

Dispatch New Event
Event Name: Synology USB Exfiltration
Event Description: This rule will potentially detect when a file/folder is copied from an internal file share to an external USB device. This type of activity could indicate potential data exfiltration.
Severity: 5 Credibility: 10 Relevance: 10
High-Level Category: Risk
Low-Level Category: Data Loss Possible
Annotate the offense with Synology USB Exfiltration
Force the dispatched event to create a NEW offense, select the offense using Source IP

Rule Condition

Apply Synology USB Exfiltration 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 (1003000086) File Copied, (1003000087) Folder Copied and when the event matches File Destination Path (custom) matches any of expressions Vusbshareld

➢ External SMB Scanning

Rule Actions

Force the detected Flow to create a NEW offense, select the offense using Source IP
Annotate this offense with: External SMB Scanning

Rule Responses

Dispatch New Event
Event Name: External SMB Scanning
Event Description: This rule detects when an endpoint on the network is attempting 10 outbound connections to unique destination IPs over the destination port 445. This type of activity could indicate an outbound SMB scan which is very suspicious for an endpoint. This type of activity is commonly associated with MS17-010 worm variants.
Severity: 5 Credibility: 10 Relevance: 10
High-Level Category: Application
Low-Level Category: SMB Session In Progress
Annotate the offense with External SMB Scanning
Force the dispatched event to create a NEW offense, select the offense using Source IP

Rule Condition

Apply QRCE-001-External SMB Scanning on events or flows which are detected by the Local system
and when the context is Local to Remote, Remote to Remote
and when the destination port is one of the following 445
and NOT when the source network is DMZ.T-Pot Docker Containers-VLAN30
and when at least 10 events or flows are seen with the same Source IP and different Destination IP in 2 minutes

➢ Inbound Exploit Followed by Outbound Traffic

Rule Actions

Force the detected Event to create a NEW offense, select the offense using Source IP. Annotate this offense with: Inbound Exploit Followed by Outbound Traffic

Rule Responses

Dispatch New Event
Event Name: Inbound Exploit Followed by Outbound Traffic
Event Description: This rule is designed to detected outbound traffic occurring after an inbound exploit attempt is observed. This could indicate that an exploit was successful.
Severity: 5 Credibility: 10 Relevance: 10
High-Level Category: Potential Exploit
Low-Level Category: Potential Misc Exploit
Annotate the offense with Inbound Exploit Followed by Outbound Traffic
Force the dispatched event to create a NEW offense, select the offense using Source IP

Rule Condition

Apply Inbound Exploit Followed by Outbound on events which are detected by the Local system
and when the event context is Local to Remote, Remote to Remote
and when the event category for the event is one of the following Access.ACL Permit, Access. Firewall Permit, Access. Firewall Session Opened, Access Firewall Session Closed, Access. Firewall Deny, Access.ACL Deny and NOT when the source network is DMZ.T-Pot Docker Containers-VLAN30, DMZ WAN External IP
and when any of Destination IP are contained in any of Inbound Exploit IPs – IP

➢ Base64 DNS Query

Rule Actions

Force the detected Event to create a NEW offense, select the offense using Source IP
Annotate this offense with: Base64 DNS Query

Rule Responses

Dispatch New Event
Event Name: Base64 DNS Query
Event Description: This rule is designed to detected Base64 encoded DNS queries. This could potentially indicate data exfiltration.
Severity: 5 Credibility: 10 Relevance: 10
High-Level Category: Application
Low-Level Category: DNS In Progress
Annotate the offense with Base64 DNS Query
Force the dispatched event to create a NEW offense, select the offense using Source IP

Rule Condition

Apply QRCE-001-Base64 DNS Query on events which are detected by the Local system
and when the event category for the event is one of the following Application.DNS In Progress, Application.DNS Opened
and when any of DNS Query (custom) match ^[a-zA-Z0-9+V](40,}={0.2}

➢ Rouge DHCP Server

Rule Actions

Force the detected Event to create a NEW offense, select the offense using Source IP
Annotate this offense with: Rouge DHCP Server

Rule Responses

Dispatch New Event
Event Name: Rouge DHCP Server
Event Description: This rule is designed to look for DHCP traffic destined to an unauthorized DHCP server. This could indicate an attacker is actively trying to DoS, MITM, or perform reconnaissance on the local network.
Severity: 5 Credibility: 10 Relevance: 10
High-Level Category: Application
Low-Level Category: DHCP Session In Progress
Annotate the offense with Rouge DHCP Server
Force the dispatched event to create a NEW offense, select the offense using Source IP

Rule Condition

Apply Rouge DHCP Server on events which are detected by the Local system
and when the event(s) were detected by one or more of Fortinet FortiGate Security Gateway
and when the event context is Local to Local
and NOT when the destination IP is one of the following 192.168.1.1
and when the event matches Service (custom) is any of DHCP

➢ Interactive Service Account Login

Rule Actions

Force the detected Event to create a NEW offense, select the offense using Username
Annotate this offense with: Interactive Service Account Login

Rule Responses

Dispatch New Event
Event Name: Interactive Service Account Login
Event Description: This rule is designed to detect when a service account is observed with an interactive login. This should not occur as non-repudiation is lost in the environment.
Severity: 5 Credibility: 10 Relevance: 10
High-Level Category: Authentication
Low-Level Category: User Login Success
Annotate the offense with Interactive Service Account Login
Force the dispatched event to create a NEW offense, select the offense using Username

Rule Condition

Apply QRCE-001-Interactive Service Account Login on events which are detected by the Local system
and when the event(s) were detected by one or more of Microsoft Windows Security Event Log
and when any of Username match ^srv
and when the event matches EventID (custom) is any of 4624
and when the event matches LogonType (custom) is any of [2 or 10 or 11 or 7]

➢ Attempted Password Guessing - Single Username

Rule Actions

Force the detected Event to create a NEW offense, select the offense using Username
Annotate this offense with: Attempted Password Guessing - Single Username

Rule Responses

Dispatch New Event
Event Name: Attempted Password Guessing - Single Username
Event Description: This rule is designed to detected 5 failed authentication attempts in a 1 minute period. This type of activity could indicate a brute force attempt against an account is occurring.
Severity: 5 Credibility: 10 Relevance: 10
High-Level Category: Authentication
Low-Level Category: User Login Failure
Annotate the offense with Attempted Password Guessing - Single Username
Force the dispatched event to create a NEW offense, select the offense using Username

Rule Condition

Apply Attempted Password Guessing - Single on events which are detected by the Local system
and when an event matches any of the following BB:Category Definition: Authentication Failures
and when at least 5 events are seen with the same Username in 1 minutes

➢ Remote VPN Brute Force

Rule Actions

Force the detected Event to create a NEW offense, select the offense using Source IP
Annotate this offense with: Remote VPN Brute Force

Rule Responses

Dispatch New Event
Event Name: Remote VPN Brute Force
Event Description: This rule detects when 5 failed login attempts are observed in a 1 minute span. This activity could indicate a potential brute force against the VPN server.
Severity: 5 Credibility: 10 Relevance: 10
High-Level Category: Exploit
Low-Level Category: Password Guess/Retrieve
Annotate the offense with Remote VPN Brute Force
Force the dispatched event to create a NEW offense, select the offense using Source IP

Rule Condition

Apply Remote VPN Brute Force on events which are detected by the Local system
and when the event(s) were detected by one or more of Fortinet FortiGate Security Gateway
and NOT when the event context is Local to Local
and when an event matches any of the following BB: Category Definition: Authentication Failures
and when at least 5 events are seen with the same Username in 1 minutes