TIME
Security
Advanced Monitoring
<table>
<thead>
<tr>
<th>Types</th>
<th>Categories</th>
</tr>
</thead>
<tbody>
<tr>
<td>Devices with High Event Rates</td>
<td>Anomaly</td>
</tr>
<tr>
<td>Excessive Firewall Denies from Single Source</td>
<td>Anomaly</td>
</tr>
<tr>
<td>Single IP with Multiple MAC addresses</td>
<td>Anomaly</td>
</tr>
<tr>
<td>First-Time User Access to Critical Asset</td>
<td>Anomaly</td>
</tr>
<tr>
<td>Remote Access from Foreign Country/Region</td>
<td>Anomaly</td>
</tr>
<tr>
<td>Anomaly: Excessive Firewall Accepts From Multiple Source to a Single Destination</td>
<td>Anomaly</td>
</tr>
<tr>
<td>Excessive Database Connections</td>
<td>Anomaly</td>
</tr>
<tr>
<td>First-Time User Access to Critical Asset</td>
<td>Authentication</td>
</tr>
<tr>
<td>Login Failure to Disabled Account</td>
<td>Authentication</td>
</tr>
<tr>
<td>Login Failure to Expired Account</td>
<td>Authentication</td>
</tr>
<tr>
<td>Multiple Login Failures from the Same Source (Windows)</td>
<td>Authentication</td>
</tr>
<tr>
<td>Possible Shared Accounts</td>
<td>Authentication</td>
</tr>
<tr>
<td>Repeat Non-Windows Login Failures</td>
<td>Authentication</td>
</tr>
<tr>
<td>Login Failures Followed By Success from the same Source IP</td>
<td>Authentication</td>
</tr>
<tr>
<td>Login Failures Followed By Success to the same Source IP</td>
<td>Authentication</td>
</tr>
<tr>
<td>Login Failures Followed By Success to the same Username</td>
<td>Authentication</td>
</tr>
<tr>
<td>Multiple Login Failures for Single Username</td>
<td>Authentication</td>
</tr>
<tr>
<td>Multiple Login Failures from the Same Source</td>
<td>Authentication</td>
</tr>
<tr>
<td>Multiple Login Failures to the Same Destination</td>
<td>Authentication</td>
</tr>
<tr>
<td>Repeat Windows Login Failures</td>
<td>Authentication</td>
</tr>
<tr>
<td>Potential Botnet Events Become Offenses</td>
<td>Botnet</td>
</tr>
<tr>
<td>DDoS Attack Detected</td>
<td>DDoS</td>
</tr>
<tr>
<td>DDoS Events with High Magnitude Become Offenses</td>
<td>DDoS</td>
</tr>
<tr>
<td>DoS Events with High Magnitude Become Offenses</td>
<td>DDoS</td>
</tr>
<tr>
<td>Network DoS Attack Detected</td>
<td>DDoS</td>
</tr>
<tr>
<td>Service DoS Attack Detected</td>
<td>DDoS</td>
</tr>
<tr>
<td>Login Failure to Disabled Account</td>
<td>Horizontal Movement</td>
</tr>
<tr>
<td>Login Failure to Expired Account</td>
<td>Horizontal Movement</td>
</tr>
<tr>
<td>Chained Exploit Followed by Suspicious Events</td>
<td>Intrusion Detection</td>
</tr>
<tr>
<td>Chained Exploit Followed by Suspicious Events on the Third Host</td>
<td>Intrusion Detection</td>
</tr>
<tr>
<td>Destination Vulnerable to Detected Exploit</td>
<td>Intrusion Detection</td>
</tr>
<tr>
<td>Exploit: Destination Vulnerable to Detected Exploited on a Different Port</td>
<td>Intrusion Detection</td>
</tr>
<tr>
<td>Exploits Events with High Magnitude Become Offenses</td>
<td>Intrusion Detection</td>
</tr>
<tr>
<td>Login Failures Followed By Success from the same Source IP</td>
<td>Intrusion Detection</td>
</tr>
<tr>
<td>Login Failures Followed By Success from the same Destination IP</td>
<td>Intrusion Detection</td>
</tr>
<tr>
<td>Login Failures Followed By Success to the same Username</td>
<td>Intrusion Detection</td>
</tr>
<tr>
<td>Source Vulnerable to any Exploit</td>
<td>Intrusion Detection</td>
</tr>
<tr>
<td>Source Vulnerable to this Exploit</td>
<td>Intrusion Detection</td>
</tr>
<tr>
<td>100% Accurate Events</td>
<td>Intrusion Detection</td>
</tr>
<tr>
<td>All Exploits Become Offenses</td>
<td>Intrusion Detection</td>
</tr>
<tr>
<td>Attack followed by Attack Response</td>
<td>Intrusion Detection</td>
</tr>
<tr>
<td>Database Failures Followed by User Changes</td>
<td>Intrusion Detection</td>
</tr>
<tr>
<td>Database Multiple Database Failures Followed by Success</td>
<td>Intrusion Detection</td>
</tr>
<tr>
<td>Destination Vulnerable to Different Exploit than Attempted on Targeted Port</td>
<td>Intrusion Detection</td>
</tr>
<tr>
<td>Exploit Followed by Suspicious Host Activity</td>
<td>Intrusion Detection</td>
</tr>
<tr>
<td>Exploit/Malware Events Across Multiple Destinations</td>
<td>Intrusion Detection</td>
</tr>
<tr>
<td>Exploits: Exploits Followed by Firewall Accepts</td>
<td>Intrusion Detection</td>
</tr>
<tr>
<td>Multiple Exploit Types Against Single Destination</td>
<td>Intrusion Detection</td>
</tr>
<tr>
<td>Multiple Vector Attack Source</td>
<td>Intrusion Detection</td>
</tr>
<tr>
<td>BadRabbit Detected in Real Time</td>
<td>Malware</td>
</tr>
<tr>
<td>Local Host Sending Malware</td>
<td>Malware</td>
</tr>
<tr>
<td>Malware or Virus Clean Failed</td>
<td>Malware</td>
</tr>
<tr>
<td>TIME-Forticlient</td>
<td>Malware</td>
</tr>
<tr>
<td>Treat Backdoor Trojan and Virus Events as Offenses</td>
<td>Malware</td>
</tr>
<tr>
<td>Treat Key Loggers as Offenses</td>
<td>Malware</td>
</tr>
<tr>
<td>Treat Non-Spyware Malware as Offenses</td>
<td>Malware</td>
</tr>
<tr>
<td>Treat Spyware and Virus as Offenses</td>
<td>Malware</td>
</tr>
<tr>
<td>Ransomware Behaviour from Endpoint Security Logs</td>
<td>Ransomware</td>
</tr>
<tr>
<td>Ransomware Behaviour from Microsoft Windows Security Event Logs</td>
<td>Ransomware</td>
</tr>
<tr>
<td>UBA: Ransomware Behavior from Endpoint Security Logs</td>
<td>Ransomware</td>
</tr>
<tr>
<td>UBA: Ransomware Behavior from Microsoft Windows Security Logs</td>
<td>Ransomware</td>
</tr>
<tr>
<td>Database Remote Login Failure</td>
<td>Recon</td>
</tr>
<tr>
<td>Excessive Database Connections</td>
<td>Recon</td>
</tr>
</tbody>
</table>
List of Threats

Excessive Failed Logins to Compliance IS
Excessive Firewall Accepts Across Multiple Hosts
Excessive Firewall Denies from Local Host
Excessive Firewall Denies from Remote Host
Multiple Login Failures from the Same Source
Multiple Login Failures from the Same Source (Windows)
Multiple Login Failures to the Same Destination
Repeat Non-Windows Login Failures
Repeat Windows Login Failures.

Anomaly: Excessive Firewall Accepts From Multiple Sources to a Single Destination
Database Attempted Configuration Modification by a remote host
Database Concurrent Logins from Multiple Locations
Database Groups Changed from Remote Host
Database User Rights Changed from Remote Host
Local Mass Mailing Host Detected
Possible Local Worm Detected
Worm Detected (Events)
Device Stopped Sending Events
Load Basic Building Blocks
System Notification
Failed Communication to a Malicious Website
Multiple Threats Detected on Same Host
Possible Shared Accounts
Potential Botnet Events Become Offenses
Potential Honeypot Access
Same Threat Detected on Multiple Hosts
Same Threat Detected on Multiple Servers
Same Threat Detected on Same Host
Same Threat Detected on Same Network Different Hosts
Successful Communication to a Malicious Website
X-Force Premium: Internal Host Communicating with Botnet Command and Control URL
X-Force Premium: Internal Host Communicating with Malware URL

UOA: Account or Group or Privileges Added
UOA: Account or Group or Privileges Modified
UOA: Anomalous Account Created From New Location
UOA: Anomalous Cloud Account Created From New Location
UOA: Browsed to Business/Service Website
UOA: Browsed to Communication Website
UOA: Browsed to Entertainment Website
UOA: Browsed to Gambling Website
UOA: Browsed to Information Technology Website
UOA: Browsed to Job Search Website
UOA: Browsed to LifeStyle Website
UOA: Browsed to Malicious Website
UOA: Browsed to Mixed Content/Potentially Adult Website
UOA: Browsed to Phishing Website
UOA: Browsed to Pornography Website
UOA: Browsed to Scam/Questionable/Illegal Website
UOA: Browsed to Uncategorized Website
UOA: Bruteforce Authentication Attempts
UOA: Common Exploit Tool Detected
UOA: Common Exploit Tool Detected (Asset)
UOA: Create Offense
UOA: Critical Systems Users Seen Update
UOA: D/DoS Attack Detected
UOA: Detect Insecure or Non-Standard Protocol
UOA: Detect IOC's For Locky
UOA: Detect IOC's for WannaCry
UOA: Detect Persistent SSH Session
UOA: Dormant Account Found (privileged)
UOA: Dormant Account Used
UOA: Executive Only Asset Accessed by Non-Executive User
UOA: Expired Account Used
UOA: First Privileged Exfiltration

Recon
Post Intrusion Activity
Post Intrusion Activity
Post Intrusion Activity
Post Intrusion Activity
Post Intrusion Activity
Post Intrusion Activity
Post Intrusion Activity
Post Intrusion Activity
Post Intrusion Activity
System
System
System
Threats
Threats
Threats
Threats
Threats
Threats
Threats
Threats
User Behavioral Analytics
User Behavioral Analytics
User Behavioral Analytics
User Behavioral Analytics
User Behavioral Analytics
User Behavioral Analytics
User Behavioral Analytics
User Behavioral Analytics
User Behavioral Analytics
User Behavioral Analytics
User Behavioral Analytics
User Behavioral Analytics
User Behavioral Analytics
User Behavioral Analytics
User Behavioral Analytics
User Behavioral Analytics
User Behavioral Analytics
User Behavioral Analytics
User Behavioral Analytics
User Behavioral Analytics
User Behavioral Analytics
User Behavioral Analytics
List of Threats

UBA: High Risk User Access to Critical Asset
UBA: Hioneytoken Activity
UBA: Internet Settings Modified
UBA: Kerberos Accpoint Mapping
UBA: Large Outbound Transfer by Hugh Risk User
UBA: Malicious Process Detected
UBA: Malware Activity - Registry Modified in Bulk
UBA: Multiple Kerberos Authentication Failures from Same User
UBA: Multiple VPN Accounts Failed Login from Single IP.
UBA: MultipleVPN Acccounts ogged in From Single IP
UBA: Netcast Process Detection (Linux)
UBA: Netcase Process Detection (Windows)
UBA: Network Share Accessed
UBA: Network Traffic: Capture, Monitoring and Analysis Program Usage
UBA: New Account Use Detected
UBA: Non-Admin Access to Domain Controller
UBA: Pash the Hash
UBA: Populate Authorized Applications
UBA: Populate Multiple VPN Accounts Failed Login from Single IP
UBA: Populate Multiple VPN Accounts Logged in From Single IP
UBA: Populate Process Filenames
UBA: Possible TGT Forgery
UBA: Potential Access to Blacklist Domain
UBA: Potential Access to DGA Domain
UBA: Potential Access to Squatting Domain
UBA: Potential Access to Tunnelling Domain
UBA: Process Creating Suspicious Remote Threads Detected (Asset)
UBA: Process Executed Outside Gold Disk Whitelist (Linux)
UBA: Process Executed Outside Gold Disk Whitelist (Windows)
UBA: Ransomware Behaviour Detected
UBA: Recent User Activity Update(privileged)
UBA: Repeat Unauthorized Access
UBA: Restricted Program Usage
UBA: Shellbags Modified by Ransomware
UBA: Subject_CN and Username Map Update
UBA: Subject_CN and Username Mapping
UBA: Suspicious Activities on Compromised Hosts
UBA: Suspicious Activities on Compromised Hosts (Asset)
UBA: Suspicious Administrative Activities Detected
UBA: Suspicious Command Prompt Activity
UBA: Suspicious Entries in System Registry (Asset)
UBA: Suspicious Image Load Detected (Asset)
UBA: Suspicious Pipe Activities (Asset)
UBA: Suspicious PowerShell Activity
UBA: Suspicious Privileged Activity (First Observed Privilege Use)
UBA: Suspicious Privileged Activity (Rarely Used Privileged)
UBA: Suspicious Scheduled Task Activities
UBA: Suspicious Service Activities
UBA: Suspicious Service Activities (Asset)
UBA: TGT Ticket Used by Multiple Hosts
UBA: Unauthorized Access
UBA: UNIX/LINUX System Accessed With Service or Machine Account
UBA: Unusual Scanning of Database Servers Detected
UBA: Unusual Scanning of DHCP Servers Detected
UBA: Unusual Scanning of DNS Servers Detected
UBA: Unusual Scanning of FTP Servers Detected
UBA: Unusual Scanning of Game Servers Detected
UBA: Unusual Scanning of Generic ICMP Detected
UBA: Unusual Scanning of Generic TCP Detected
UBA: Unusual Scanning of Generic UDP Detected
UBA: Unusual Scanning of IRC Servers Detected
UBA: Unusual Scanning of LDAP Servers Detected
UBA: Unusual Scanning of Mail Servers Detected
UBA: Unusual Scanning of Messaging Servers Detected

User Behavioral Analytics