ADVANCED SECURITY MONITORING

Security

time.com.my

time™

List of Threats

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

List of Threats

Ransomware Behaviour from Endpoint Security Logs	**Ransomware**
Ransomware Behaviour from Microsoft Windows Security Event Logs	Ransomware
UBA: Ransomware Behavior from Endpoint Security Logs	Ransomware
UBA: Ransomware Behavior from Microsoft Windows Security Logs	Ransomware
Database Remote Login Failure	**Recon**
Excessive Database Connections	Recon
Excessive Failed Logins to Compliance IS	Recon
Excessive Firewall Accepts Across Multiple Hosts	Recon
Excessive Firewall Denies from Local Host	Recon
Excessive Firewall Denies from Remote Host	Recon
Multiple Login Failures from the Same Source	Recon
Multiple Login Failures from the Same Source (Windows)	Recon
Multiple Login Failures to the Same Destination	Recon
Repeat Non-Windows Login Failures	Recon
Repeat Windows Login Failures	Recon
Anomaly: Excessive Firewall Accepts from Multiple Sources to a Single Destination	**Post Intrusion Activity**
Database Attempted Configuration Modification by a remote host	Post Intrusion Activity
Database Concurrent Logins from Multiple Locations	Post Intrusion Activity
Database Groups Changed from Remote Host	Post Intrusion Activity
Database User Rights Changed from Remote Host	Post Intrusion Activity
Local Mass Mailing Host Detected	Post Intrusion Activity
Possible Local Worm Detected	Post Intrusion Activity
Worm Detected (Events)	Post Intrusion Activity
Device Stopped Sending Events	System
Load Basic Building Blocks	System
System Notification	System
Failed Communication to a Malicious Website	**Threats**
Multiple Threats Detected on Same Host	Threats
Possible Shared Accounts	Threats
Potential Botnet Events Become Offenses	Threats
Potential Honeypot Access	Threats
Same Threat Detected on Multiple Hosts	Threats
Same Threat Detected on Multiple Servers	Threats
Same Threat Detected on Same Host	Threats
Same Threat Detected on Same Network Different Hosts	Threats
Successful Communication to a Malicious Website	Threats
X-Force Premium: Internal Host Communicating with Botnet Command and Control URL	Threats
X-Force Premium: Internal Host Communicating with Malware URL	Threats
UBA: Account or Group or Privileges Added	**User Behavioural Analytics**
UBA: Account or Group or Privileges Modified	User Behavioural Analytics
UBA: Anomalous Account Created from New Location	User Behavioural Analytics
UBA: Anomalous Cloud Account Created from New Location	User Behavioural Analytics
UBA: Browsed to Business/Service Website	User Behavioural Analytics
UBA: Browsed to Communication Website	User Behavioural Analytics
UBA: Browsed to Entertainment Website	User Behavioural Analytics
UBA: Browsed to Gambling Website	User Behavioural Analytics
UBA: Browsed to Information Technology Website	User Behavioural Analytics
UBA: Browsed to Job Search Website	User Behavioural Analytics
UBA: Browsed to Lifestyle Website	User Behavioural Analytics
UBA: Browsed to Malicious Website	User Behavioural Analytics
UBA: Browsed to Mixed Content/Potentially Adult Website	User Behavioural Analytics
UBA: Browsed to Phishing Website	User Behavioural Analytics
UBA: Browsed to Pornography Website	User Behavioural Analytics
UBA: Browsed to Scam/Questionable/Illegal Website	User Behavioural Analytics
UBA: Browsed to Uncategorised Website	User Behavioural Analytics
UBA: Bruteforce Authentication Attempts	User Behavioural Analytics
UBA: Common Exploit Tool Detected	User Behavioural Analytics
UBA: Common Exploit Tool Detected (Asset)	User Behavioural Analytics
UBA: Create Offense	User Behavioural Analytics
UBA: Critical Systems Users Seen Update	User Behavioural Analytics

List of Threats

UBA: D/DoS Attack Detected	User Behavioural Analytics
UBA: Detect Insecure or Non-Standard Protocol	User Behavioural Analytics
UBA: Detect IOC's For Locky	User Behavioural Analytics
UBA: Detect IOC's for WannaCry	User Behavioural Analytics
UBA: Detect Persistent SSH Session	User Behavioural Analytics
UBA: Dormant Account Found (privileged)	User Behavioural Analytics
UBA: Dormant Account Used	User Behavioural Analytics
UBA: Executive Only Asset Accessed by Non-Executive User	User Behavioural Analytics
UBA: Expired Account Used	User Behavioural Analytics
UBA: First Privileged Escalation	User Behavioural Analytics
UBA: High Risk User Access to Critical Asset	User Behavioural Analytics
UBA: Honeytoken Activity	User Behavioural Analytics
UBA: Internet Settings Modified	User Behavioural Analytics
UBA: Kerberos Account Mapping	User Behavioural Analytics
UBA: Large Outbound Transfer by Hugh Risk User	User Behavioural Analytics
UBA: Malicious Process Detected	User Behavioural Analytics
UBA: Malware Activity - Registry Modified in Bulk	User Behavioural Analytics
UBA: Multiple Kerberos Authentication Failures from Same User	User Behavioural Analytics
UBA: Multiple VPN Accounts Failed Login from Single IP.	User Behavioural Analytics
UBA: Multiple VPN Accounts Logged in From Single IP	User Behavioural Analytics
UBA: Netcast Process Detection (Linux)	User Behavioural Analytics
UBA: Netcast Process Detection (Windows)	User Behavioural Analytics
UBA: Network Share Accessed	User Behavioural Analytics
UBA: Network Traffic: Capture, Monitoring and Analysis Program Usage	User Behavioural Analytics
UBA: New Account Use Detected	User Behavioural Analytics
UBA: Non-Admin Access to Domain Controller	User Behavioural Analytics
UBA: Pash the Hash	User Behavioural Analytics
UBA: Populate Authorized Applications	User Behavioural Analytics
UBA: Populate Multiple VPN Accounts Failed Login from Single IP	User Behavioural Analytics
UBA: Populate Multiple VPN Accounts Logged in From Single IP	User Behavioural Analytics
UBA: Populate Process Filenames	User Behavioural Analytics
UBA: Possible TGT Forgery	User Behavioural Analytics
UBA: Potential Access to Blacklist Domain	User Behavioural Analytics
UBA: Potential Access to DGA Domain	User Behavioural Analytics
UBA: Potential Access to Squatting Domain	User Behavioural Analytics
UBA: Potential Access to Tunnelling Domain	User Behavioural Analytics
UBA: Process Creating Suspicious Remote Threads Detected (Asset)	User Behavioural Analytics
UBA: Process Executed Outside Gold Disk Whitelist (Linux)	User Behavioural Analytics
UBA: Process Executed Outside Gold Disk Whitelist (Windows)	User Behavioural Analytics
UBA: Ransomware Behaviour Detected	User Behavioural Analytics
UBA: Recent User Activity Update(privileged)	User Behavioural Analytics
UBA: Repeat Unauthorized Access	User Behavioural Analytics
UBA: Restricted Program Usage	User Behavioural Analytics
UBA: Shellbags Modified by Ransomware	User Behavioural Analytics
UBA: Subject_CN and Username Map Update	User Behavioural Analytics
UBA: Subject_CN and Username Mapping	User Behavioural Analytics
UBA: Suspicious Activities on Compromised Hosts	User Behavioural Analytics
UBA: Suspicious Activities on Compromised Hosts (Asset)	User Behavioural Analytics
UBA: Suspicious Administrative Activities Detected	User Behavioural Analytics
UBA: Suspicious Command Prompt Activity	User Behavioural Analytics
UBA: Suspicious Entries in System Registry (Asset)	User Behavioural Analytics
UBA: Suspicious Image Load Detected (Asset)	User Behavioural Analytics
UBA: Suspicious Pipe Activities (Asset)	User Behavioural Analytics
UBA: Suspicious PowerShell Activity	User Behavioural Analytics
UBA: Suspicious Privileged Activity (First Observed Privilege Use)	User Behavioural Analytics
UBA: Suspicious Privileged Activity (Rarely Used Privileged)	User Behavioural Analytics
UBA: Suspicious Scheduled Task Activities	User Behavioural Analytics
UBA: Suspicious Service Activities	User Behavioural Analytics
UBA: Suspicious Service Activities (Asset)	User Behavioural Analytics
UBA: TGT Ticket Used by Multiple Hosts	User Behavioural Analytics
UBA: Unauthorized Access	User Behavioural Analytics
UBA: UNIX/LINUX System Accessed With Service or Machine Account	User Behavioural Analytics

List of Threats

UBA: Unusual Scanning of Database Servers Detected	User Behavioural Analytics
UBA: Unusual Scanning of DHCP Servers Detected	User Behavioural Analytics
UBA: Unusual Scanning of DNS Servers Detected	User Behavioural Analytics
UBA: Unusual Scanning of FTP Servers Detected	User Behavioural Analytics
UBA: Unusual Scanning of Game Servers Detected	User Behavioural Analytics
UBA: Unusual Scanning of Generic ICMP Detected	User Behavioural Analytics
UBA: Unusual Scanning of Generic TCP Detected	User Behavioural Analytics
UBA: Unusual Scanning of Generic UDP Detected	User Behavioural Analytics
UBA: Unusual Scanning of IRC Servers Detected	User Behavioural Analytics
UBA: Unusual Scanning of LDAP Servers Detected	User Behavioural Analytics
UBA: Unusual Scanning of Mail Servers Detected	User Behavioural Analytics
UBA: Unusual Scanning of Messaging Servers Detected	User Behavioural Analytics
UBA: Unusual Scanning of P2P Servers Detected	User Behavioural Analytics
UBA: Unusual Scanning of Proxy Servers Detected	User Behavioural Analytics
UBA: Unusual Scanning of RPC Servers Detected	User Behavioural Analytics
UBA: Unusual Scanning of SNMP Servers Detected	User Behavioural Analytics
UBA: Unusual Scanning of SSH Servers Detected	User Behavioural Analytics
UBA: Unusual Scanning of Web Servers Detected	User Behavioural Analytics
UBA: Unusual Scanning of Windows Servers Detected	User Behavioural Analytics
UBA: User Access - Failed Access to Critical Assets	User Behavioural Analytics
UBA: User Access - First Access to Critical Assets	User Behavioural Analytics
UBA: User Access Control Bypass Detected (Asset)	User Behavioural Analytics
UBA: User Access from Multiple Locations	User Behavioural Analytics
UBA: User Access from Prohibited Locations	User Behavioural Analytics
UBA: User Access from Restricted Locations	User Behavioural Analytics
UBA: User Access Login Anomaly	User Behavioural Analytics
UBA: User Access to Internal Server from Jump Server	User Behavioural Analytics
UBA: User Accessing Account from Anonymous Source	User Behavioural Analytics
UBA: User Accessing Risky IP, Anonymization	User Behavioural Analytics
UBA: User Accessing Risky IP, Botnet	User Behavioural Analytics
UBA: User Accessing Risky IP, Dynamic	User Behavioural Analytics
UBA: User Accessing Risky IP, Malware,	User Behavioural Analytics
UBA: User Accessing Risky IP, Spam	User Behavioural Analytics
UBA: User Accessing Risky URL	User Behavioural Analytics
UBA: User Account Created and Deleted in a Short Period of Time	User Behavioural Analytics
UBA: User Attempt to Use a Suspended Account	User Behavioural Analytics
UBA: User Geography Change	User Behavioural Analytics
UBA: User Geography Map	User Behavioural Analytics
UBA: User Geography, Access from Unusual Locations	User Behavioural Analytics
UBA: User Installing Suspicious Application	User Behavioural Analytics
UBA: User Running New Process	User Behavioural Analytics
UBA: User Time, Access at Unusual Times	User Behavioural Analytics
UBA: Username to User Accounts, Privileged, Observed	User Behavioural Analytics
UBA: Username to User Accounts, Successful, Dormant	User Behavioural Analytics
UBA: Username to User Accounts, Successful, Observed	User Behavioural Analytics
UBA: Username to User Accounts, Successful, Recent	User Behavioural Analytics
UBA: Username to User Accounts, Successful, Recent Update	User Behavioural Analytics
UBA: Volume Shadow Copy Created	User Behavioural Analytics
UBA: VPN Access By Service or Machine Account	User Behavioural Analytics
UBA: VPN Certificate Sharing	User Behavioural Analytics
UBA: Windows Access with Service or Machine Account	User Behavioural Analytics
X-Force Risky URL	User Behavioural Analytics
Time Device Unreachable	**Other**
Vulnerabilitised: Vulnerability Reported by Scanner	Other
Whitelist IP	Other
Whitelist Log Source	Other
Whitelist Log Source 2	Other
Petya Detected in Real Time	Other
Wcry Detect	Other