TIME Security Advanced Monitoring

Security

1800-18-2828 | www.time.com.my

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
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 Againts 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
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

List of Threats

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

List of Threats

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