



# Service and Application Events

CYBER INCIDENT RESPONSE

## Service/Application Events

- Services and Applications should be monitored per good ITSM processes
  - Are they up/down?
  - Are they responding properly?
  - Are they functioning properly?
  - Are they conducting transactions properly?
  - Are they logging properly?



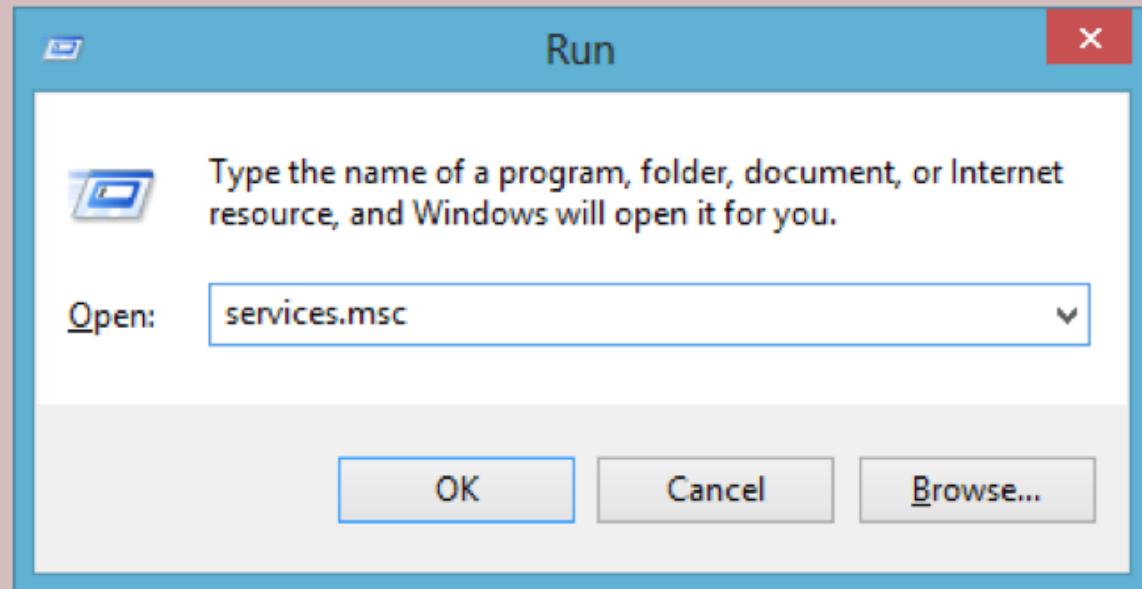
# Service Anomalies

- Non-security issues:
  - Authentication errors
  - Permission issues
  - Services don't start on boot up
  - Service failures
- Investigate the issue to ensure it is not security related
- Use antivirus, antimalware, file integrity checking, and whitelisting to verify



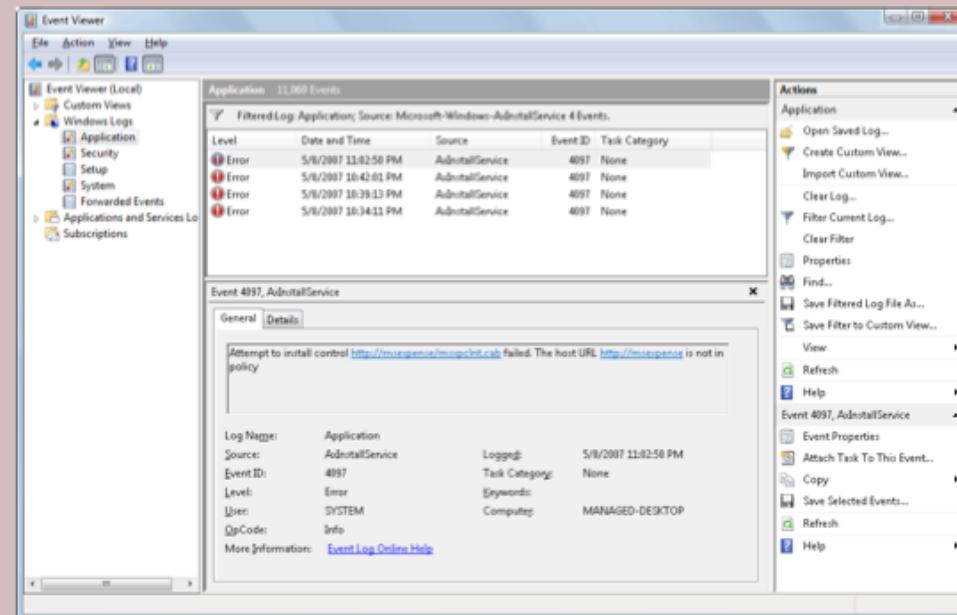
# Checking Service Status

- Windows:
  - services.msc (GUI) or sc (command line)
- Linux:
  - service –status-all (command line)



# Service/Application Logs

- Windows:
  - Use Windows Event Viewer to view Application Logs
- Linux:
  - Log to the /var/log directory
  - Use tail to view the end of the log files



# Service/Application Behavior

- Create and understand a baseline
- Log/alert on anything outside of baseline

McAfee Host Intrusion Prevention

Task Edit View Help

IPS Policy | Evasion Policy | Application Policy | Blocked Hosts | Application Protection Log | Activity Log |

Use this tab to view activity logs.

Traffic Logging

Log All Blocked

Traffic

Applications

Ignores

Filter Options

Time	Event	IP Address/User	Application	Message
7/12/2010 3:12:32 PM	Traffic	15.255.101.110	HP SUM Source Repository Client (SourceClient)	Blocked Incoming TCP - Source 15.255.101.110 : (46089) Destination 15.255.146.195 : http (80)
7/12/2010 3:12:38 PM	Traffic	15.255.101.110	HP SUM Source Repository Client (SourceClient)	Blocked Incoming TCP - Source 15.255.101.110 : (46089) Destination 15.255.146.195 : http (80)
7/12/2010 3:12:50 PM	Traffic	15.255.101.110	HP SUM Source Repository Client (SourceClient)	Blocked Incoming TCP - Source 15.255.101.110 : (46089) Destination 15.255.146.195 : http (80)
7/12/2010 3:13:14 PM	Traffic	15.255.101.110	HP SUM Source Repository Client (SourceClient)	Blocked Incoming TCP - Source 15.255.101.110 : (46089) Destination 15.255.146.195 : http (80)
7/12/2010 4:44:37 PM	Traffic	15.8.144.78	Host Process for Windows Services (svchost)	Blocked Incoming UDP - Source 15.8.144.78 : (1230) Destination 15.8.151.255 : ntp (123)
7/13/2010 1:00:55 PM	Traffic	15.255.101.110	HP SUM Source Repository Client (SourceClient)	Blocked Incoming TCP - Source 15.255.101.110 : (61323) Destination 15.255.146.195 : http (80)
7/13/2010 1:00:58 PM	Traffic	15.255.101.110	HP SUM Source Repository Client (SourceClient)	Blocked Incoming TCP - Source 15.255.101.110 : (61323) Destination 15.255.146.195 : http (80)
7/13/2010 1:01:04 PM	Traffic	15.255.101.110	HP SUM Source Repository Client (SourceClient)	Blocked Incoming TCP - Source 15.255.101.110 : (61323) Destination 15.255.146.195 : http (80)
7/13/2010 1:01:16 PM	Traffic	15.255.101.110	HP SUM Source Repository Client (SourceClient)	Blocked Incoming TCP - Source 15.255.101.110 : (61323) Destination 15.255.146.195 : http (80)
7/13/2010 1:01:40 PM	Traffic	15.255.101.110	HP SUM Source Repository Client (SourceClient)	Blocked Incoming TCP - Source 15.255.101.110 : (61323) Destination 15.255.146.195 : http (80)
7/13/2010 1:03:32 PM	Traffic	15.255.101.110	HP SUM Source Repository Client (SourceClient)	Blocked Incoming TCP - Source 15.255.101.110 : (43000) Destination 15.255.146.195 : http (80)
7/13/2010 1:03:35 PM	Traffic	15.255.101.110	HP SUM Source Repository Client (SourceClient)	Blocked Incoming TCP - Source 15.255.101.110 : (43000) Destination 15.255.146.195 : http (80)
7/13/2010 1:03:41 PM	Traffic	15.255.101.110	HP SUM Source Repository Client (SourceClient)	Blocked Incoming TCP - Source 15.255.101.110 : (43000) Destination 15.255.146.195 : http (80)
7/13/2010 1:03:53 PM	Traffic	15.255.101.110	HP SUM Source Repository Client (SourceClient)	Blocked Incoming TCP - Source 15.255.101.110 : (43000) Destination 15.255.146.195 : http (80)
7/13/2010 1:04:17 PM	Traffic	15.255.101.110	HP SUM Source Repository Client (SourceClient)	Blocked Incoming TCP - Source 15.255.101.110 : (43000) Destination 15.255.146.195 : http (80)

Host IPS is enabled, Network IPS is enabled



# Service/Application Attacks

- Anomalous Activity
  - Doesn't match the typical behavior
  - Investigate the activity and solve
- New Accounts
  - Were they authorized?
  - Do they have excessive permissions?
- Unexpected Output
  - Improper output or garbage output
  - User and admin training imperative to determining the root cause



# Service/Application Attacks

- Unexpected outbound communication
  - Why is the application sending out data?
  - Detect with network monitoring
- Service Interruption
  - Simple issue or a DDoS?
  - Monitoring tools can help determine reason
- Memory Overflows
  - Causes OS errors and crashes
  - Monitoring for them is hard
  - Detecting after a crash is easier

