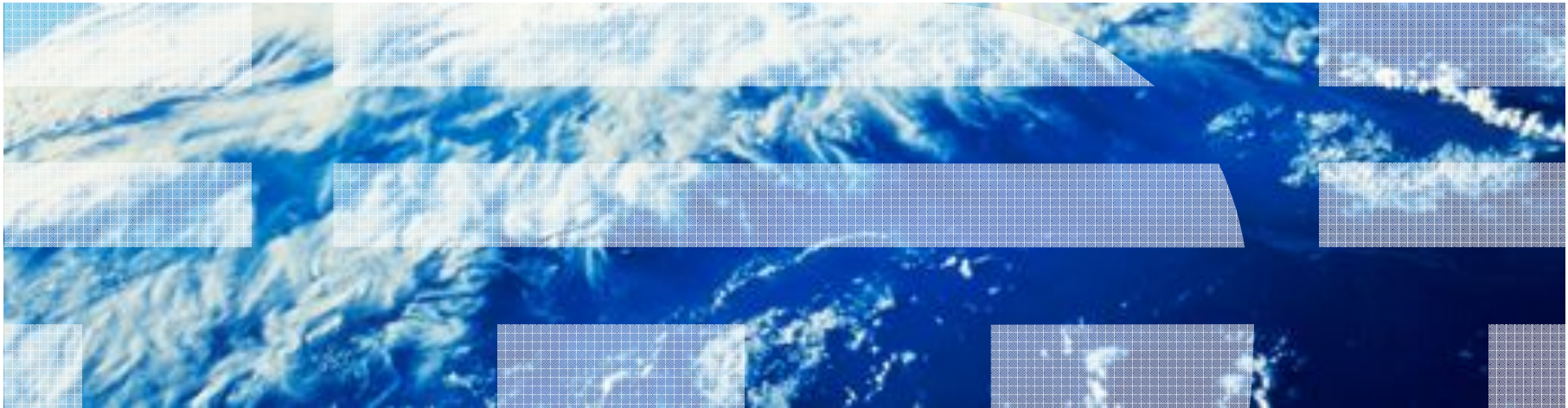
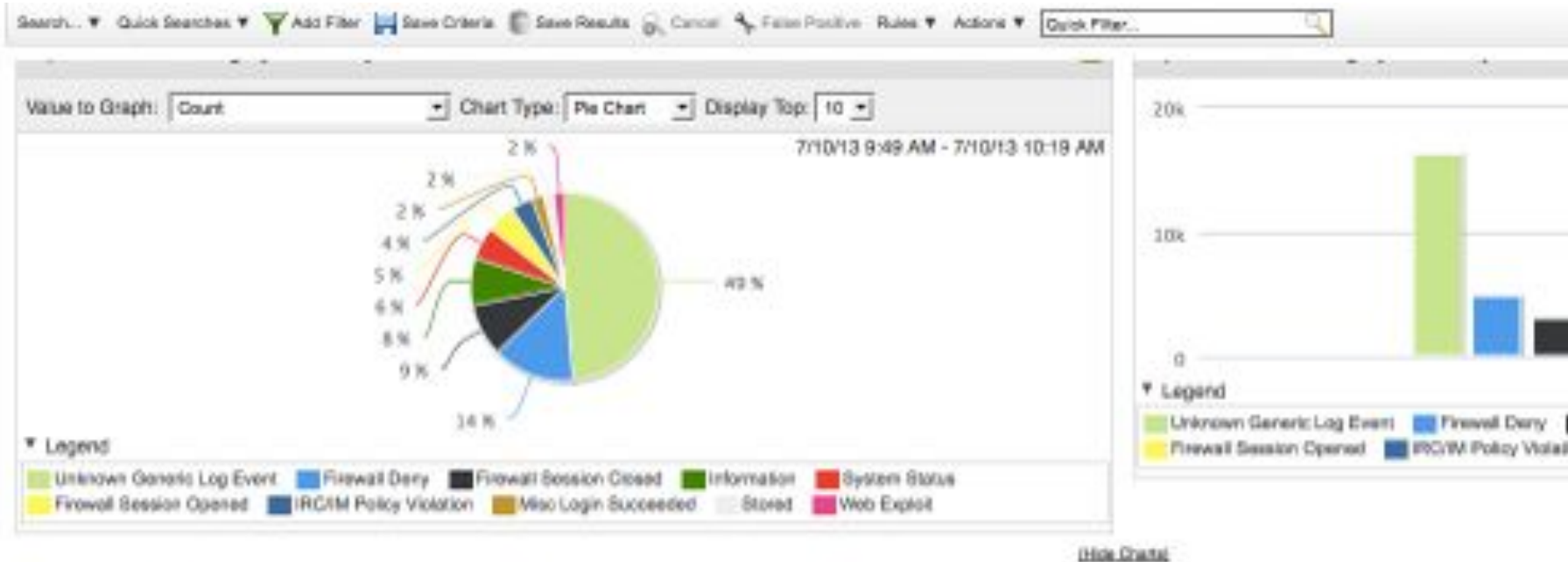


# All Things NBAD



# Today



Low Level Category	Source IP (Unique Count)	Destination IP (Unique Count)	Destination Port (Unique Count)	Event Name (Unique Count)	Log Source (Unique Count)	Protocol (Unique Count)	Username (Unique Count)
Unknown Generic L...	Multiple (3)	Multiple (3)	0	Unknown log event	SIM Generic Log D...	other	N/A
Firewall Deny	Multiple (1,071)	Multiple (1,188)	Multiple (518)	Multiple (6)	Multiple (3)	Multiple (4)	Multiple (2)
Firewall Session Cl...	Multiple (357)	Multiple (344)	Multiple (26)	Multiple (3)	FWSM @ 1.1.1.6	Multiple (3)	N/A
Information	Multiple (15)	Multiple (2)	0	Multiple (4)	Multiple (2)	other	Multiple (10)
System Status	Multiple (2)	Multiple (2)	Multiple (6)	Multiple (9)	Multiple (2)	Multiple (2)	Multiple (94)
Firewall Session Op...	Multiple (86)	Multiple (2)	Multiple (622)	Multiple (2)	FWSM @ 1.1.1.6	Multiple (2)	N/A
IRC/M Policy Violat...	Multiple (118)	Multiple (25)	Multiple (3)	IRC Connections	Custom Rule Engin...	tcp_ip	N/A
Misc Login Succeed...	Multiple (33)	Multiple (3)	Multiple (2)	Multiple (4)	Multiple (2)	Multiple (2)	Multiple (85)

## Anomaly Rule

TYPE TO FIND

- when the average value (per interval) of this accumulated property over the last 1 min is at least percentage% different from the average value (per interval) of the same property over the last 1 min
- when the tested interval value is greater than or equal to 0
- when the date is between this date and this date
- when the day of the week is any of these selected days
- when the time of day is between this time and this time

Test the [Selected Accumulated Property] value of each Low Level Category separately.

Rule (Click on an underlined value to edit it)  
Invalid tests are highlighted and must be fixed before rule can be saved.

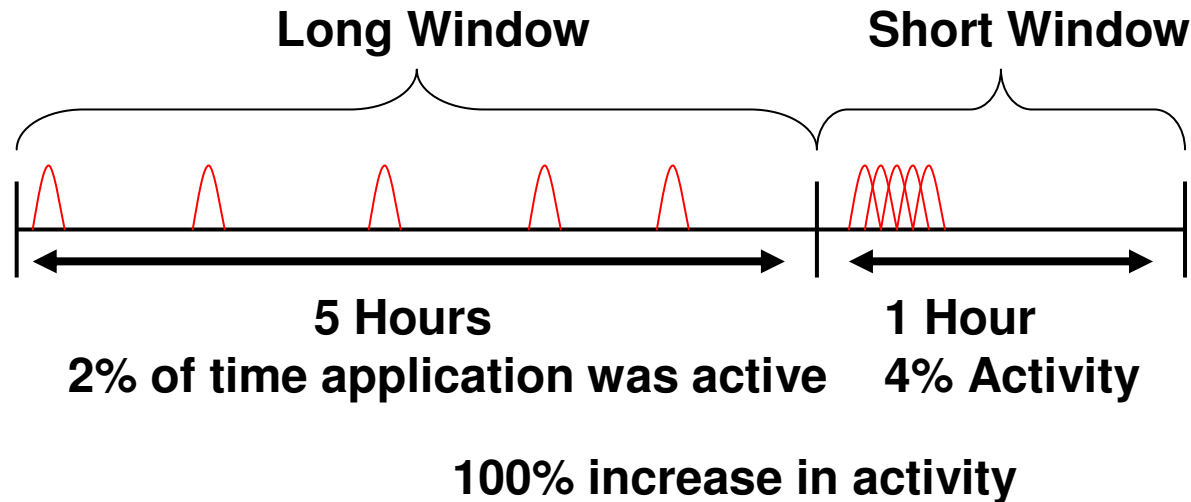
Apply (enter rule name here) when time series data is being aggregated by Low Level Category

and when the average value (per interval) of this accumulated property over the last 1 min is at least 40% different from the average value (per interval) of the same property over the last 24 hours

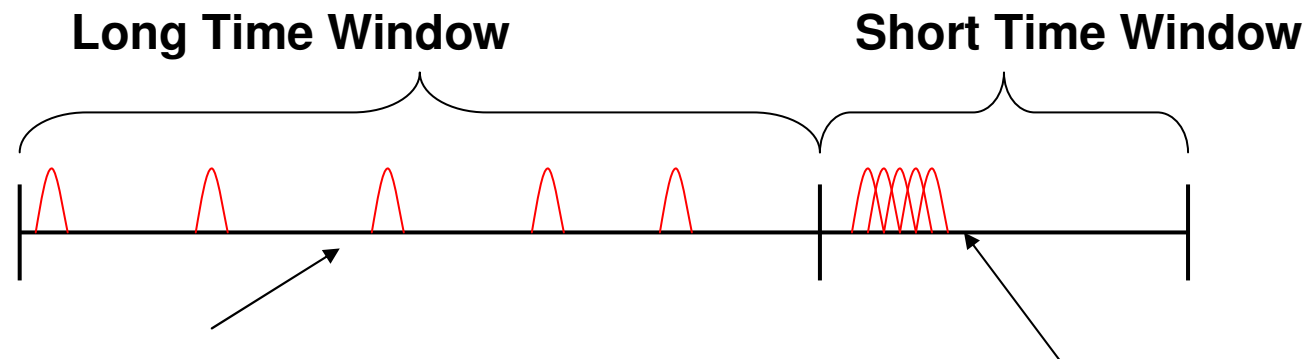
Please select any groups you would like this rule to be a member of:

- Anomaly
- Authentication

- Looks for obvious changes in traffic patterns, very good at catching
  - Sudden increase in traffic/event rates
  - Sudden decreases in traffic
  - New Traffic that has never been seen
- Large Window (Long Window):
- Short Window:
- % of Change required to alert



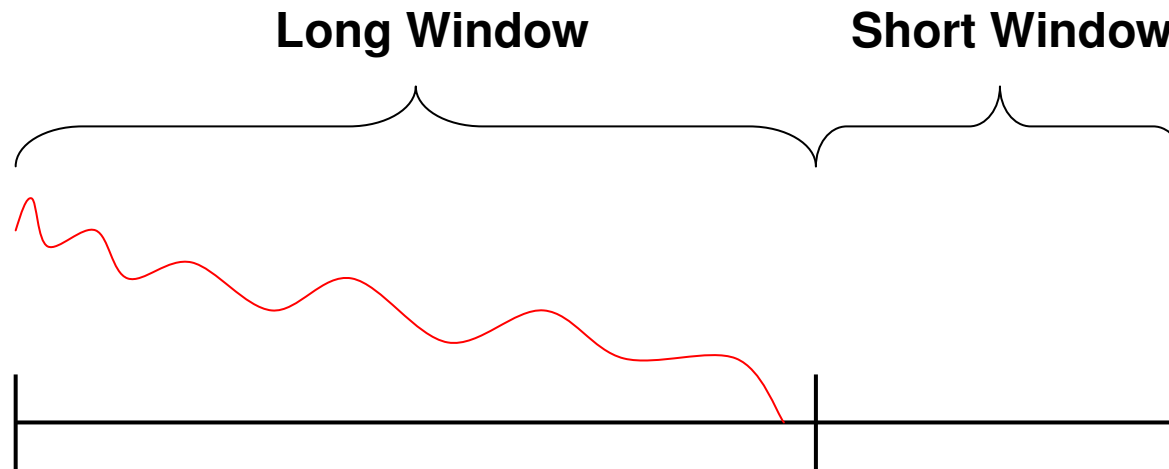
## Sudden Increase in Traffic Patterns



**Long Window: Defines Normal Behavior:**  
**Example: Over long window the cumulative average time SSH traffic is active is 2% of the time**

**Short Window: Comparison window average is compared against the long window average. In this case the short window shows 4% activity of SSH traffic. This 100% increase in volume triggers an event**

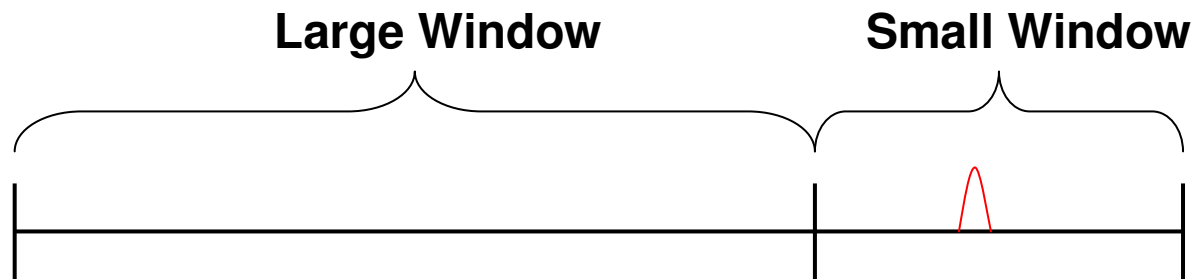
## Sudden Decrease in Traffic Patterns



**Type of Issues this could capture:**

- **Service DoS (i.e. business application stops responding to requests)**
- **Hardware Failure on critical asset: Web Server Died**

## New Traffic on the scene



- Type of Issues this could capture:**
- **New Service Installed on a server**
  - **Rogue Server Deployed**

# Threshold

**Rule Wizard - Rule Test Stack Editor**

Which threshold tests do you wish to perform on the time series data?

Test Group:

Type to filter

- when this accumulated property is greater than this value
- when this accumulated property is between this value and this value
- when the date is between this date and this date
- when the day of the week is any of these selected days
- when the time of day is between this time and this time

Select a comparator

- greater than
- less than
- equal to

Test the [Selected Accumulated Property] value of each Low Level Category separately.

Rule (Click on an underlined value to edit it)  
Invalid tests are highlighted and must be fixed before rule can be saved.

Apply  when time series data is being aggregated by Low Level Category

and when this accumulated property is greater than 0 (accumulated in 1 min intervals)



# Behavior

Test Group:

Type to filter

- when this accumulated property is the tested property
- when the importance of the current traffic level (on a scale of 0 to 100) is importance compared to learned traffic trends and behavior
- when the importance of the current traffic trend (on a scale of 0 to 100) is importance compared to learned traffic levels and behavior
- when the importance of the current traffic behavior (on a scale of 0 to 100) is importance compared to learned traffic levels and trends
- when the actual field value deviates by a margin of at least deviation% of the extrapolated (predicted) field value
- when the season length is a day
- when the tested interval value is greater than or equal to 0
- when the date is between this date and this date

Test the [Selected Accumulated Property] value of each Low Level Category separately.

Rule (Click on an underlined value to edit it)  
 Invalid tests are highlighted and must be fixed before rule can be saved.

Apply  when time series data is being aggregated by Low Level Category

- and when this accumulated property is the tested property
- and when the importance of the current traffic level (on a scale of 0 to 100) is 70 compared to learned traffic trends and behavior
- and when the importance of the current traffic trend (on a scale of 0 to 100) is 30 compared to learned traffic levels and behavior

Please select any groups you would like this rule to be a member of.

Exponential smoothing schemes weight past observations using exponentially decreasing weights. This is a very popular scheme to produce a smoothed Time Series. Whereas in Single Moving Averages the past observations are weighted equally, Exponential Smoothing assigns exponentially decreasing weights as the observations get older.

In other words, recent observations are given relatively more weight in forecasting than the older observations.