ULTIMATE WINDOWS SECURITY .COM

Integrating Splunk with native Windows Event Collection (WEC) and Optional 2-Stage Noise Filtering

Sponsored by

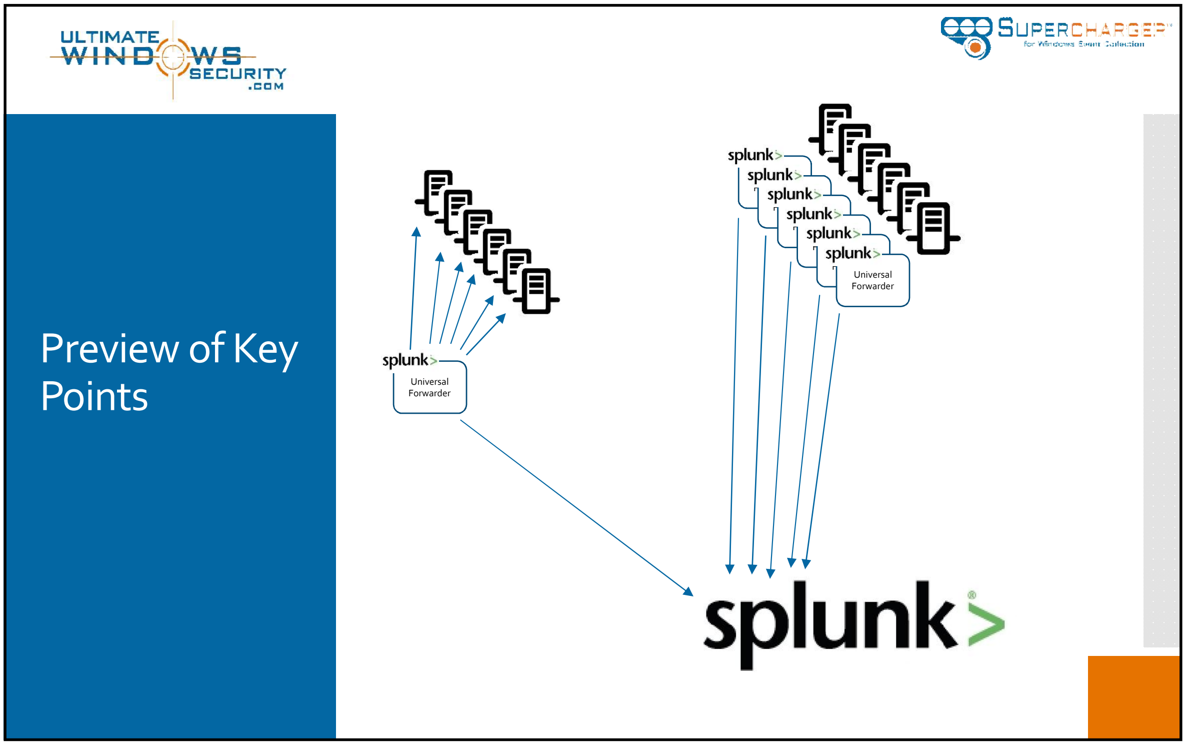
SUPERCHARGER for Windows Event Collection

ULTIMATE WINDOWS SECURITY .COM

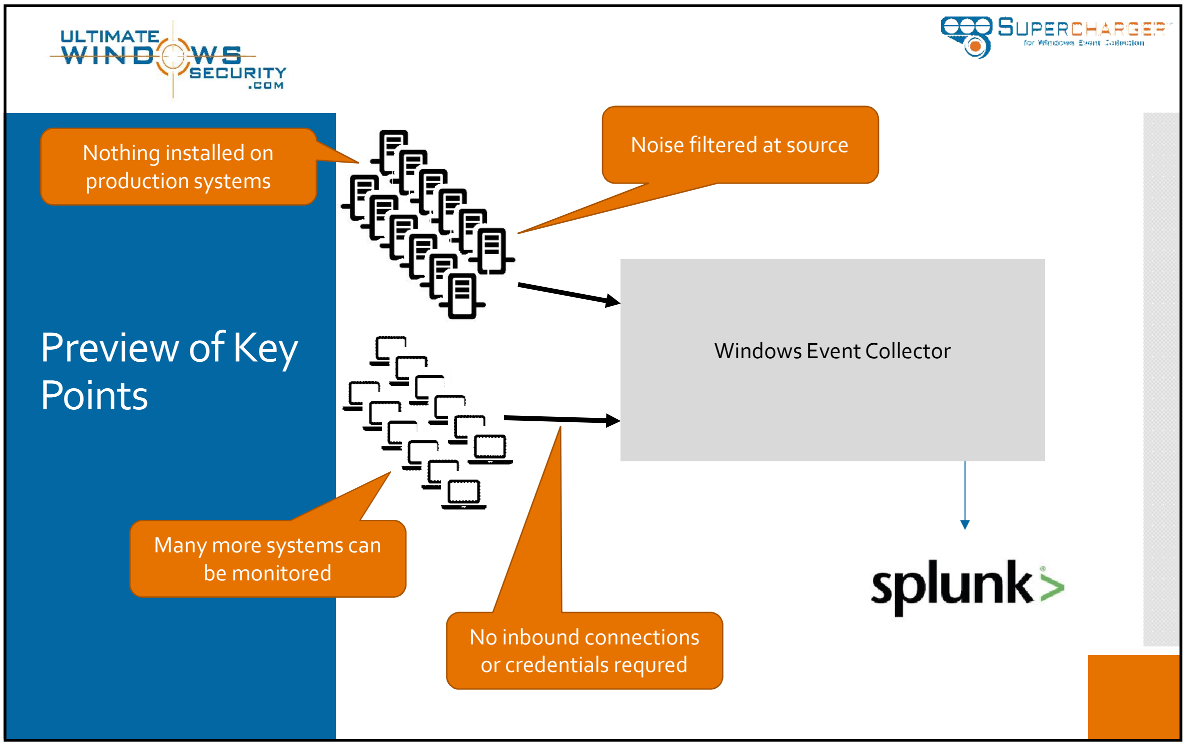
Thanks to

- Made possible by

SUPERCHARGER™ for Windows Event Collection



Preview of Key Points



ULTIMATE WINDOWS SECURITY .COM
SUPERCHARGER for Windows Event Collection
splunk>

Preview of Key Points

Nothing installed on production systems

Noise filtered at source

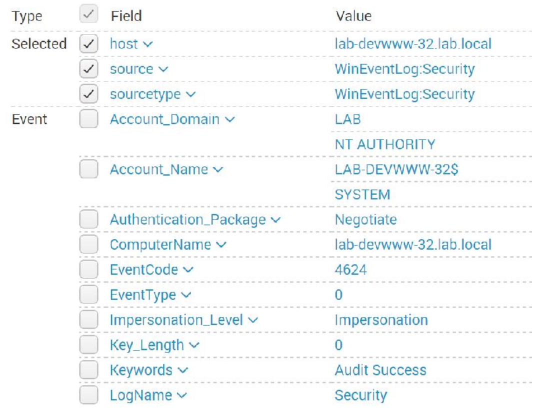
Windows Event Collector

Many more systems can be monitored

No inbound connections or credentials requred

Requirements

- **Existing Splunk Applications, searches, reports, filters should continue to work with forwarded events**
- **Forwarded** Events indexed by Splunk look **identical** to events collected **directly** by Splunk Universal Forwarder



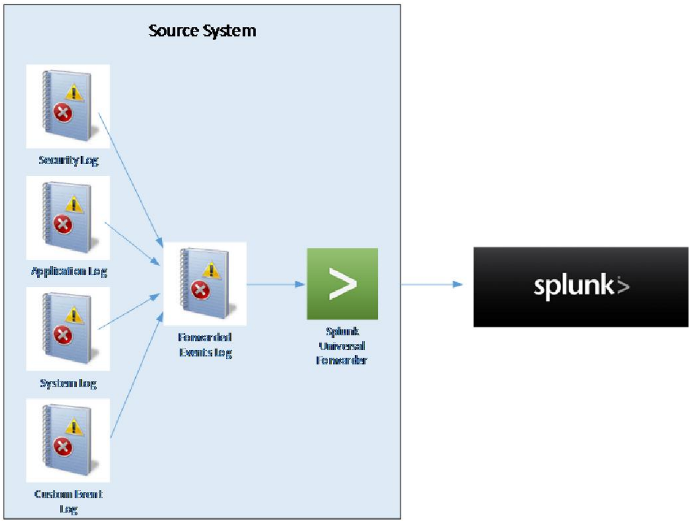
Type	✓	Field	Value
Selected	☑	host ⌄	lab-devwww-32.lab.local
	☑	source ⌄	WinEventLog:Security
	☑	sourcetype ⌄	WinEventLog:Security
Event	☐	Account_Domain ⌄	LAB NT AUTHORITY
	☐	Account_Name ⌄	LAB-DEVWWW-32$ SYSTEM
	☐	Authentication_Package ⌄	Negotiate
	☐	ComputerName ⌄	lab-devwww-32.lab.local
	☐	EventCode ⌄	4624
	☐	EventType ⌄	0
	☐	Impersonation_Level ⌄	Impersonation
	☐	Key_Length ⌄	0
	☐	Keywords ⌄	Audit Success
	☐	LogName ⌄	Security

Consuming forwarded events with Splunk

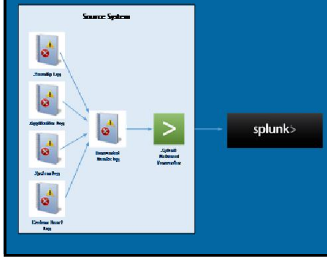
- Universal Forwarder makes assumptions by default about collected event logs
- Host, source and sourcetype misidentified which breaks log analysis

Problem: Multiple source logs to ForwardedEvents log to Splunk

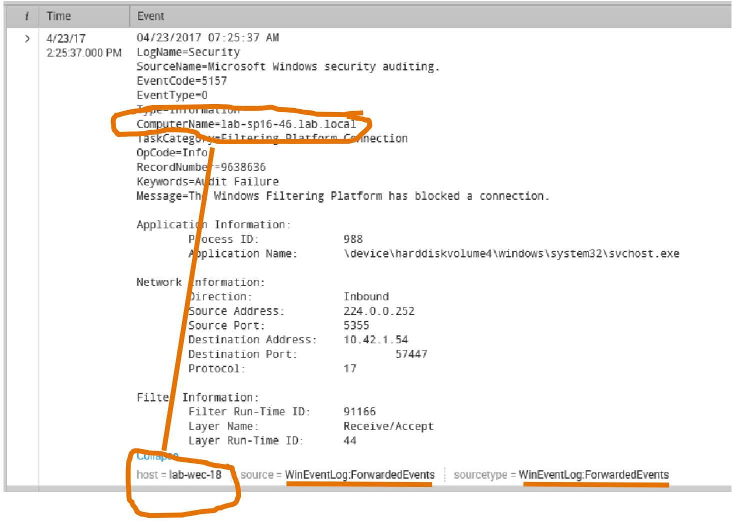
Scenario - The Forwarded Events log on the source system where the Universal Forwarder is installed contains events from various source computers (forwarders) and various logs from those systems.



Problem: Multiple source logs to ForwardedEvents log to Splunk



Issue - Splunk doesn't understand that forwarded events are from many different systems. It's failing to look at the Computer Name field in the event header



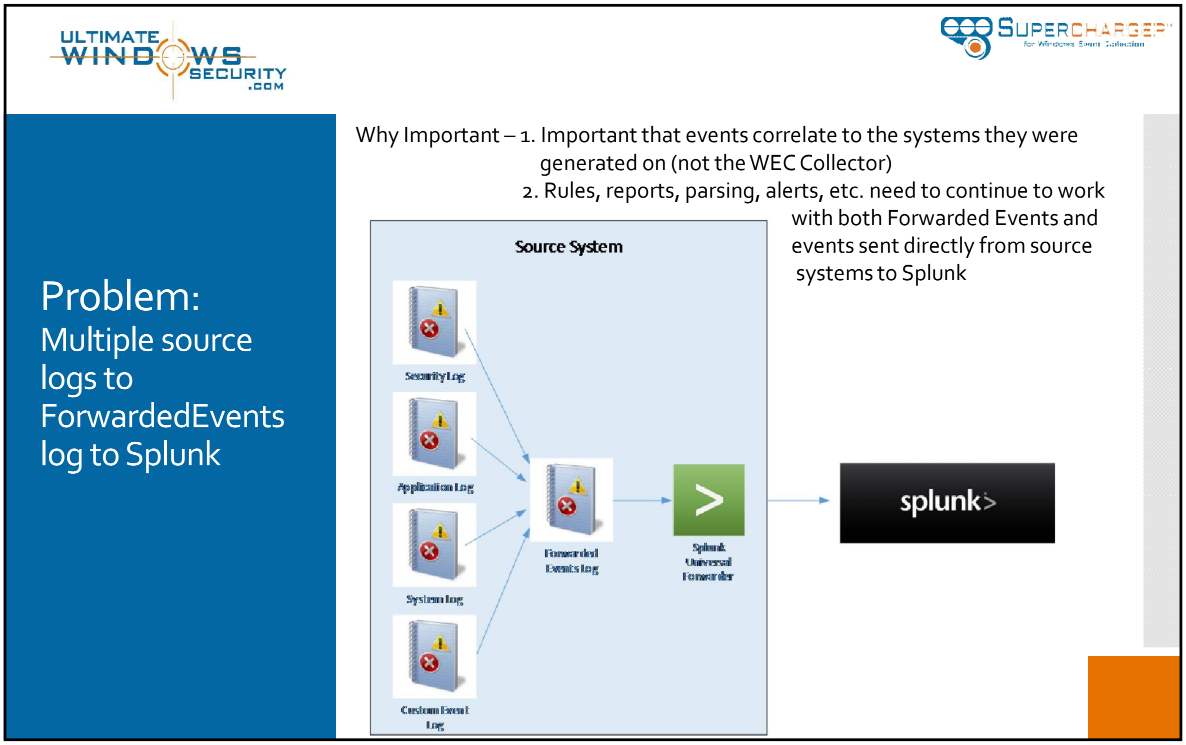
i	Time	Event

>	4/23/17
	2:25:37.000 PM
		04/23/2017 07:25:37 AM
		LogName=Security
		SourceName=Microsoft Windows security auditing.
		EventCode=5157
		EventType=0
		Type=Information
		ComputerName=lab-sp16-46.lab.local
		TaskCategory=Filtering Platform Connection
		OpCode=Info
		RecordNumber=9638636
		Keywords=Audit Failure
		Message=The Windows Filtering Platform has blocked a connection.

```
Application Information:
        Process ID:             988
        Application Name:       \device\harddiskvolume4\windows\system32\svchost.exe

Network Information:
        Direction:              Inbound
        Source Address:         224.0.0.252
        Source Port:            5355
        Destination Address:    10.42.1.54
        Destination Port:               57447
        Protocol:               17

Filter Information:
        Filter Run-Time ID:     91166
        Layer Name:             Receive/Accept
        Layer Run-Time ID:      44
Collapse
host = lab-wec-18   source = WinEventLog:ForwardedEvents   sourcetype = WinEventLog:ForwardedEvents
```

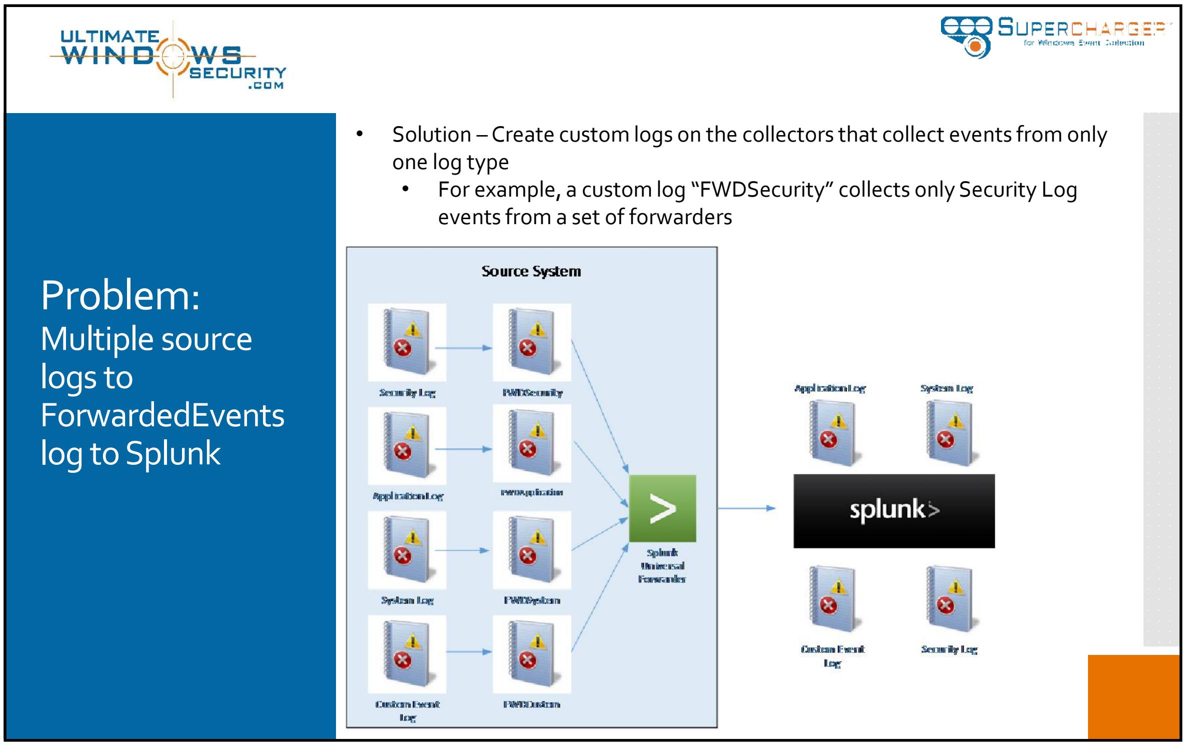


Problem:
Multiple source logs to ForwardedEvents log to Splunk

Why Important – 1. Important that events correlate to the systems they were generated on (not the WEC Collector)

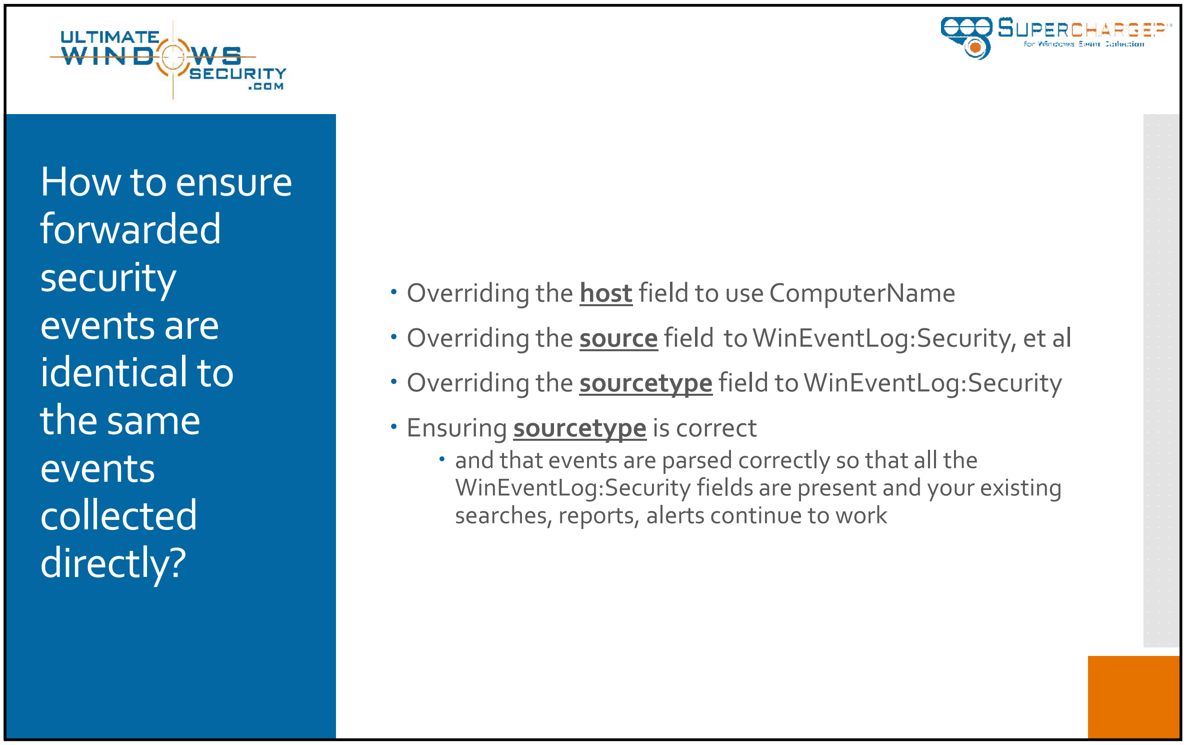
2. Rules, reports, parsing, alerts, etc. need to continue to work with both Forwarded Events and events sent directly from source systems to Splunk

ULTIMATE WINDOWS SECURITY .COM
SUPERCHARGER for Windows Event Collection
Source System
Security Log
Application Log
System Log
Custom Event Log
Forwarded Events Log
Splunk Universal Forwarder
splunk>



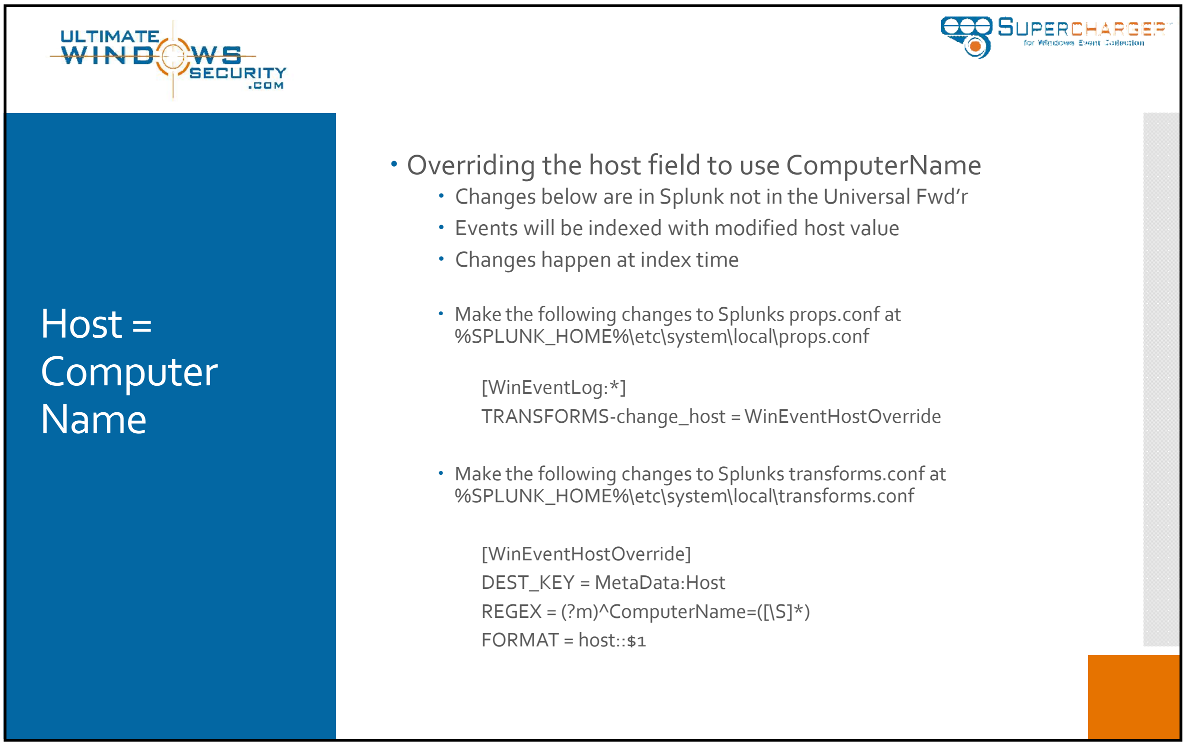
Problem:
Multiple source logs to ForwardedEvents log to Splunk

- Solution – Create custom logs on the collectors that collect events from only one log type
  - For example, a custom log “FWDSecurity” collects only Security Log events from a set of forwarders



How to ensure forwarded security events are identical to the same events collected directly?

- Overriding the **host** field to use ComputerName
- Overriding the **source** field to WinEventLog:Security, et al
- Overriding the **sourcetype** field to WinEventLog:Security
- Ensuring **sourcetype** is correct
  - and that events are parsed correctly so that all the WinEventLog:Security fields are present and your existing searches, reports, alerts continue to work



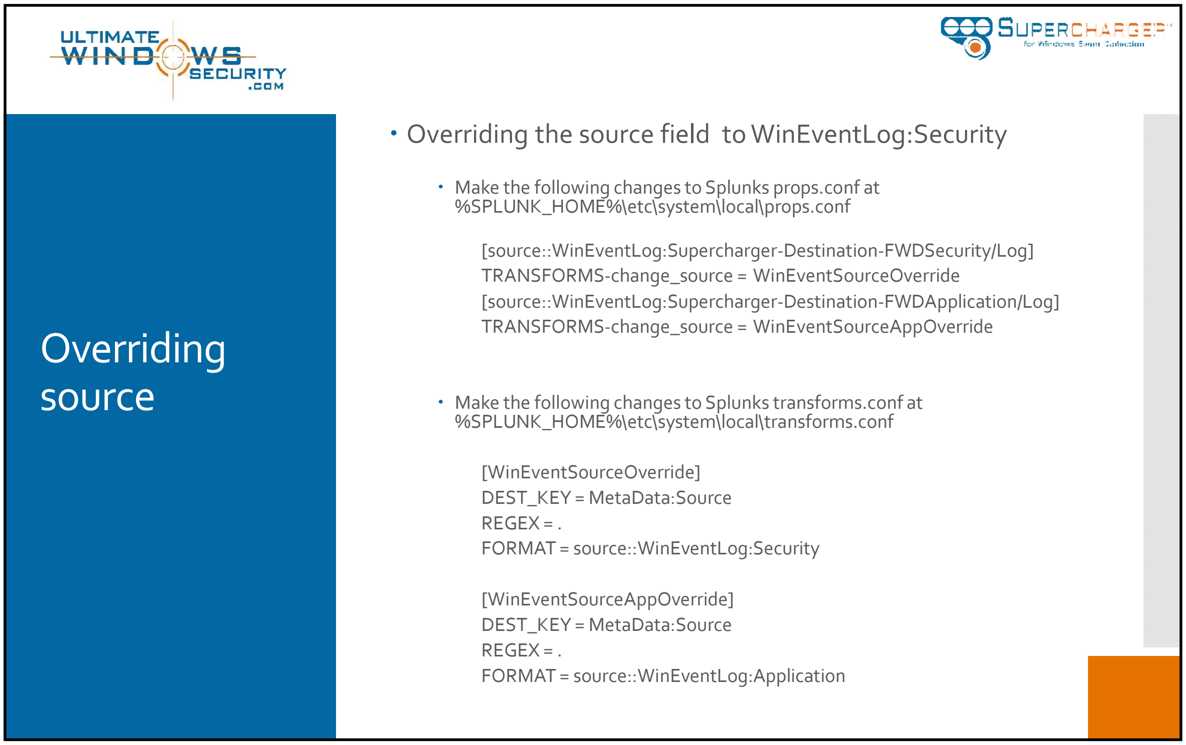
Host = Computer Name

- Overriding the host field to use ComputerName
  - Changes below are in Splunk not in the Universal Fwd'r
  - Events will be indexed with modified host value
  - Changes happen at index time
  - Make the following changes to Splunks props.conf at %SPLUNK_HOME%\etc\system\local\props.conf

```
[WinEventLog:*]
TRANSFORMS-change_host = WinEventHostOverride
```

  - Make the following changes to Splunks transforms.conf at %SPLUNK_HOME%\etc\system\local\transforms.conf

```
[WinEventHostOverride]
DEST_KEY = MetaData:Host
REGEX = (?m)^ComputerName=([\S]*)
FORMAT = host::$1
```



Overriding source

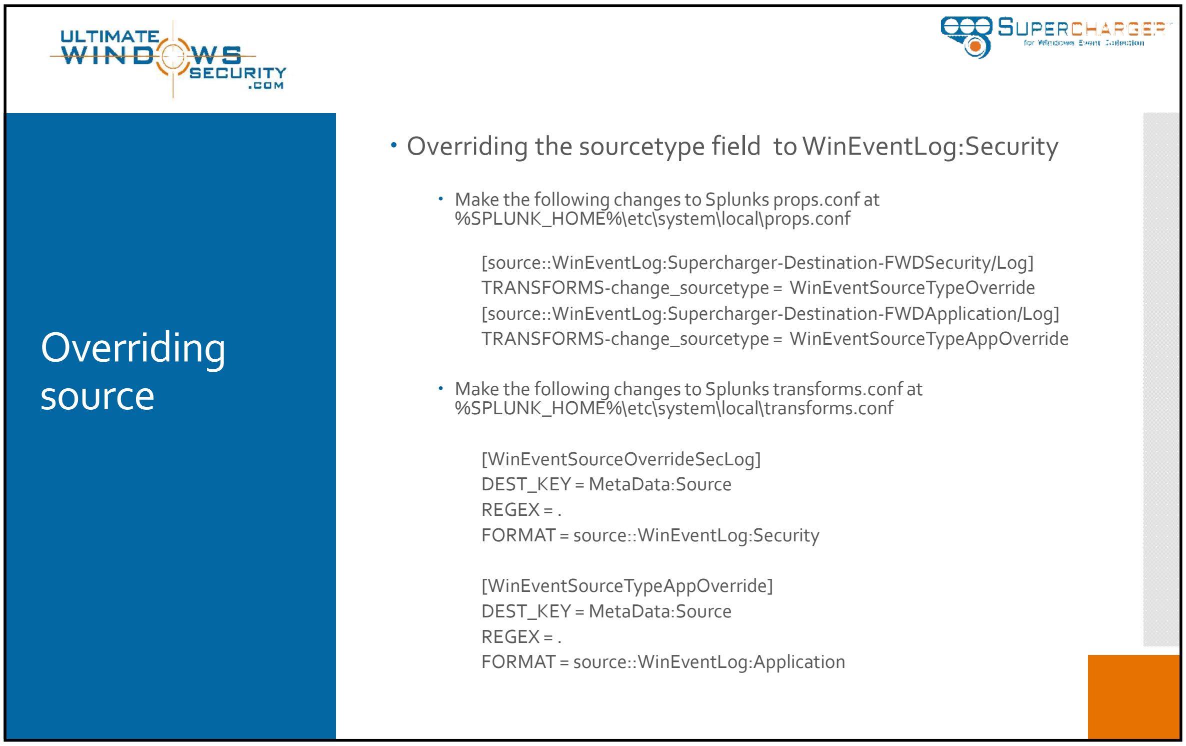
- Overriding the source field to WinEventLog:Security
  - Make the following changes to Splunks props.conf at %SPLUNK_HOME%\etc\system\local\props.conf

```
[source::WinEventLog:Supercharger-Destination-FWDSecurity/Log]
TRANSFORMS-change_source = WinEventSourceOverride
[source::WinEventLog:Supercharger-Destination-FWDApplication/Log]
TRANSFORMS-change_source = WinEventSourceAppOverride
```

  - Make the following changes to Splunks transforms.conf at %SPLUNK_HOME%\etc\system\local\transforms.conf

```
[WinEventSourceOverride]
DEST_KEY = MetaData:Source
REGEX = .
FORMAT = source::WinEventLog:Security

[WinEventSourceAppOverride]
DEST_KEY = MetaData:Source
REGEX = .
FORMAT = source::WinEventLog:Application
```



Overriding source

- Overriding the sourcetype field to WinEventLog:Security
  - Make the following changes to Splunks props.conf at %SPLUNK_HOME%\etc\system\local\props.conf

```
[source::WinEventLog:Supercharger-Destination-FWDSecurity/Log]
TRANSFORMS-change_sourcetype = WinEventSourceTypeOverride
[source::WinEventLog:Supercharger-Destination-FWDApplication/Log]
TRANSFORMS-change_sourcetype = WinEventSourceTypeAppOverride
```

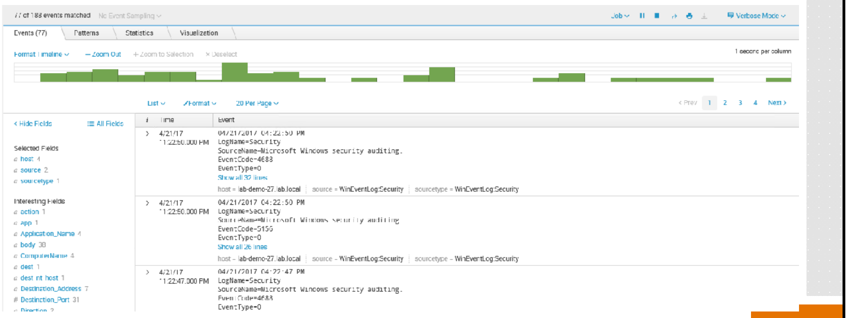
  - Make the following changes to Splunks transforms.conf at %SPLUNK_HOME%\etc\system\local\transforms.conf

```
[WinEventSourceOverrideSecLog]
DEST_KEY = MetaData:Source
REGEX = .
FORMAT = source::WinEventLog:Security

[WinEventSourceTypeAppOverride]
DEST_KEY = MetaData:Source
REGEX = .
FORMAT = source::WinEventLog:Application
```

Overriding sourcetype

- Ensuring sourcetype is correct and that events are parsed correctly so that all the WinEventLog:Security fields are present and your existing searches, reports, alerts continue to work
  - A quick check is to search the destination index in verbose mode and to visually verify that the fields are listed on the left side.



77 of 188 events matched   No Event Sampling ⌄   Job ⌄   Verbose Mode ⌄

Events (77)   Patterns   Statistics   Visualization

Format Timeline ⌄   — Zoom Out   + Zoom to Selection   × Deselect   1 second per column

List ⌄   Format ⌄   20 Per Page ⌄   < Prev 1 2 3 4 Next >

< Hide Fields   ☰ All Fields

Selected Fields
- a host 4
- a source 2
- a sourcetype 1

Interesting Fields
- a action 1
- a app 1
- a Application_Name 4
- a body 38
- a ComputerName 4
- a dest 1
- a dest_nt_host 1
- a Destination_Address 7
- # Destination_Port 31
- a Direction 2

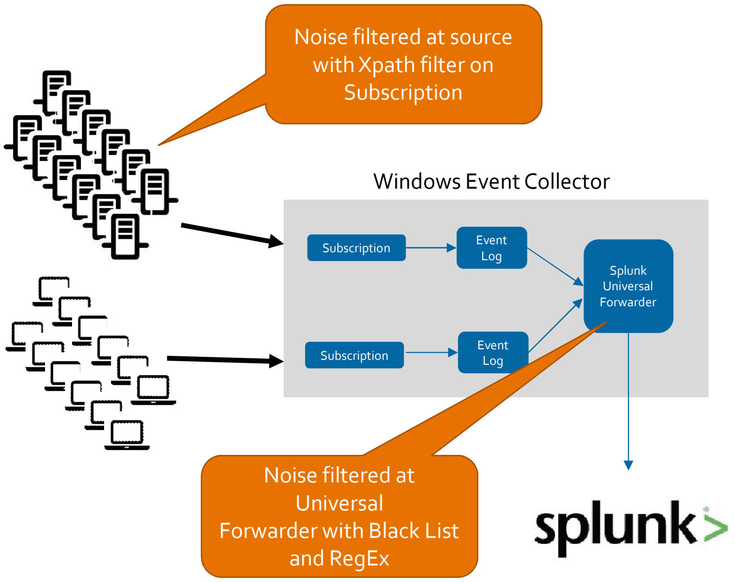
i	Time	Event

>	4/21/17
	11:22:50.000 PM
		04/21/2017 04:22:50 PM
		LogName=Security
		SourceName=Microsoft Windows security auditing.
		EventCode=4688
		EventType=0
		Show all 32 lines
		host = lab-demo-27.lab.local source = WinEventLog:Security sourcetype = WinEventLog:Security

>	4/21/17
	11:22:50.000 PM
		04/21/2017 04:22:50 PM
		LogName=Security
		SourceName=Microsoft Windows security auditing
		EventCode=5156
		EventType=0
		Show all 26 lines
		host = lab-demo-27.lab.local source = WinEventLog:Security sourcetype = WinEventLog:Security

>	4/21/17
	11:22:47.000 PM
		04/21/2017 04:22:47 PM
		LogName=Security
		SourceName=Microsoft Windows security auditing.
		EventCode=4688
		EventType=0

2-level noise filtering



Noise filtered at source with Xpath filter on Subscription

Windows Event Collector

Subscription → Event Log

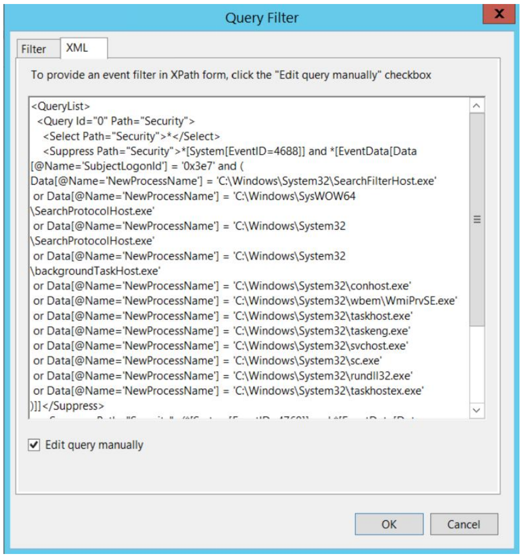
Subscription → Event Log

Splunk Universal Forwarder

Noise filtered at Universal Forwarder with Black List and RegEx

splunk>

Level 1 – WEC Subscription Xpath filters



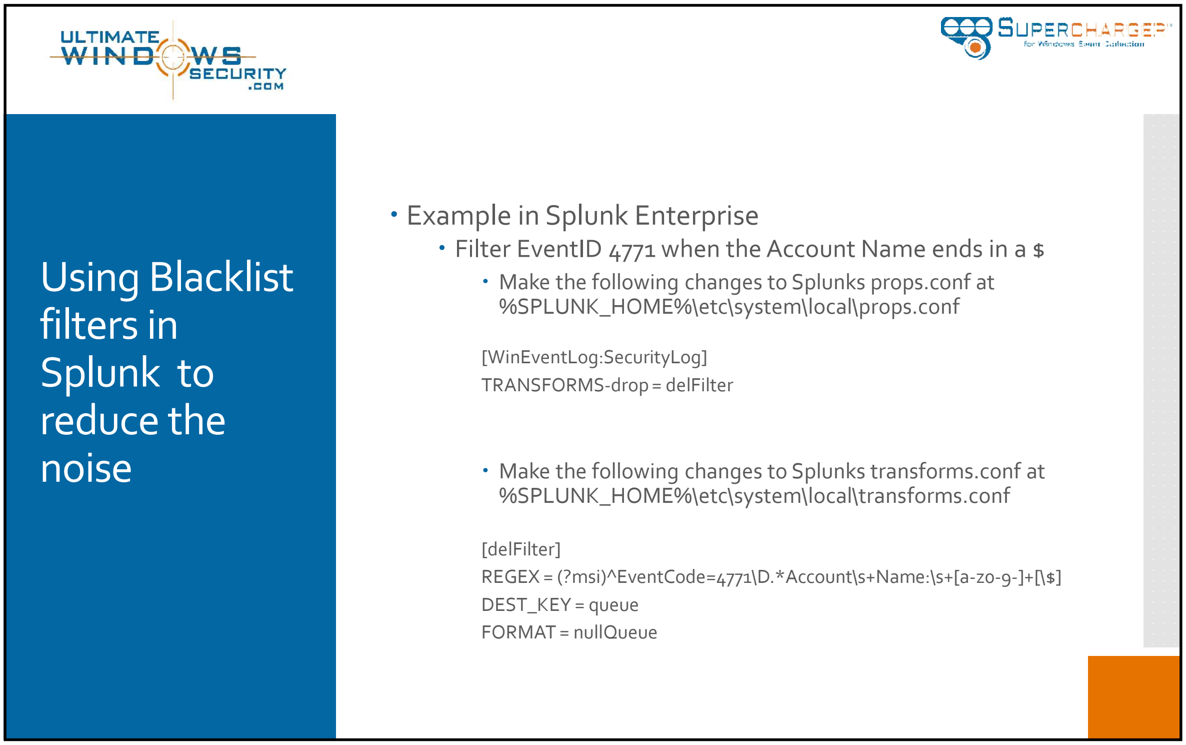
To provide an event filter in XPath form, click the "Edit query manually" checkbox

```
<QueryList>
  <Query Id="0" Path="Security">
    <Select Path="Security">*</Select>
    <Suppress Path="Security">*[System[EventID=4688]] and *[EventData[Data
[@Name='SubjectLogonId'] = '0x3e7' and (
Data[@Name='NewProcessName'] = 'C:\Windows\System32\SearchFilterHost.exe'
 or Data[@Name='NewProcessName'] = 'C:\Windows\SysWOW64
\SearchProtocolHost.exe'
 or Data[@Name='NewProcessName'] = 'C:\Windows\System32
\SearchProtocolHost.exe'
 or Data[@Name='NewProcessName'] = 'C:\Windows\System32
\backgroundTaskHost.exe'
 or Data[@Name='NewProcessName'] = 'C:\Windows\System32\conhost.exe'
 or Data[@Name='NewProcessName'] = 'C:\Windows\System32\wbem\WmiPrvSE.exe'
 or Data[@Name='NewProcessName'] = 'C:\Windows\System32\taskhost.exe'
 or Data[@Name='NewProcessName'] = 'C:\Windows\System32\taskeng.exe'
 or Data[@Name='NewProcessName'] = 'C:\Windows\System32\svchost.exe'
 or Data[@Name='NewProcessName'] = 'C:\Windows\System32\sc.exe'
 or Data[@Name='NewProcessName'] = 'C:\Windows\System32\rundll32.exe'
 or Data[@Name='NewProcessName'] = 'C:\Windows\System32\taskhostex.exe'
)]]</Suppress>
```

☑ Edit query manually

Level 2 – Using Blacklist filters in Splunk to reduce the noise

- Blacklist filters can be applied:
  - In Splunk Enterprise
    - Filters events as they are received
  - On the Universal Forwarder
    - in versions later than 6.1.1
    - Saves overhead by applying filters at the source



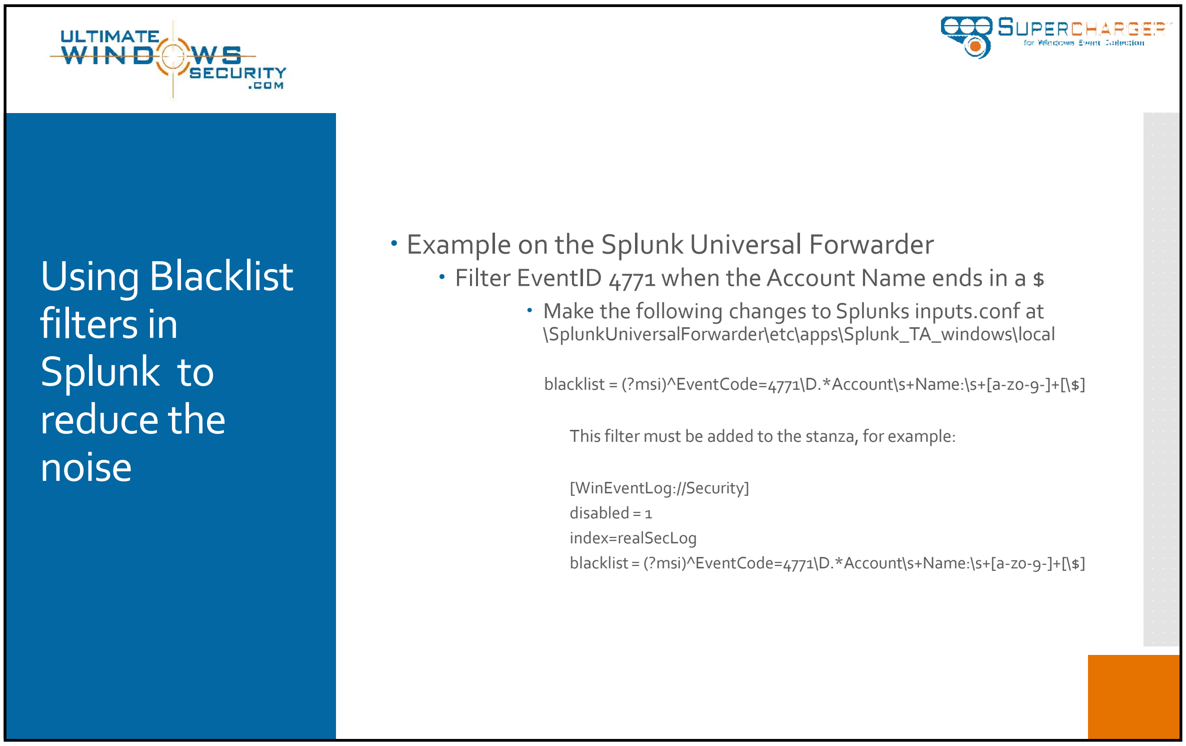
Using Blacklist filters in Splunk to reduce the noise

- Example in Splunk Enterprise
  - Filter EventID 4771 when the Account Name ends in a $
    - Make the following changes to Splunks props.conf at %SPLUNK_HOME%\etc\system\local\props.conf

```
[WinEventLog:SecurityLog]
TRANSFORMS-drop = delFilter
```

    - Make the following changes to Splunks transforms.conf at %SPLUNK_HOME%\etc\system\local\transforms.conf

```
[delFilter]
REGEX = (?msi)^EventCode=4771\D.*Account\s+Name:\s+[a-z0-9-]+[\$]
DEST_KEY = queue
FORMAT = nullQueue
```



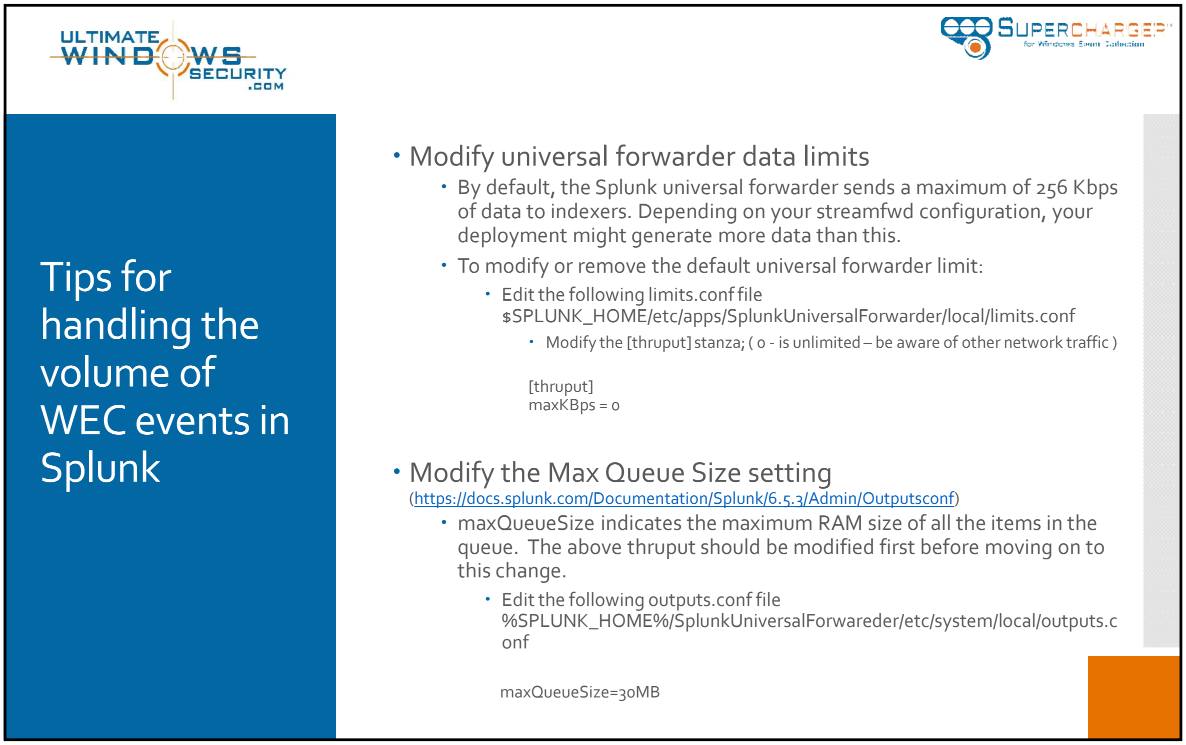
Using Blacklist filters in Splunk to reduce the noise

- Example on the Splunk Universal Forwarder
  - Filter EventID 4771 when the Account Name ends in a $
    - Make the following changes to Splunks inputs.conf at \SplunkUniversalForwarder\etc\apps\Splunk_TA_windows\local

```
blacklist = (?msi)^EventCode=4771\D.*Account\s+Name:\s+[a-z0-9-]+[\$]
```

This filter must be added to the stanza, for example:

```
[WinEventLog://Security]
disabled = 1
index=realSecLog
blacklist = (?msi)^EventCode=4771\D.*Account\s+Name:\s+[a-z0-9-]+[\$]
```



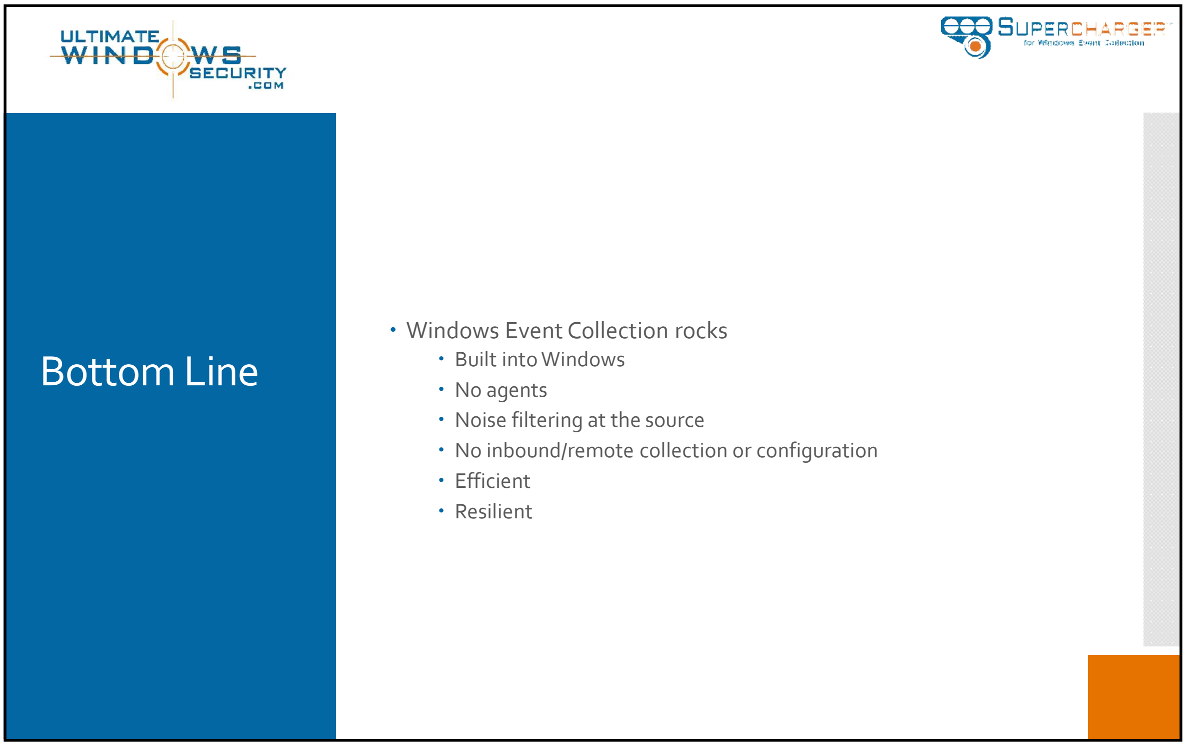
Tips for handling the volume of WEC events in Splunk

- Modify universal forwarder data limits
  - By default, the Splunk universal forwarder sends a maximum of 256 Kbps of data to indexers. Depending on your streamfwd configuration, your deployment might generate more data than this.
  - To modify or remove the default universal forwarder limit:
    - Edit the following limits.conf file $SPLUNK_HOME/etc/apps/SplunkUniversalForwarder/local/limits.conf
      - Modify the [thruput] stanza; (0 - is unlimited – be aware of other network traffic)

```
[thruput]
maxKBps = 0
```

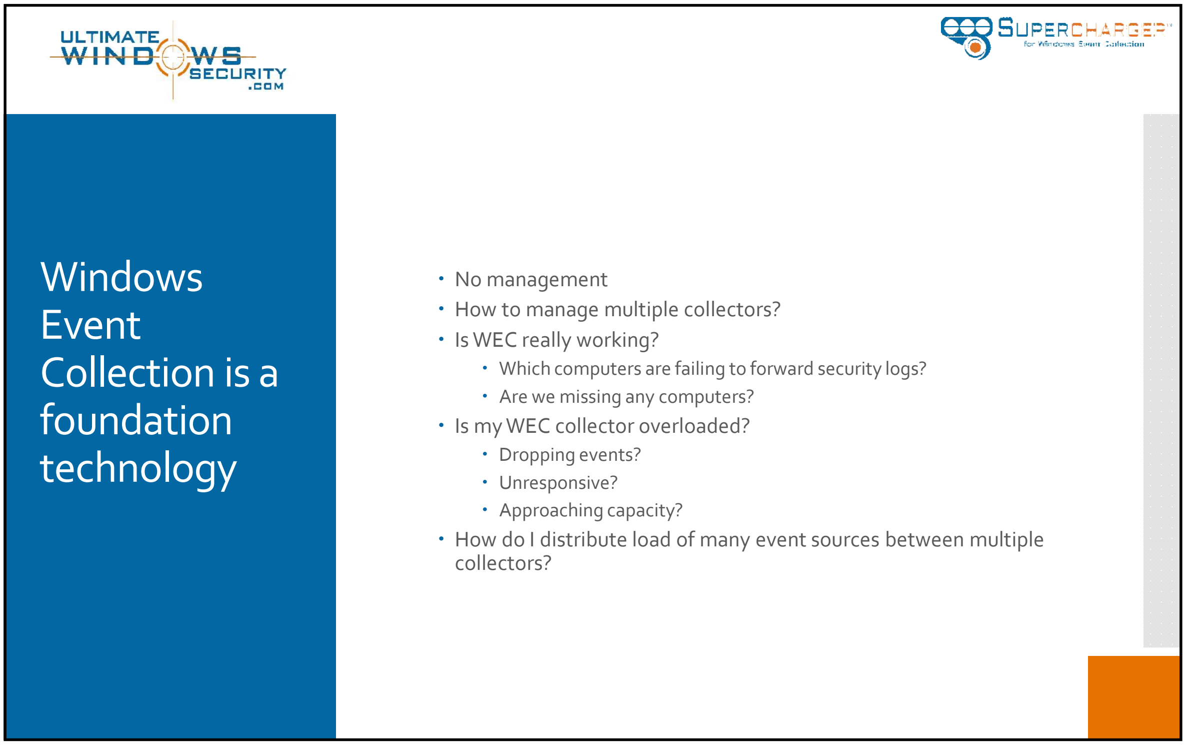
- Modify the Max Queue Size setting
  (https://docs.splunk.com/Documentation/Splunk/6.5.3/Admin/Outputsconf)
  - maxQueueSize indicates the maximum RAM size of all the items in the queue. The above thruput should be modified first before moving on to this change.
    - Edit the following outputs.conf file %SPLUNK_HOME%/SplunkUniversalForwareder/etc/system/local/outputs.conf

```
maxQueueSize=30MB
```



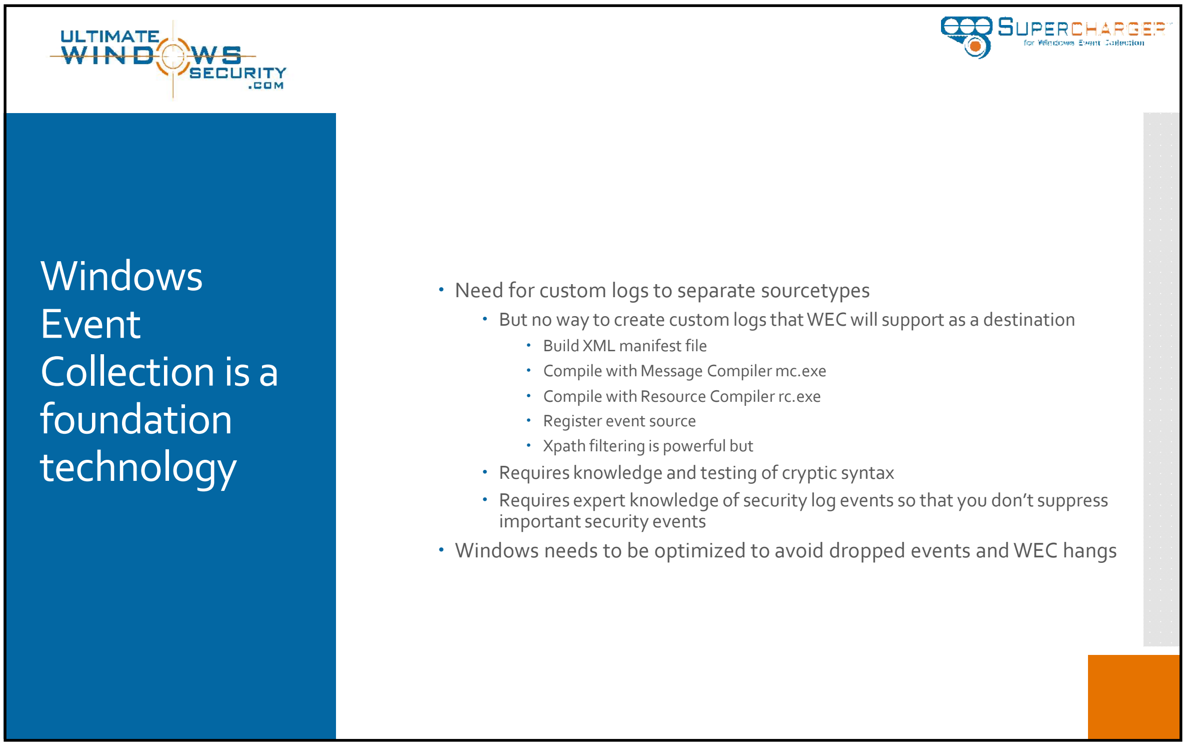
Bottom Line

- Windows Event Collection rocks
  - Built into Windows
  - No agents
  - Noise filtering at the source
  - No inbound/remote collection or configuration
  - Efficient
  - Resilient



Windows Event Collection is a foundation technology

- No management
- How to manage multiple collectors?
- Is WEC really working?
  - Which computers are failing to forward security logs?
  - Are we missing any computers?
- Is my WEC collector overloaded?
  - Dropping events?
  - Unresponsive?
  - Approaching capacity?
- How do I distribute load of many event sources between multiple collectors?

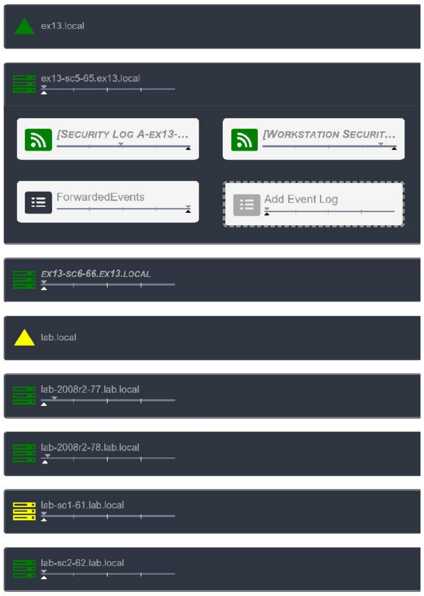


Windows Event Collection is a foundation technology

- Need for custom logs to separate sourcetypes
  - But no way to create custom logs that WEC will support as a destination
    - Build XML manifest file
    - Compile with Message Compiler mc.exe
    - Compile with Resource Compiler rc.exe
    - Register event source
    - Xpath filtering is powerful but
  - Requires knowledge and testing of cryptic syntax
  - Requires expert knowledge of security log events so that you don't suppress important security events
- Windows needs to be optimized to avoid dropped events and WEC hangs

Supercharger for Windows Event Collection

- Brings all your WEC collectors around the world onto one pane of glass



ex13.local

ex13-sc5-65.ex13.local

[SECURITY LOG A-EX13-...

[WORKSTATION SECURIT...

ForwardedEvents

Add Event Log

EX13-SC6-66.EX13.LOCAL

lab.local

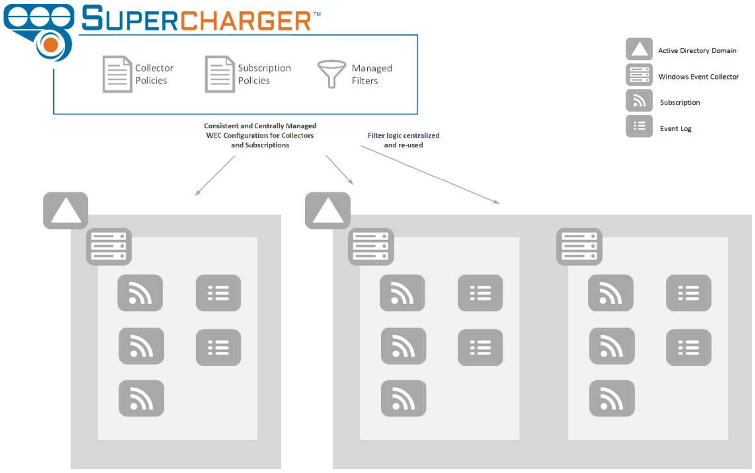
lab-2008r2-77.lab.local

lab-2008r2-78.lab.local

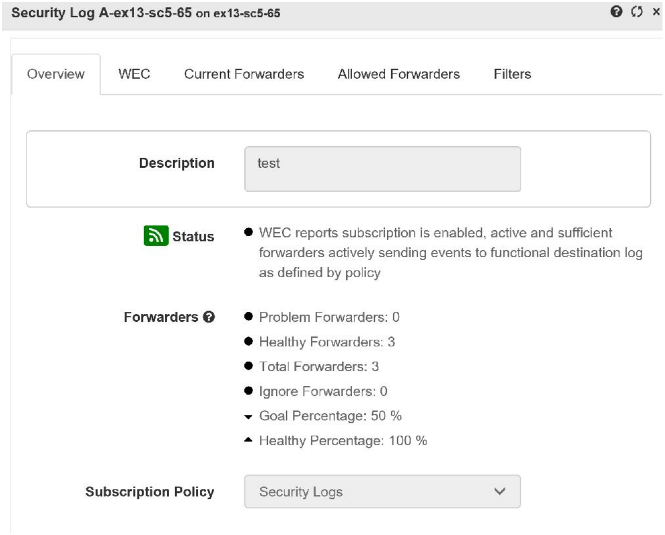
lab-sc1-61.lab.local

lab-sc2-62.lab.local

Supercharger for Windows Event Collection



Manage subscriptions consistently across all collectors



Security Log A-ex13-sc5-65 on ex13-sc5-65

Description: test

Status

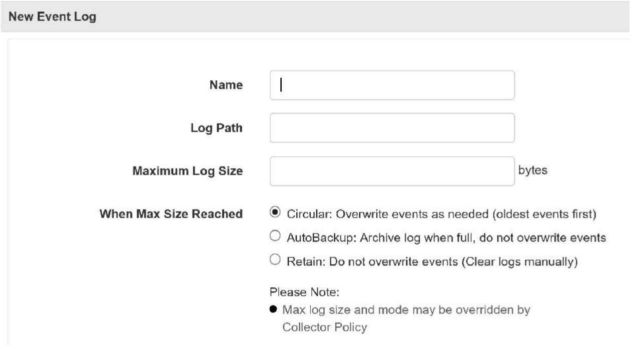
- WEC reports subscription is enabled, active and sufficient forwarders actively sending events to functional destination log as defined by policy

Forwarders

- Problem Forwarders: 0
- Healthy Forwarders: 3
- Total Forwarders: 3
- Ignore Forwarders: 0
- Goal Percentage: 50 %
- Healthy Percentage: 100 %

Subscription Policy: Security Logs

Create custom logs supported by WEC in seconds



New Event Log

Name

Log Path

Maximum Log Size bytes

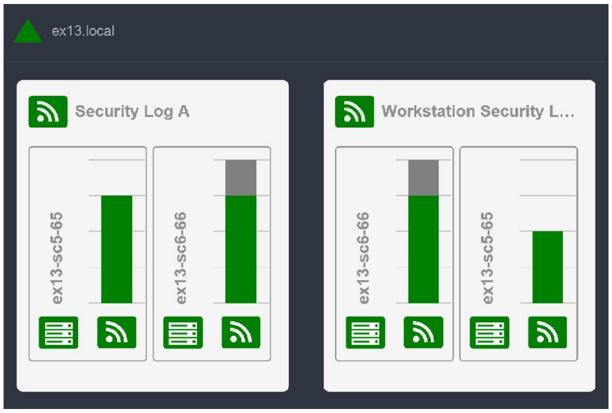
When Max Size Reached

- ● Circular: Overwrite events as needed (oldest events first)
- ○ AutoBackup: Archive log when full, do not overwrite events
- ○ Retain: Do not overwrite events (Clear logs manually)

Please Note:

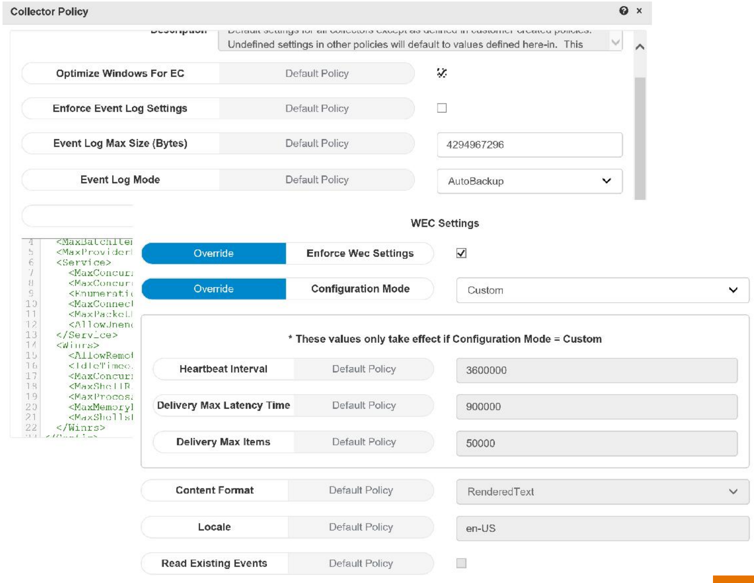
- Max log size and mode may be overridden by Collector Policy

Load balance computers between collectors



Optimize each collector automatically to support high volume WEC

All settings exposed via UI


Collector Policy

Description: Default settings for all collectors except as defined in customer created policies. Undefined settings in other policies will default to values defined here-in. This

Optimize Windows For EC	Default Policy	☑
Enforce Event Log Settings	Default Policy	☐
Event Log Max Size (Bytes)	Default Policy	4294967296
Event Log Mode	Default Policy	AutoBackup

```
<MaxBatchIte
<MaxProvider
<Service>
  <MaxConcur
  <MaxConcur
  <Enumerati
  <MaxConnec
  <MaxPacketI
  <AllowUnen
</Service>
<Winrs>
  <AllowRemo
  <IdleTimeo
  <MaxConcur
  <MaxShellR
  <MaxProces
  <MaxMemory
  <MaxShellsI
</Winrs>
```

WEC Settings

Override	Enforce Wec Settings	☑
Override	Configuration Mode	Custom

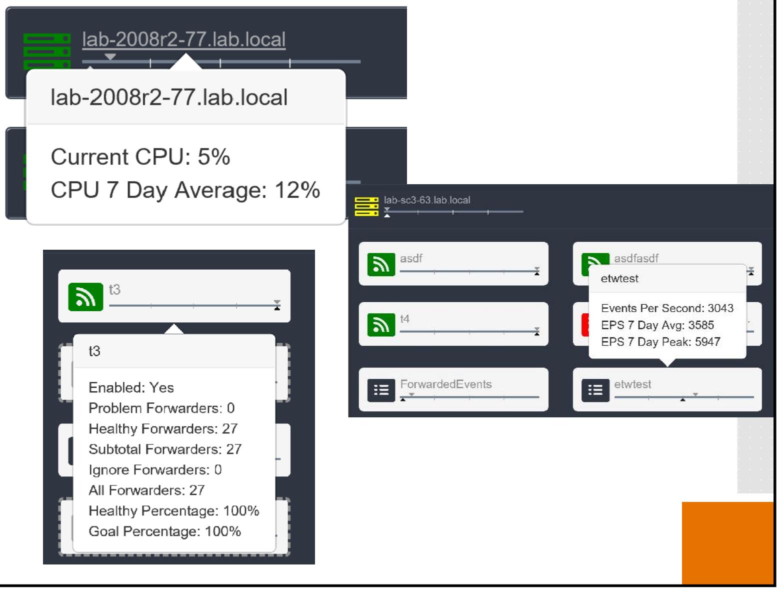
* These values only take effect if Configuration Mode = Custom

Heartbeat Interval	Default Policy	3600000
Delivery Max Latency Time	Default Policy	900000
Delivery Max Items	Default Policy	50000
Content Format	Default Policy	RenderedText
Locale	Default Policy	en-US
Read Existing Events	Default Policy	☐

ULTIMATE WINDOWS SECURITY .COM

SUPERCHARGER for Windows Event Collection

At a glance performance and health indicators



lab-2008r2-77.lab.local

lab-2008r2-77.lab.local

Current CPU: 5%
CPU 7 Day Average: 12%

lab-sc3-63.lab.local

etwtest

Events Per Second: 3043
EPS 7 Day Avg: 3585
EPS 7 Day Peak: 5947

t3

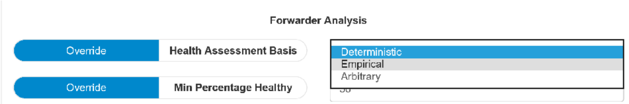
t3

Enabled: Yes
Problem Forwarders: 0
Healthy Forwarders: 27
Subtotal Forwarders: 27
Ignore Forwarders: 0
All Forwarders: 27
Healthy Percentage: 100%
Goal Percentage: 100%

ULTIMATE WINDOWS SECURITY .COM

SUPERCHARGER for Windows Event Collection

3 ways to measure health

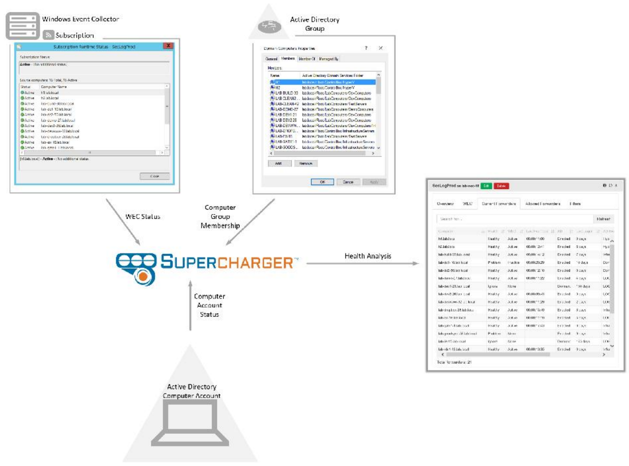


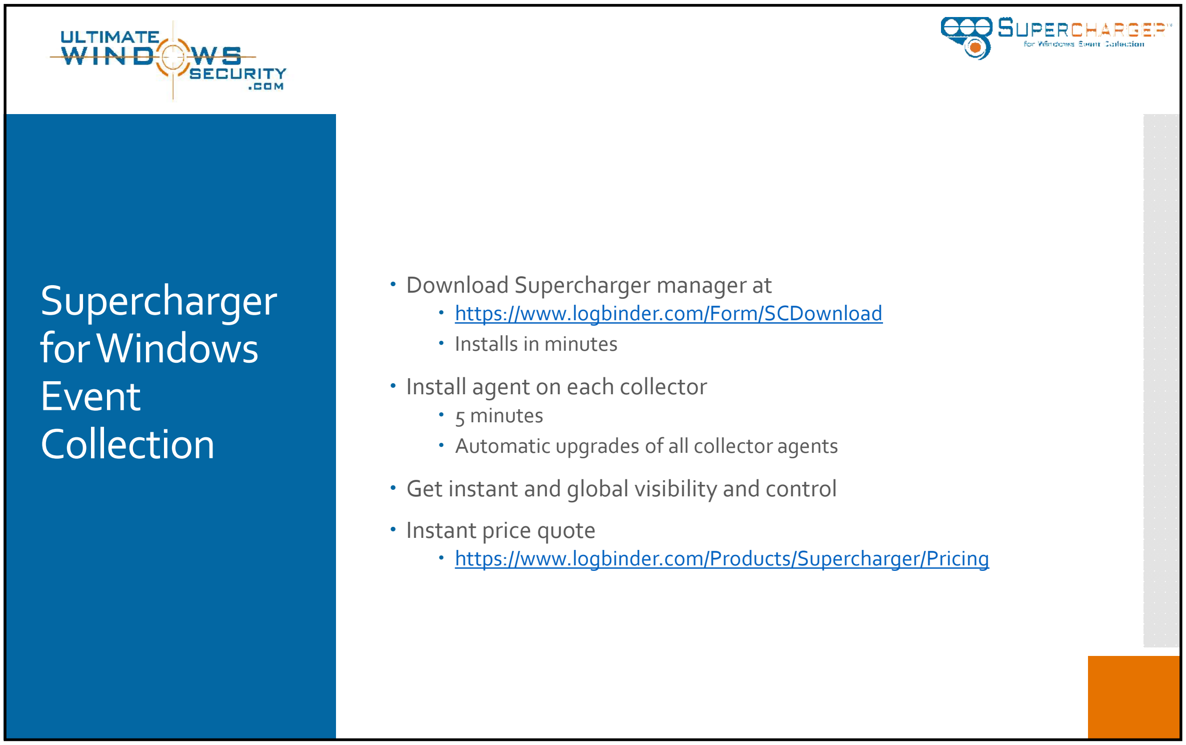
Forwarder Analysis

Override | Health Assessment Basis

Override | Min Percentage Healthy

Deterministic
Empirical
Arbitrary





Supercharger for Windows Event Collection

- Download Supercharger manager at
  - https://www.logbinder.com/Form/SCDownload
  - Installs in minutes
- Install agent on each collector
  - 5 minutes
  - Automatic upgrades of all collector agents
- Get instant and global visibility and control
- Instant price quote
  - https://www.logbinder.com/Products/Supercharger/Pricing

SUPERCHARGER™
for Windows Event Collection

~~POLLING~~

~~NOISE~~

~~AGENTS~~

www.logbinder.com