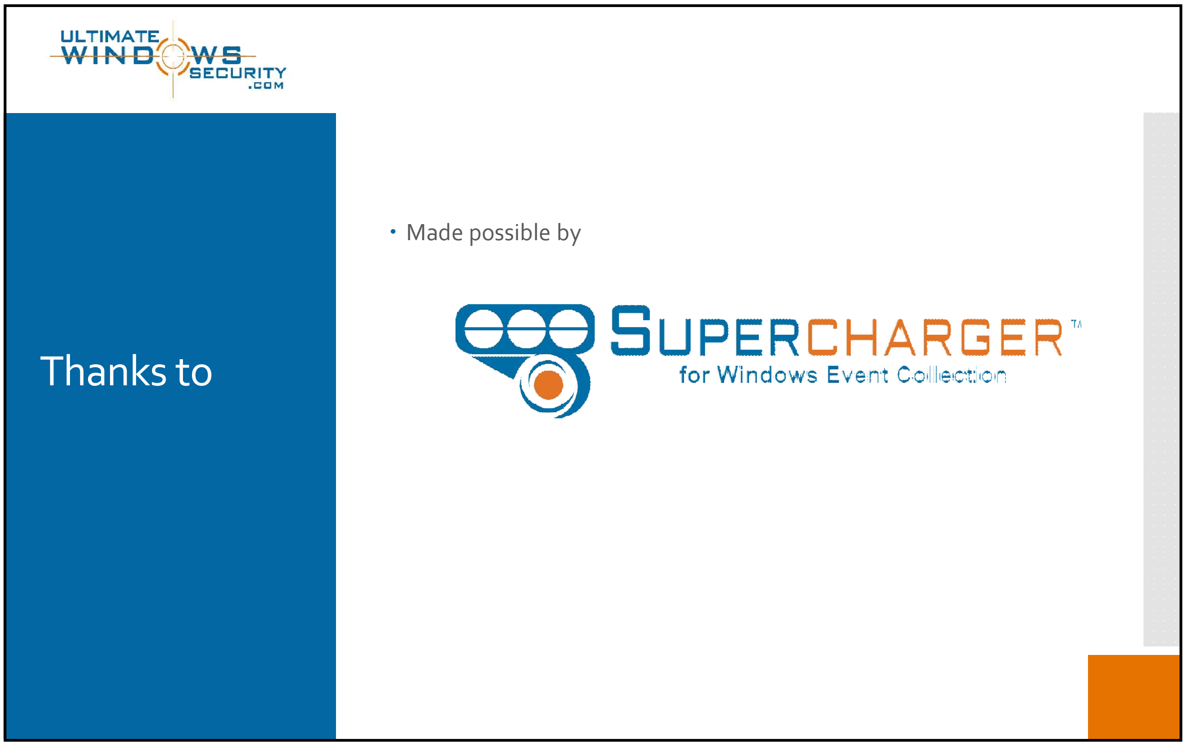
It's Time to Unleash the Power of Native Windows Event Collection

Sponsored by

SUPERCHARGER for Windows Event Collection



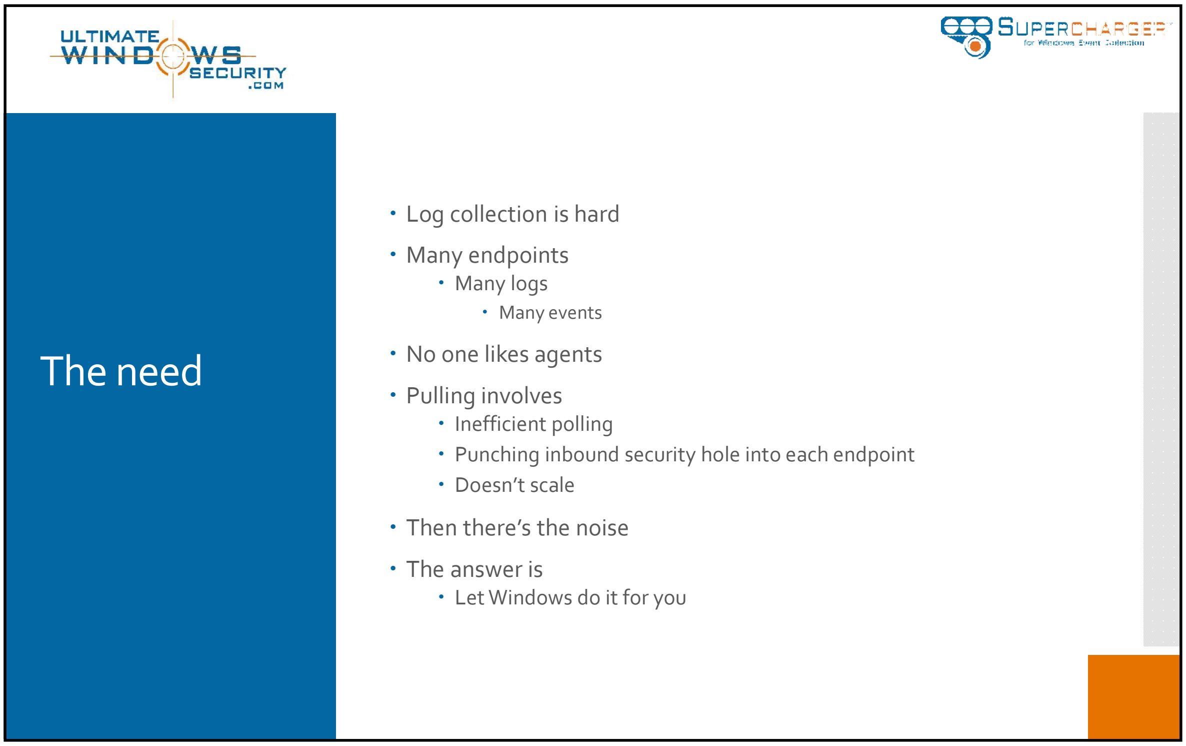
Thanks to

- Made possible by

SUPERCHARGER™ for Windows Event Collection

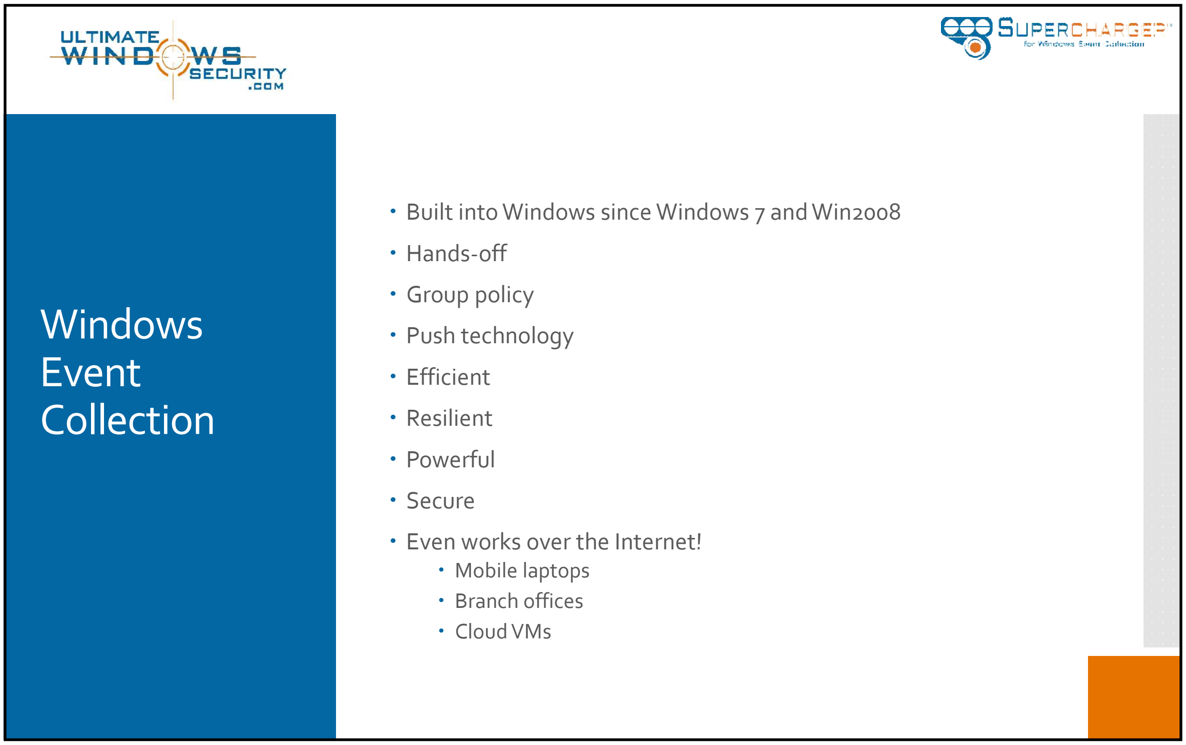
Preview of Key Points

- Windows Event Collection
- How it works
- Setting it up
- Meeting Enterprise Requirements
  - Managing
  - Advanced filtering
  - Load balancing
  - Troubleshooting
  - Capacity planning



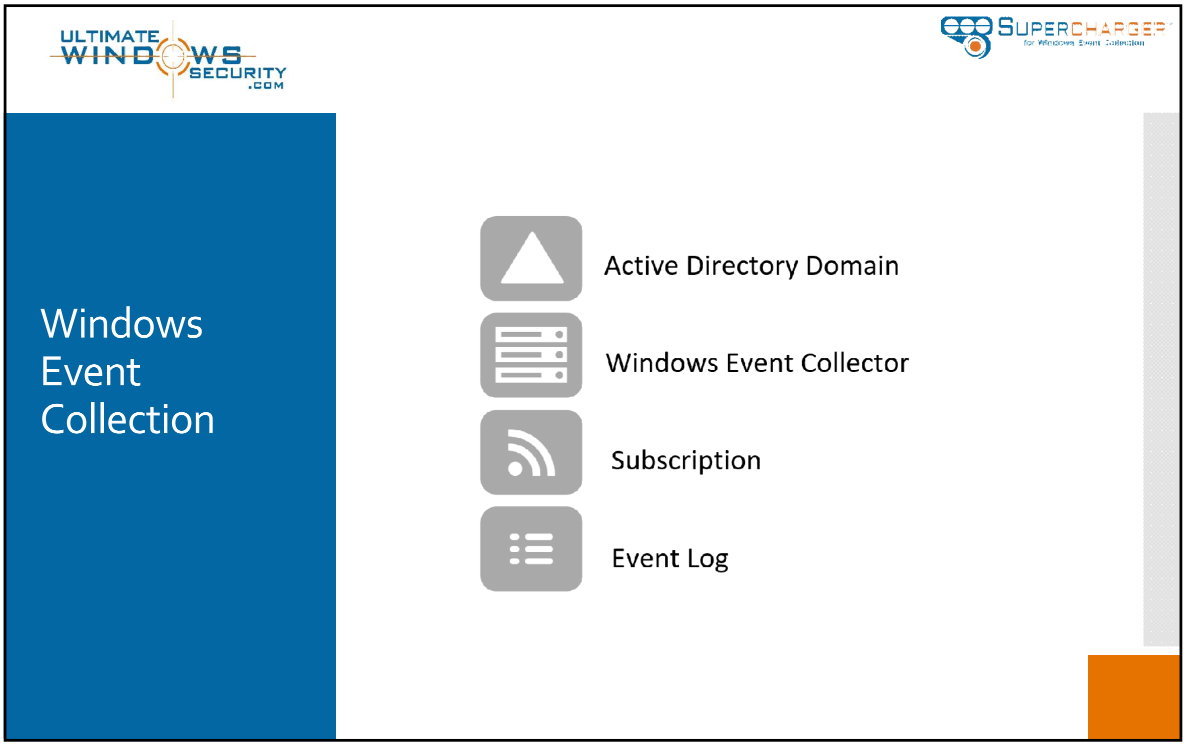
The need

- Log collection is hard
- Many endpoints
  - Many logs
    - Many events
- No one likes agents
- Pulling involves
  - Inefficient polling
  - Punching inbound security hole into each endpoint
  - Doesn’t scale
- Then there’s the noise
- The answer is
  - Let Windows do it for you



Windows Event Collection

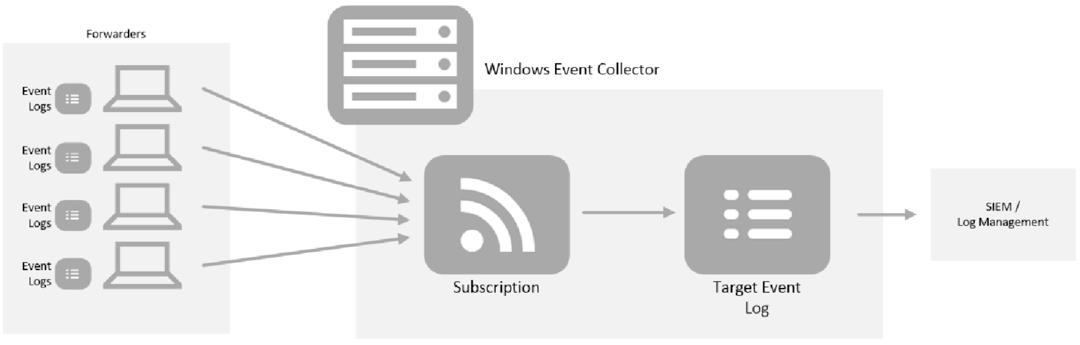
- Built into Windows since Windows 7 and Win2008
- Hands-off
- Group policy
- Push technology
- Efficient
- Resilient
- Powerful
- Secure
- Even works over the Internet!
  - Mobile laptops
  - Branch offices
  - Cloud VMs



Windows Event Collection

- Active Directory Domain
- Windows Event Collector
- Subscription
- Event Log

Windows Event Collection



Forwarders

Event Logs

Event Logs

Event Logs

Event Logs

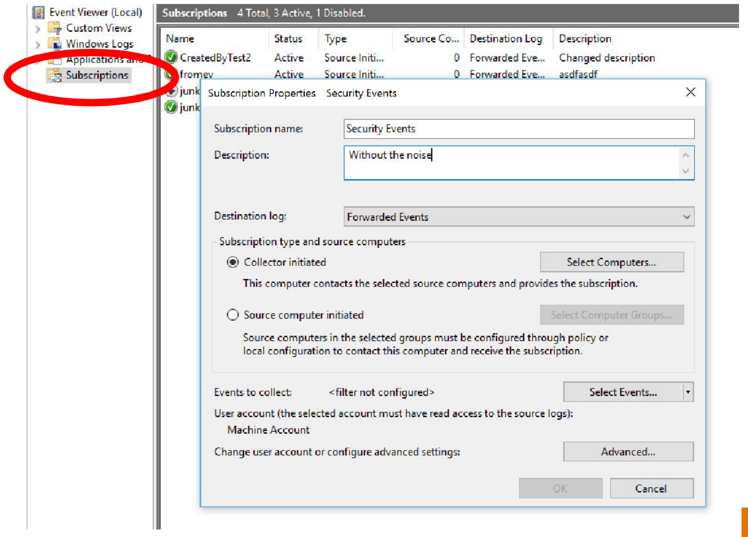
Windows Event Collector

Subscription

Target Event Log

SIEM / Log Management

Windows Event Collection



Subscriptions 4 Total, 3 Active, 1 Disabled.

Name	Status	Type	Source Co...	Destination Log	Description
CreatedByTest2	Active	Source Initi...	0	Forwarded Eve...	Changed description
fromev	Active	Source Initi...	0	Forwarded Eve...	asdfasdf
junk					
junk					

Subscription Properties   Security Events

Subscription name: Security Events

Description: Without the noise

Destination log: Forwarded Events

Subscription type and source computers

● Collector initiated   Select Computers...

This computer contacts the selected source computers and provides the subscription.

○ Source computer initiated   Select Computer Groups...

Source computers in the selected groups must be configured through policy or local configuration to contact this computer and receive the subscription.

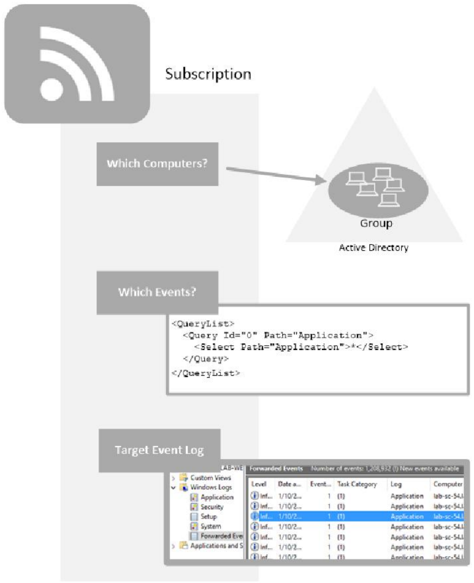
Events to collect: <filter not configured>   Select Events...

User account (the selected account must have read access to the source logs):

Machine Account

Change user account or configure advanced settings: Advanced...

WEC Subscription

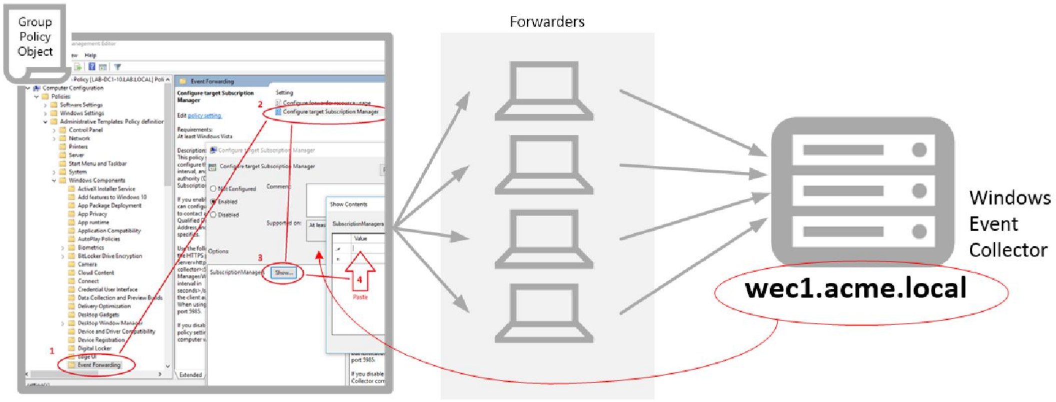


```
<QueryList>
  <Query Id="0" Path="Application">
    <Select Path="Application">*</Select>
  </Query>
</QueryList>
```

Forwarded Events Number of events: 1,208,932 (!) New events available

Level	Date a...	Event...	Task Category	Log	Computer
Inf...	1/10/2...	1	(1)	Application	lab-sc-54.l
Inf...	1/10/2...	1	(1)	Application	lab-sc-54.l
Inf...	1/10/2...	1	(1)	Application	lab-sc-54.l
Inf...	1/10/2...	1	(1)	Application	lab-sc-54.l
Inf...	1/10/2...	1	(1)	Application	lab-sc-54.l
Inf...	1/10/2...	1	(1)	Application	lab-sc-54.l
Inf...	1/10/2...	1	(1)	Application	lab-sc-54.l

Targeting via Group Policy



Policy [LAB-DC1-10.LAB.LOCAL] Poli

Event Forwarding

Configure target Subscription Manager

Edit policy setting.

Requirements:
At least Windows Vista

Setting
Configure forwarder resource usage
Configure target Subscription Manager

Configure target Subscription Manager
○ Not Configured
● Enabled
○ Disabled
Comment:
Supported on:
Options:
SubscriptionManagers Show...

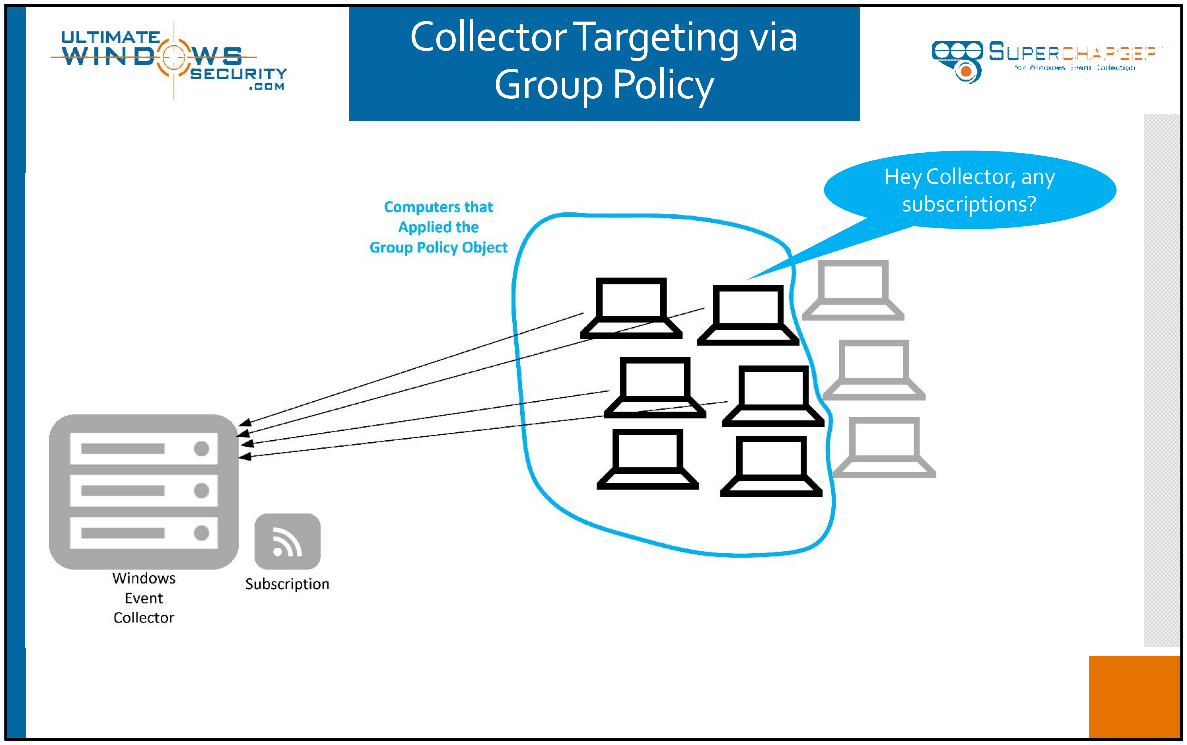
port 5985.

Group Policy vs Group Membership

- For a given computer
  - Group policy
    - Targets the computer at the ***collector***
  - Group membership
    - Controls which ***subscriptions*** on that collector

Group Policy vs Group Membership

- Multiple
  - A computer can be targeted at multiple collectors
  - A computer can be assigned to multiple subscriptions



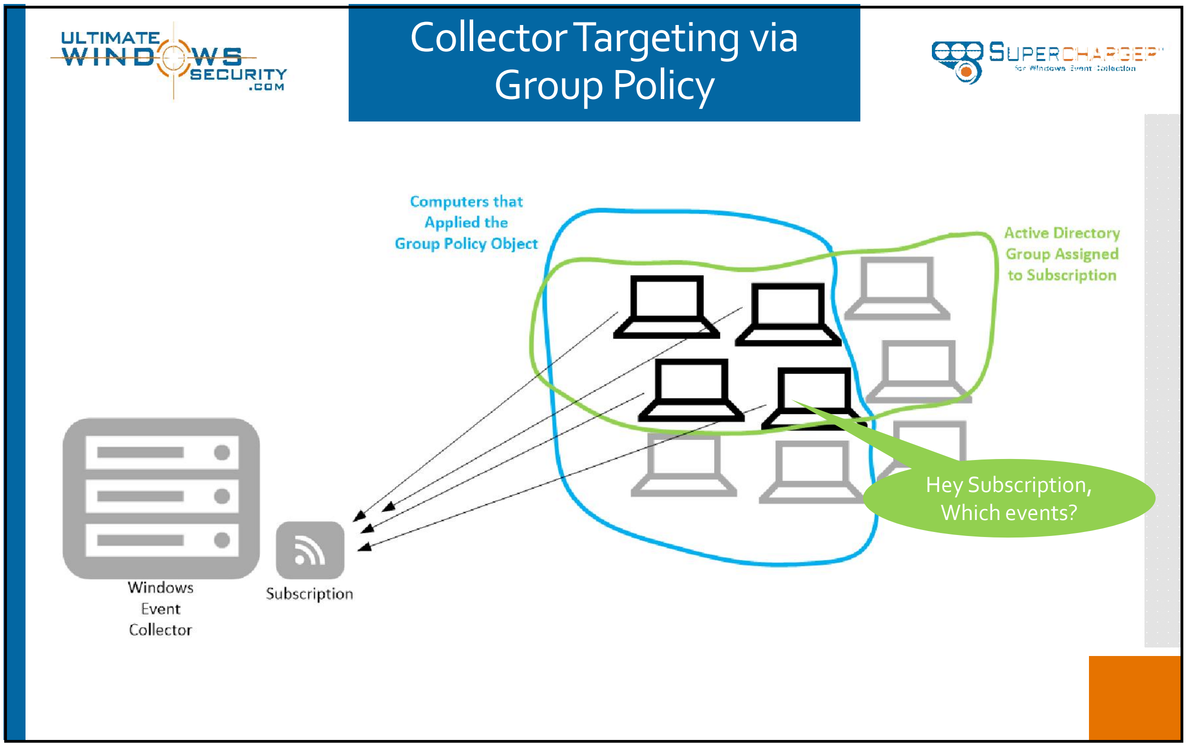
Collector Targeting via Group Policy

Hey Collector, any subscriptions?

Computers that Applied the Group Policy Object

Windows Event Collector

Subscription



Collector Targeting via Group Policy

Computers that Applied the Group Policy Object

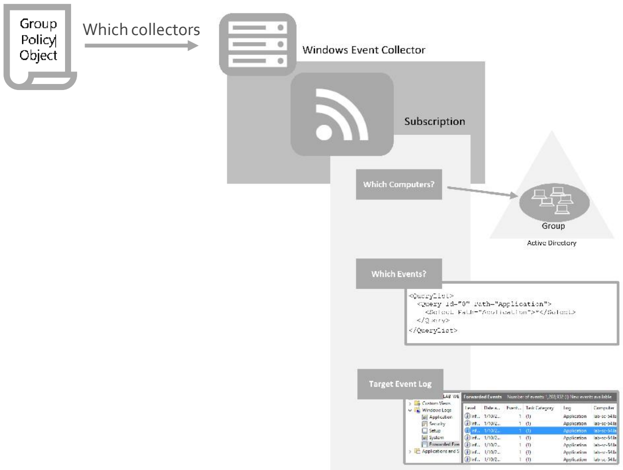
Active Directory Group Assigned to Subscription

Hey Subscription, Which events?

Windows Event Collector

Subscription

Which collector, subscription, event, log?



```
<QueryList>
  <Query Id="0" Path="Application">
    <Select Path="Application">*</Select>
  </Query>
</QueryList>
```

Forwarded Events Number of events: 1,203,932 (!) New events available

Level	Date a...	Event...	Task Category	Log	Computer
Inf...	1/10/2...	1	(1)	Application	lab-sc-54.la
Inf...	1/10/2...	1	(1)	Application	lab-sc-54.la
Inf...	1/10/2...	1	(1)	Application	lab-sc-54.la
Inf...	1/10/2...	1	(1)	Application	lab-sc-54.la
Inf...	1/10/2...	1	(1)	Application	lab-sc-54.la
Inf...	1/10/2...	1	(1)	Application	lab-sc-54.la
Inf...	1/10/2...	1	(1)	Application	lab-sc-54.la

Targeting

- Use group policy to target all your computers at all potential collectors
  - Even if you don't currently have any applicable subscriptions
- Got sites? Don't want event forwarding crossing sites?
  - Group policy can be linked to sites
  - But there's a lot more to the story
    - Future webinar on managing WEC in a distributed network

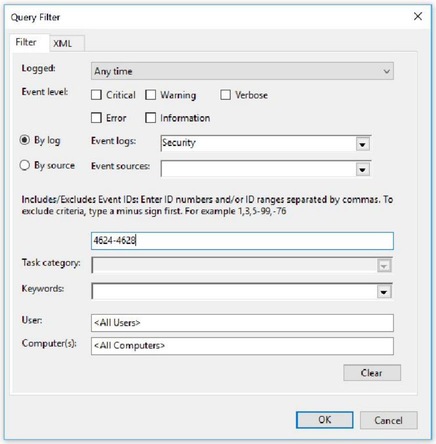
Industrial strength

- Resilience
  - What if a collector is down?
  - What if a forwarder (source) is disconnected from network?
  - Computers will catch up events when they can reconnect
- Security
  - Source and Collectors mutually authenticate via Kerberos
    - Or certificates if non-domain computers
  - Event forwarding traffic can be encrypted via https
    - Requires trusted server certificate on collector
- Scalability
  - Control how often
    - Computers ask collectors about new or changed subscriptions

      `Server=http://lab-wecdev-53.lab.local:5985/wsman/SubscriptionManager/WEC,`***Refresh=60***
    - Computers send latest events for assigned subscriptions
  - Balance
    - Batch size
    - Latency
  - Many configurable settings for optimization
  - Collectors can handle thousands of forwarders

Filtering - Which events?

- Each subscription has a query filter to define which
  - Source logs
  - Which events in those logs



Logged: Any time

Event level: □ Critical □ Warning □ Verbose □ Error □ Information

● By log Event logs: Security

○ By source Event sources:

Includes/Excludes Event IDs: Enter ID numbers and/or ID ranges separated by commas. To exclude criteria, type a minus sign first. For example 1,3,5-99,-76

4624-4628

Task category:

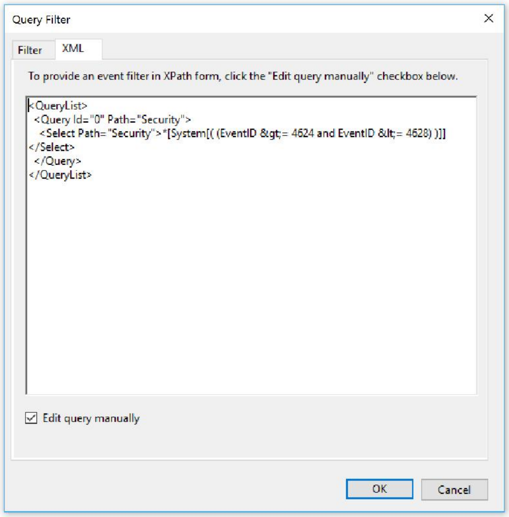
Keywords:

User: <All Users>

Computer(s): <All Computers>

Filtering - Which events?

- XML/Xpath provides much more sophisticated filtering



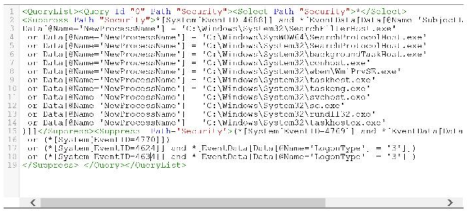
To provide an event filter in XPath form, click the "Edit query manually" checkbox below.

```
<QueryList>
  <Query Id="0" Path="Security">
    <Select Path="Security">*[System[( (EventID &gt;= 4624 and EventID &lt;= 4628) )]]
</Select>
  </Query>
</QueryList>
```

☑ Edit query manually

Filtering - Which events?

- Security events with common noise filtered out



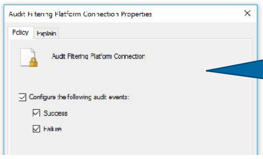
```
<QueryList><Query Id="0" Path="Security"><Select Path="Security">*</Select>
<Suppress Path="Security">*[System[EventID=4688]] and *[EventData[Data[@Name='SubjectL
Data[@Name='NewProcessName'] = 'C:\Windows\System32\SearchFilterHost.exe'
 or Data[@Name='NewProcessName'] = 'C:\Windows\SysWOW64\SearchProtocolHost.exe'
 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><Suppress Path="Security">(*[System[EventID=4769]] and *[EventData[Data
 or (*[System[EventID=4770]])
 or (*[System[EventID=4624]] and *[EventData[Data[@Name='LogonType'] = '3']])
 or (*[System[EventID=4634]] and *[EventData[Data[@Name='LogonType'] = '3']])
</Suppress> </Query></QueryList>
```

ULTIMATE WINDOWS SECURITY.COM

SUPERCHARGER for Windows Event Collection

Filtering - Which events?

- Or limiting events forwarded with more granularity than you get with audit policy



Audit Filtering Platform Connection Properties

Policy | Explain

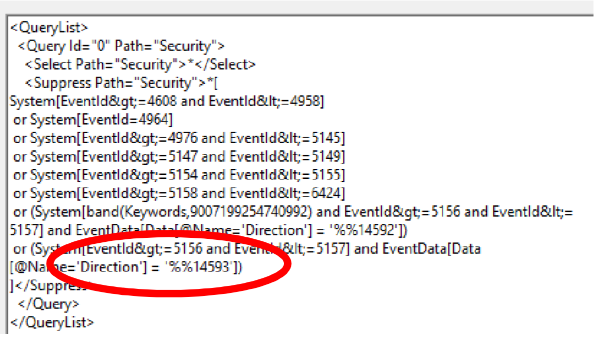
Audit Filtering Platform Connection

☑ Configure the following audit events:

☑ Success

☑ Failure

What if you only want to audit ***inbound*** connections?



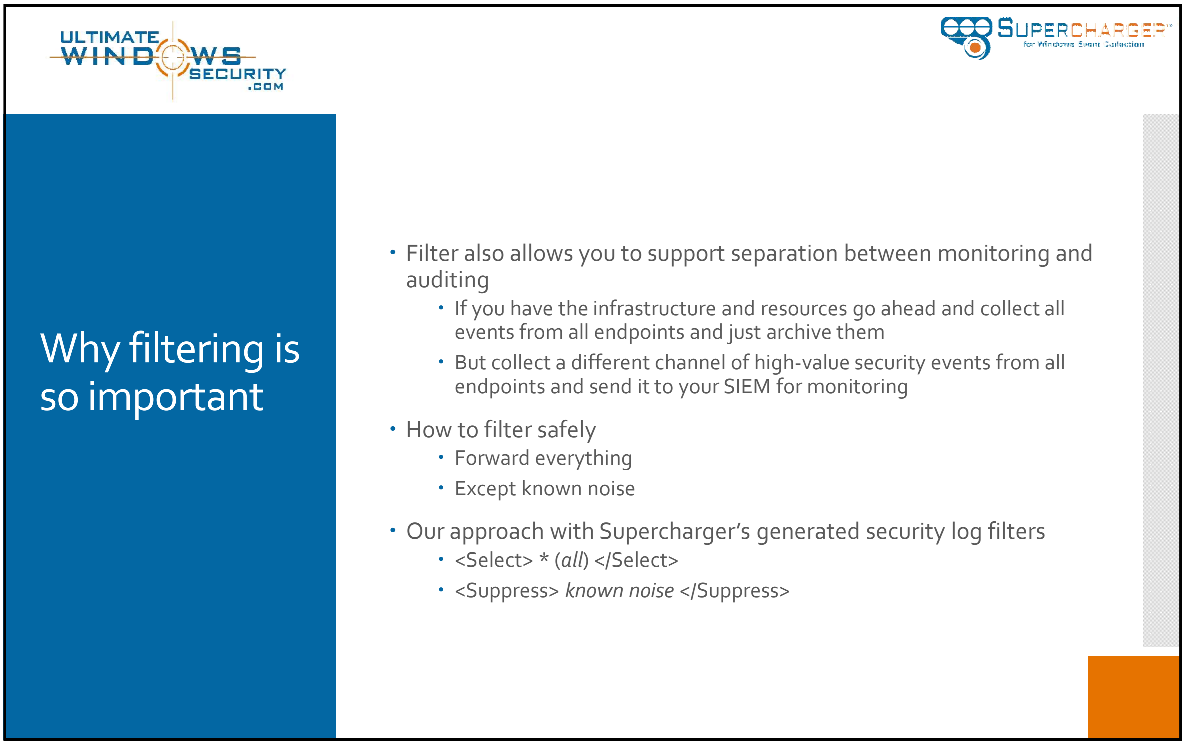
```
<QueryList>
  <Query Id="0" Path="Security">
   <Select Path="Security">*</Select>
   <Suppress Path="Security">*[
System[EventId&gt;=4608 and EventId&lt;=4958]
 or System[EventId=4964]
 or System[EventId&gt;=4976 and EventId&lt;=5145]
 or System[EventId&gt;=5147 and EventId&lt;=5149]
 or System[EventId&gt;=5154 and EventId&lt;=5155]
 or System[EventId&gt;=5158 and EventId&lt;=6424]
 or (System[band(Keywords,9007199254740992) and EventId&gt;=5156 and EventId&lt;=
5157] and EventData[Data[@Name='Direction'] = '%%14592'])
 or (System[EventId&gt;=5156 and EventId&lt;=5157] and EventData[Data
[@Name='Direction'] = '%%14593'])
]</Suppress>
  </Query>
</QueryList>
```

ULTIMATE WINDOWS SECURITY.COM

SUPERCHARGER for Windows Event Collection

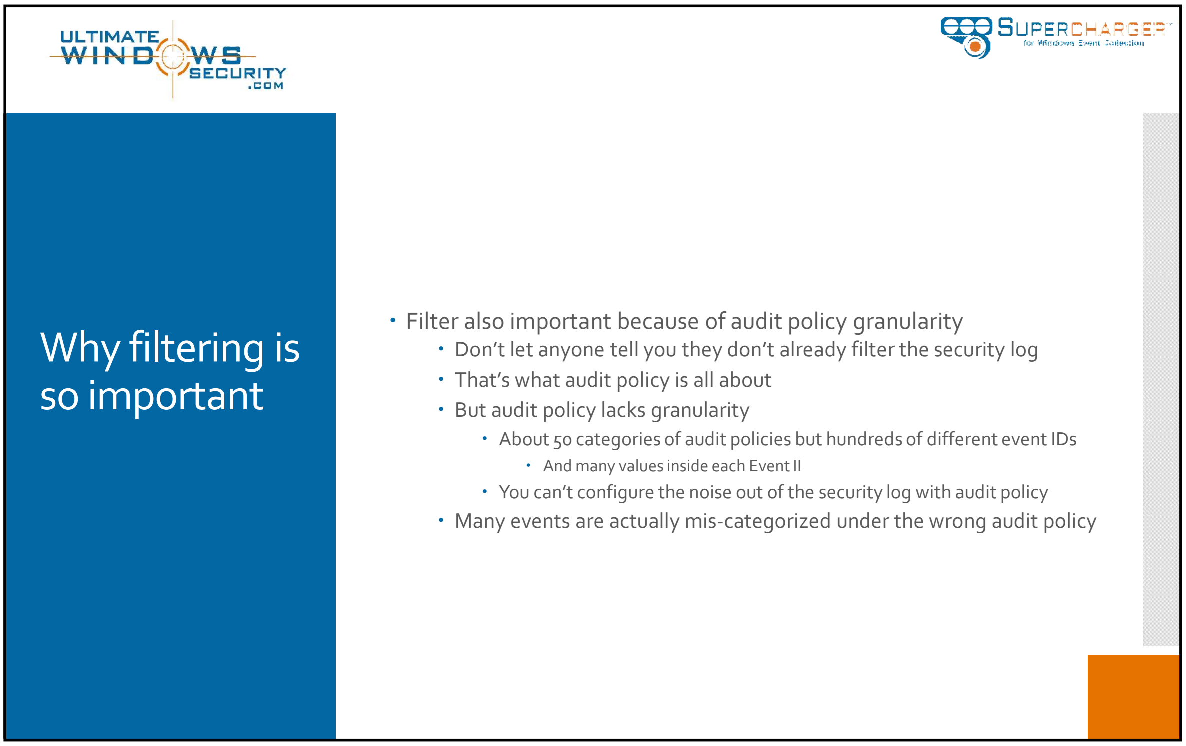
Why filtering is so relevant right now

- Resources
  - So much of logs is noise/spam
  - Yet the biggest SIEMs charge based on volume
  - Very few organizations have the resources to collect every event from every endpoint
- Risks
  - Results in many organizations scaling back and only monitoring “important” computers
  - That’s what allows
    - APTs horizontal spread and long time till detection
    - Ransomware to spread and reach critical mass
- Solution
  - If you can’t get all events from all endpoints
    - At least get the important events from all endpoints
    - And all events from important endpoints



Why filtering is so important

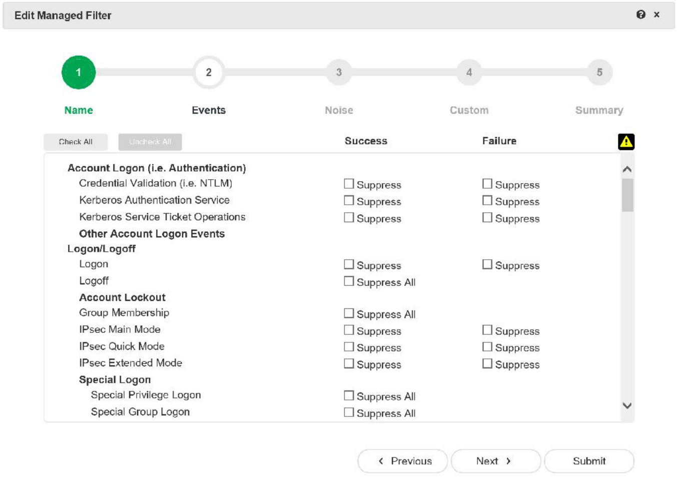
- Filter also allows you to support separation between monitoring and auditing
  - If you have the infrastructure and resources go ahead and collect all events from all endpoints and just archive them
  - But collect a different channel of high-value security events from all endpoints and send it to your SIEM for monitoring
- How to filter safely
  - Forward everything
  - Except known noise
- Our approach with Supercharger's generated security log filters
  - <Select> * (*all*) </Select>
  - <Suppress> *known noise* </Suppress>



Why filtering is so important

- Filter also important because of audit policy granularity
  - Don't let anyone tell you they don't already filter the security log
  - That's what audit policy is all about
  - But audit policy lacks granularity
    - About 50 categories of audit policies but hundreds of different event IDs
      - And many values inside each Event II
    - You can't configure the noise out of the security log with audit policy
  - Many events are actually mis-categorized under the wrong audit policy

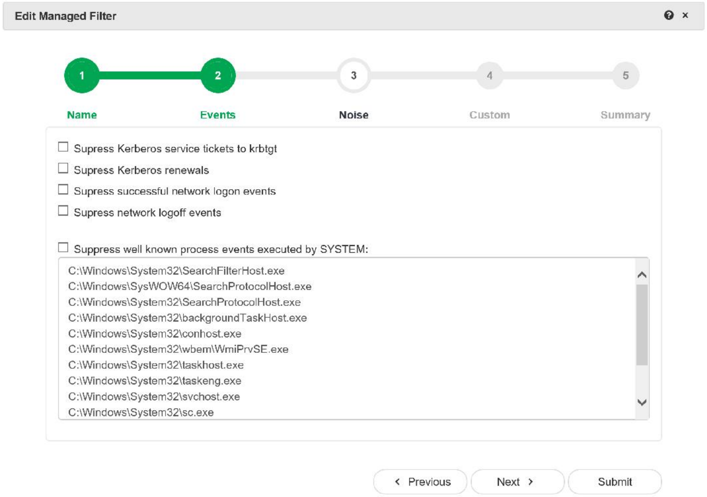
Supercharger advanced security log filtering



Edit Managed Filter

	Success	Failure
Account Logon (i.e. Authentication)		
Credential Validation (i.e. NTLM)	□ Suppress	□ Suppress
Kerberos Authentication Service	□ Suppress	□ Suppress
Kerberos Service Ticket Operations	□ Suppress	□ Suppress
Other Account Logon Events		
Logon/Logoff		
Logon	□ Suppress	□ Suppress
Logoff	□ Suppress All	
Account Lockout		
Group Membership	□ Suppress All	
IPsec Main Mode	□ Suppress	□ Suppress
IPsec Quick Mode	□ Suppress	□ Suppress
IPsec Extended Mode	□ Suppress	□ Suppress
Special Logon		
Special Privilege Logon	□ Suppress All	
Special Group Logon	□ Suppress All	

Supercharger advanced security log filtering



Edit Managed Filter

□ Supress Kerberos service tickets to krbtgt

□ Supress Kerberos renewals

□ Supress successful network logon events

□ Supress network logoff events

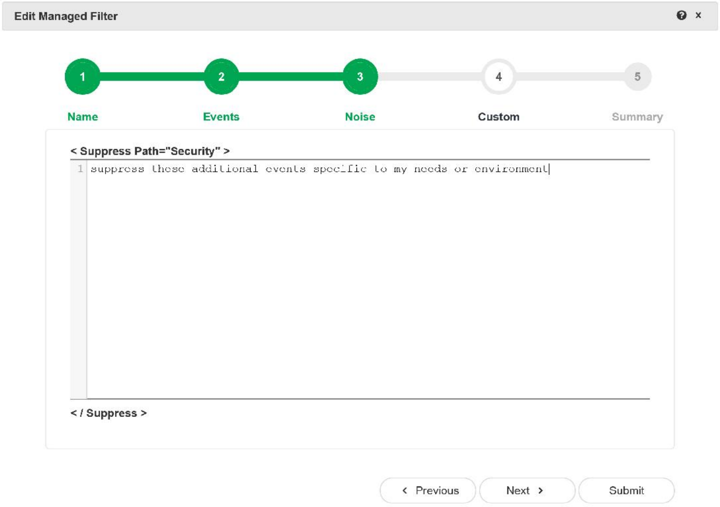
□ Suppress well known process events executed by SYSTEM:

```
C:\Windows\System32\SearchFilterHost.exe
C:\Windows\SysWOW64\SearchProtocolHost.exe
C:\Windows\System32\SearchProtocolHost.exe
C:\Windows\System32\backgroundTaskHost.exe
C:\Windows\System32\conhost.exe
C:\Windows\System32\wbem\WmiPrvSE.exe
C:\Windows\System32\taskhost.exe
C:\Windows\System32\taskeng.exe
C:\Windows\System32\svchost.exe
C:\Windows\System32\sc.exe
```

ULTIMATE WINDOWS SECURITY .COM

SUPERCHARGER for Windows Event Collection

Supercharger advanced security log filtering


Edit Managed Filter

< Suppress Path="Security" >

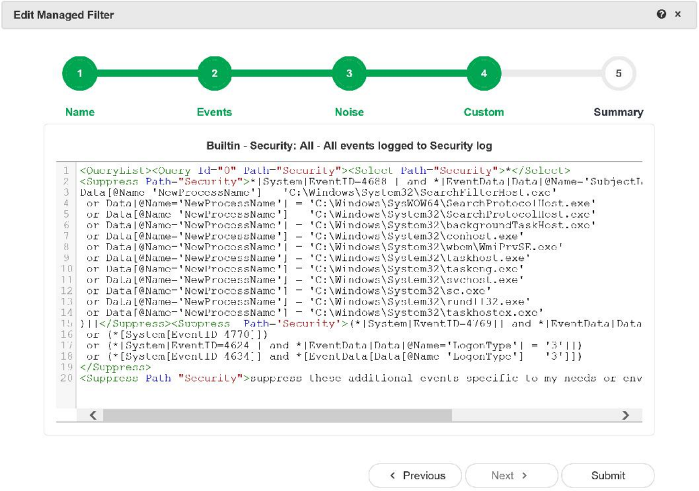
```
suppress these additional events specific to my needs or environment
```

< / Suppress >

ULTIMATE WINDOWS SECURITY .COM

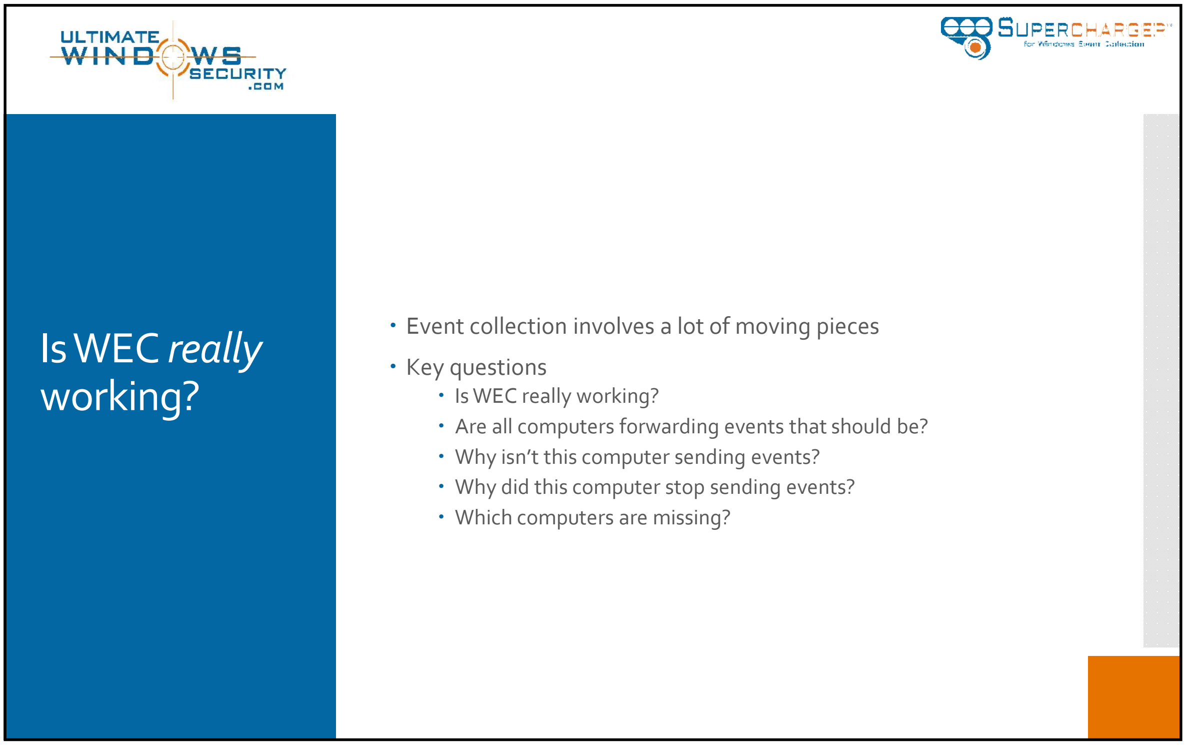
SUPERCHARGER for Windows Event Collection

Supercharger advanced security log filtering


Edit Managed Filter

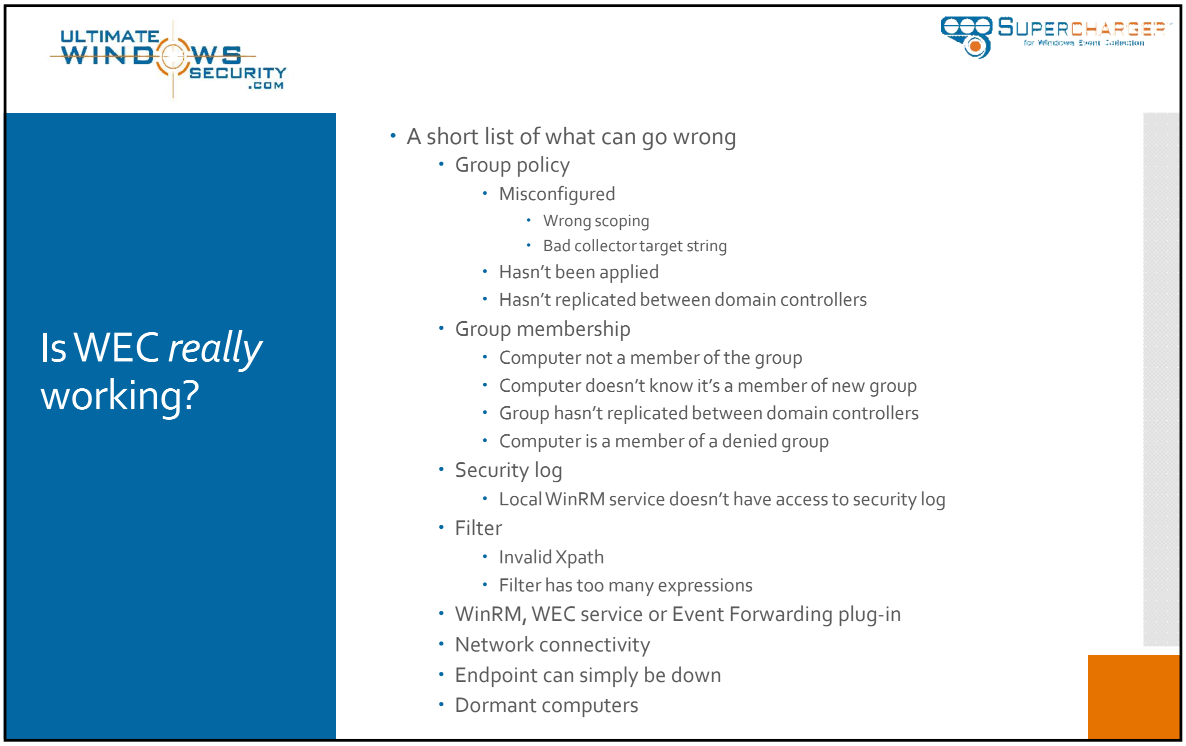
Builtin - Security: All - All events logged to Security log

```
<QueryList><Query Id="0" Path="Security"><Select Path="Security">*</Select>
<Suppress Path="Security">*[System[EventID=4688 ] and *[EventData[Data[@Name='SubjectL
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><Suppress  Path='Security'>(*[System[EventID=4769]] and *[EventData[Data
 or (*[System[EventID=4770]])
 or (*[System[EventID=4624 ] and *[EventData[Data[@Name='LogonType'] = '3']])
 or (*[System[EventID=4634]] and *[EventData[Data[@Name='LogonType'] = '3']])
</Suppress>
<Suppress Path="Security">suppress these additional events specific to my needs or env
```



Is WEC *really* working?

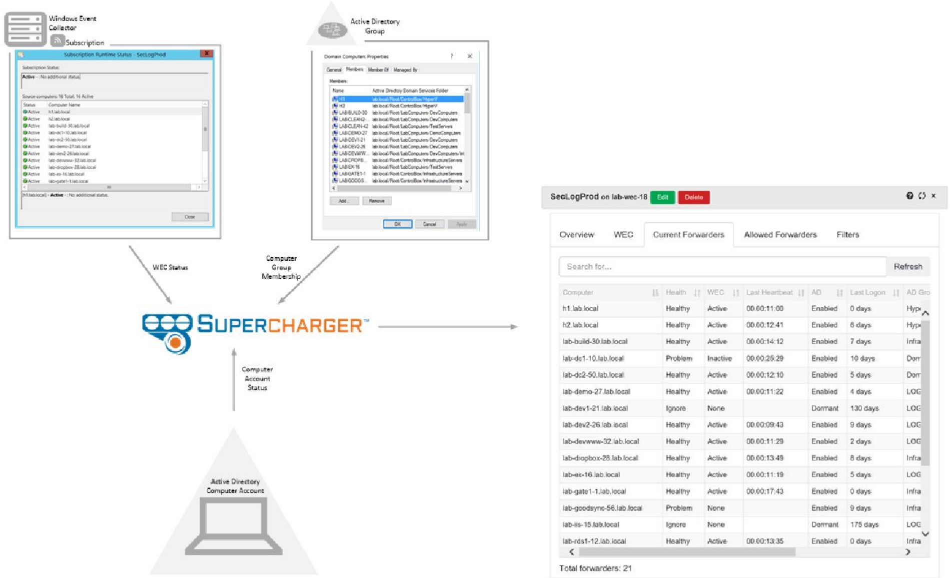
- Event collection involves a lot of moving pieces
- Key questions
  - Is WEC really working?
  - Are all computers forwarding events that should be?
  - Why isn't this computer sending events?
  - Why did this computer stop sending events?
  - Which computers are missing?



Is WEC *really* working?

- A short list of what can go wrong
  - Group policy
    - Misconfigured
      - Wrong scoping
      - Bad collector target string
    - Hasn't been applied
    - Hasn't replicated between domain controllers
  - Group membership
    - Computer not a member of the group
    - Computer doesn't know it's a member of new group
    - Group hasn't replicated between domain controllers
    - Computer is a member of a denied group
  - Security log
    - Local WinRM service doesn't have access to security log
  - Filter
    - Invalid Xpath
    - Filter has too many expressions
  - WinRM, WEC service or Event Forwarding plug-in
  - Network connectivity
  - Endpoint can simply be down
  - Dormant computers

Supercharger deterministic forwarder analysis


Windows Event Collector
Subscription
Subscription Runtime Status - SecLogProd
Active Directory Group
Domain Computers Properties
WEC Status
Computer Group Membership
SUPERCHARGER
Computer Account Status
Active Directory Computer Account

SecLogProd on lab-wec-18 Edit Delete

Overview | WEC | Current Forwarders | Allowed Forwarders | Filters

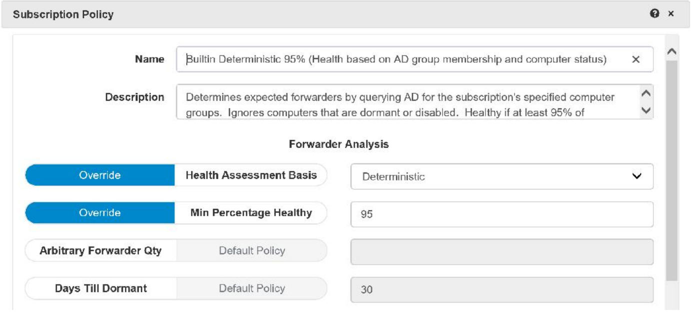
Search for... Refresh

Computer	Health	WEC	Last Heartbeat	AD	Last Logon	AD Gro
h1.lab.local	Healthy	Active	00:00:11:00	Enabled	0 days	Hyp
h2.lab.local	Healthy	Active	00:00:12:41	Enabled	6 days	Hyp
lab-build-30.lab.local	Healthy	Active	00:00:14:12	Enabled	7 days	Infra
lab-dc1-10.lab.local	Problem	Inactive	00:00:25:29	Enabled	10 days	Dom
lab-dc2-50.lab.local	Healthy	Active	00:00:12:10	Enabled	5 days	Dom
lab-demo-27.lab.local	Healthy	Active	00:00:11:22	Enabled	4 days	LOG
lab-dev1-21.lab.local	Ignore	None		Dormant	130 days	LOG
lab-dev2-26.lab.local	Healthy	Active	00:00:09:43	Enabled	9 days	LOG
lab-devwww-32.lab.local	Healthy	Active	00:00:11:29	Enabled	2 days	LOG
lab-dropbox-28.lab.local	Healthy	Active	00:00:13:49	Enabled	8 days	Infra
lab-ex-16.lab.local	Healthy	Active	00:00:11:19	Enabled	5 days	LOG
lab-gate1-1.lab.local	Healthy	Active	00:00:17:43	Enabled	0 days	Infra
lab-goodsync-56.lab.local	Problem	None		Enabled	9 days	Infra
lab-iis-15.lab.local	Ignore	None		Dormant	175 days	LOG
lab-rds1-12.lab.local	Healthy	Active	00:00:13:35	Enabled	0 days	Infra

Total forwarders: 21

Health analysis

- Some subscriptions should always have 100% active forwarders
  - Domain controllers
  - High security value servers
- Subscriptions for desktops and laptops will never be 100% active



Subscription Policy

Name: Builtin Deterministic 95% (Health based on AD group membership and computer status)

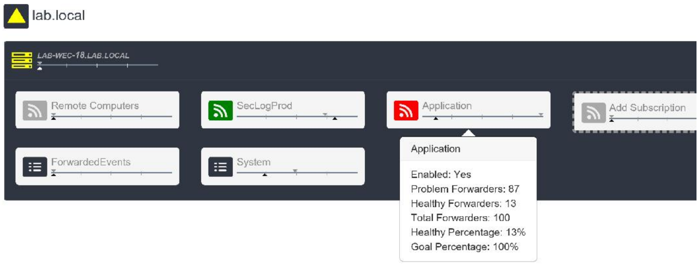
Description: Determines expected forwarders by querying AD for the subscription's specified computer groups. Ignores computers that are dormant or disabled. Healthy if at least 95% of

Forwarder Analysis

Override	Health Assessment Basis	Deterministic
Override	Min Percentage Healthy	95
Arbitrary Forwarder Qty	Default Policy	
Days Till Dormant	Default Policy	30

Health analysis

- Forwarder health rolls up to subscription health
- Rolls up to collector health

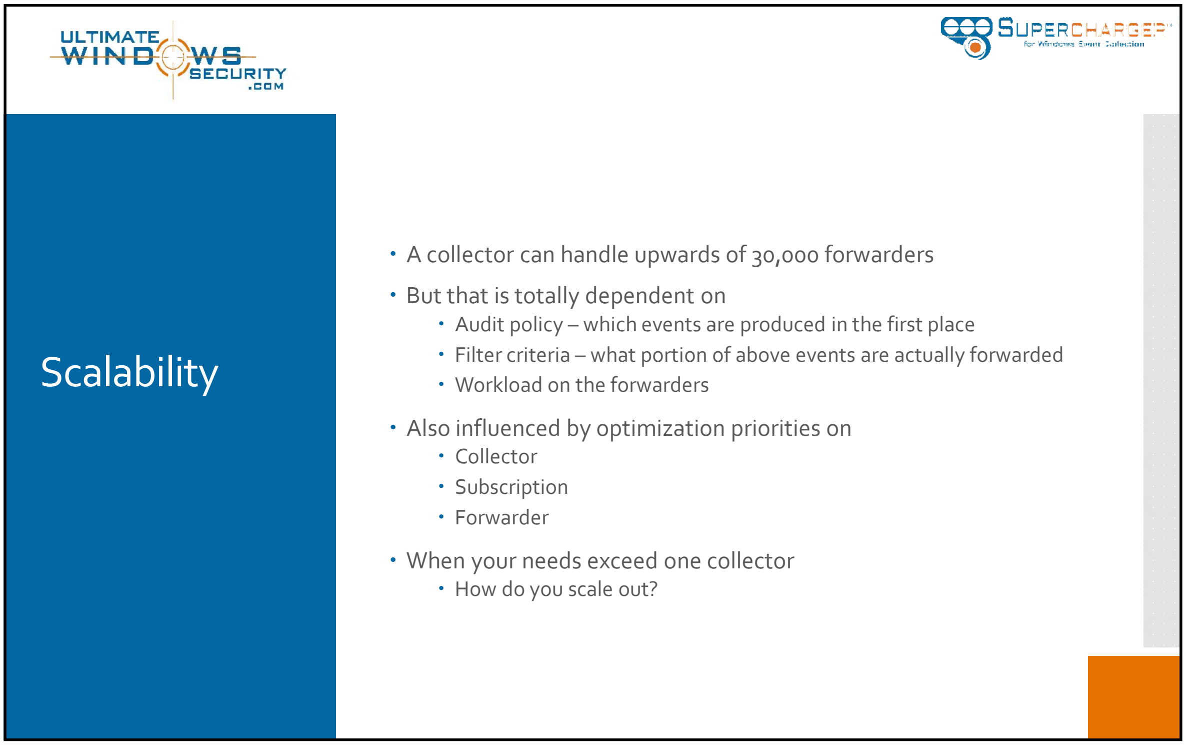


Application

Enabled: Yes
Problem Forwarders: 87
Healthy Forwarders: 13
Total Forwarders: 100
Healthy Percentage: 13%
Goal Percentage: 100%

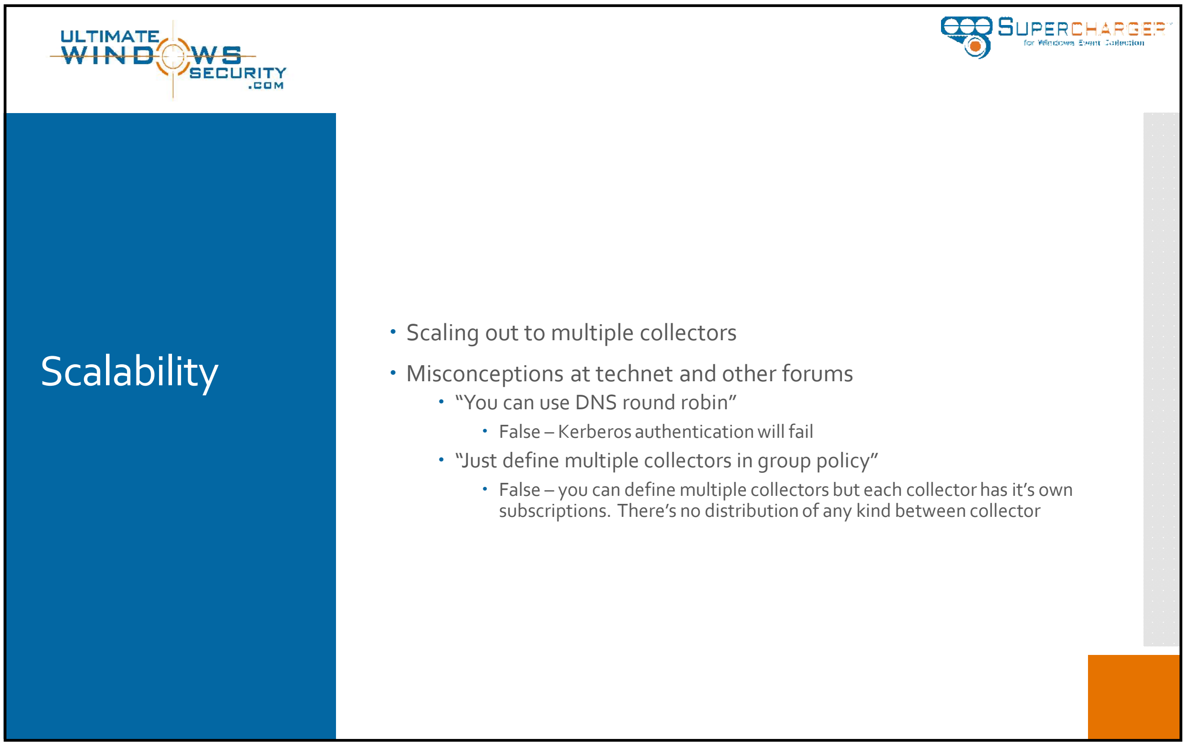
Scalability

- A collector can handle upwards of 30,000 forwarders
- But that is totally dependent on
  - Audit policy – which events are produced in the first place
  - Filter criteria – what portion of above events are actually forwarded
  - Workload on the forwarders
- Also influenced by optimization priorities on
  - Collector
  - Subscription
  - Forwarder
- When your needs exceed one collector
  - How do you scale out?



Scalability

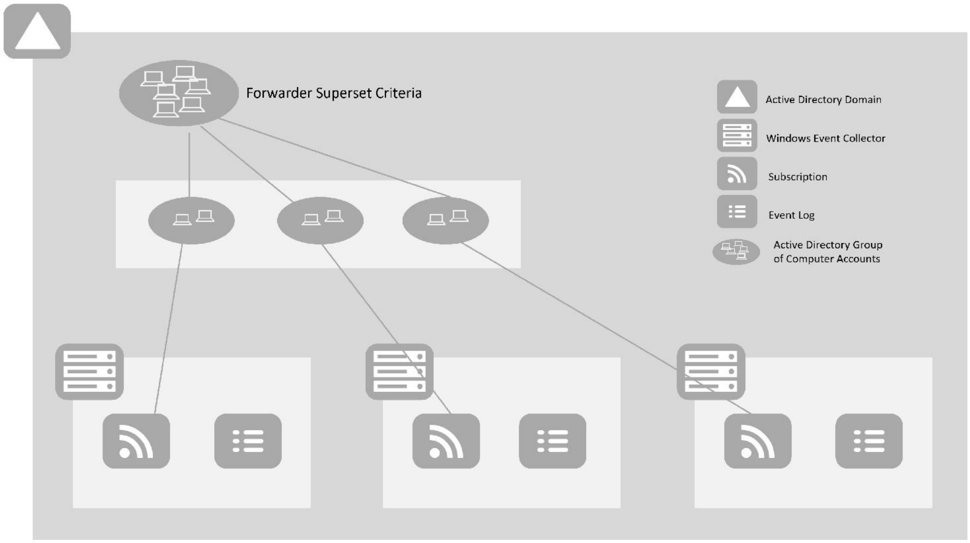
- A collector can handle upwards of 30,000 forwarders
- But that is totally dependent on
  - Audit policy – which events are produced in the first place
  - Filter criteria – what portion of above events are actually forwarded
  - Workload on the forwarders
- Also influenced by optimization priorities on
  - Collector
  - Subscription
  - Forwarder
- When your needs exceed one collector
  - How do you scale out?



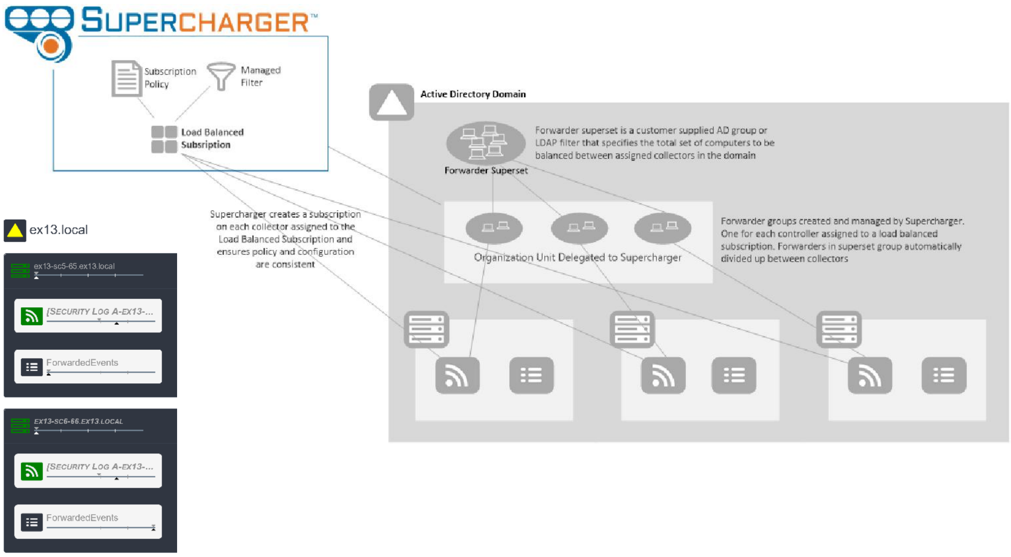
Scalability

- Scaling out to multiple collectors
- Misconceptions at technet and other forums
  - "You can use DNS round robin"
    - False – Kerberos authentication will fail
  - "Just define multiple collectors in group policy"
    - False – you can define multiple collectors but each collector has it's own subscriptions. There's no distribution of any kind between collector

Scaling out WEC



Scaling out WEC

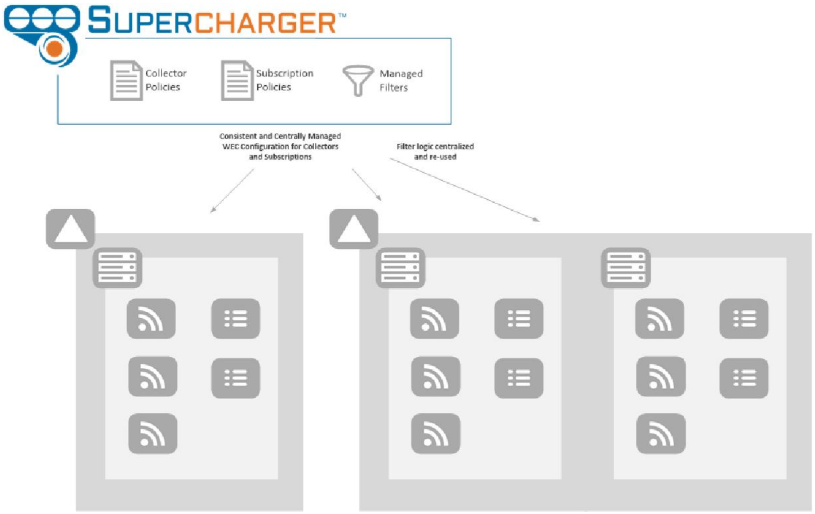


Supercharger creates a subscription on each collector assigned to the Load Balanced Subscription and ensures policy and configuration are consistent

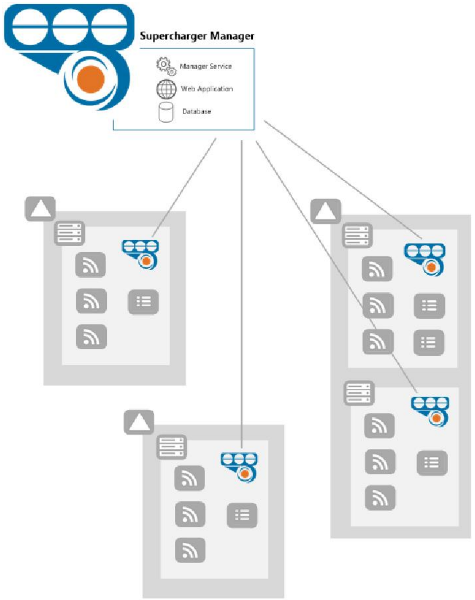
Forwarder superset is a customer supplied AD group or LDAP filter that specifies the total set of computers to be balanced between assigned collectors in the domain

Forwarder groups created and managed by Supercharger. One for each controller assigned to a load balanced subscription. Forwarders in superset group automatically divided up between collectors

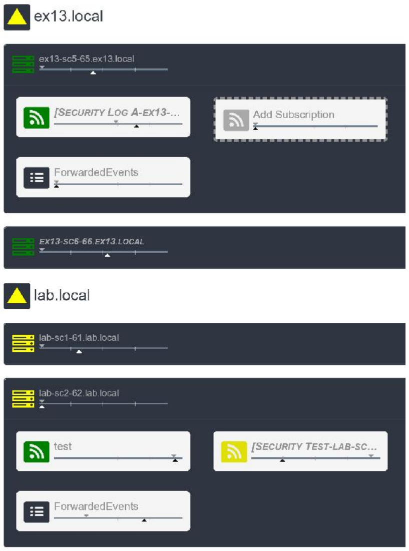
Supercharger architecture


SUPERCHARGER™
Collector Policies
Subscription Policies
Managed Filters
Consistent and Centrally Managed WEC Configuration for Collectors and Subscriptions
Filter logic centralized and re-used

Physical manager/ agent architecture

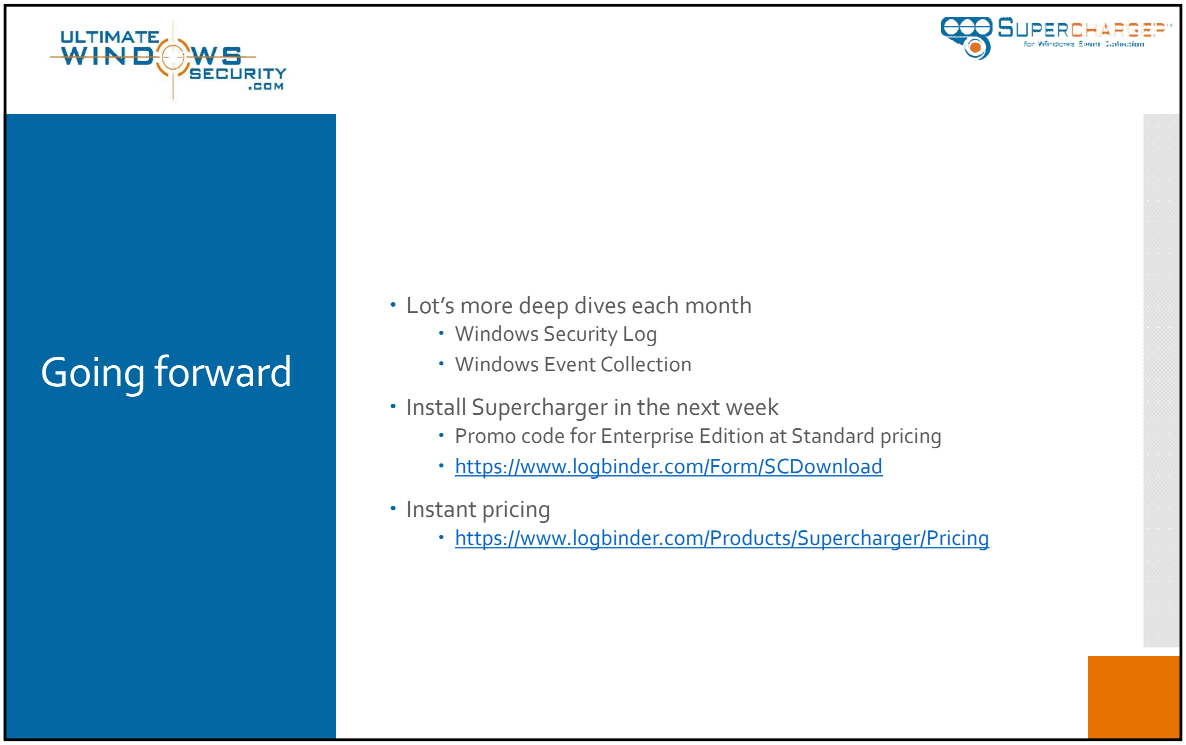


Dashboard



Bottom line

- WEC is powerful and particularly relevant right now given the state of endpoint security
- WEC eliminates the lesser of 2 evils of polling vs. agents
- WEC is a foundation technology
- Supercharger makes WEC fast, easy and fun to
  - Implement
  - Manage
  - Scale



ULTIMATE WINDOWS SECURITY.COM

SUPERCHARGER for Windows Event Collection

Going forward

- Lot’s more deep dives each month
  - Windows Security Log
  - Windows Event Collection
- Install Supercharger in the next week
  - Promo code for Enterprise Edition at Standard pricing
  - https://www.logbinder.com/Form/SCDownload
- Instant pricing
  - https://www.logbinder.com/Products/Supercharger/Pricing