



# How to Monitor Active Directory Changes for Free Using Splunk Free, Supercharger Free and My New Splunk App

Sponsored by





© 2017 Monterey Technology Group Inc.



Thanks to

• Made possible by





## Preview of Key Points

- Active Directory changes
- The free solution overview
- Setting it up step by step





## AD Changes

- What we all need to be monitoring
  - Users
    - New
    - Deleted, disabled
    - Significant change
  - Groups
    - Members
      - Added
      - Removed
    - Scope/type changed
    - Added
    - Deleted



## AD Changes

- What we all need to be monitoring
  - OUs
    - Permission changes – delegation of privileged authority
  - Group Policy
    - GPOs
      - Creation, deletion, Modification
    - OU and Domain
      - Linked GPOs
      - Inheritance blocking / Enforcement
      - Priority
  - Domain and Domain Controller security policy changes



## Analysis


- Over time
- By domain
- Bubble up outliers
  - Infrequent admins
  - Active admins
- Users and groups
  - Rarely changed
  - Frequently changed

## Windows Security Events

[1100 The event logging service has shut down](#)  
[1101 Audit events have been dropped by the transport.](#)  
[1102 The audit log was cleared](#)  
[1104 The security Log is now full](#)  
[1108 The event logging service encountered an error](#)  
[4610 An authentication package has been loaded by the Local Security Authority](#)  
[4611 A trusted logon process has been registered with the Local Security Authority](#)  
[4614 A notification package has been loaded by the Security Account Manager.](#)  
[4622 A security package has been loaded by the Local Security Authority.](#)  
[4697 A service was installed in the system](#)  
[4704 A user right was assigned](#)  
[4705 A user right was removed](#)  
[4706 A new trust was created to a domain](#)  
[4707 A trust to a domain was removed](#)  
[4713 Kerberos policy was changed](#)  
[4716 Trusted domain information was modified](#)  
[4717 System security access was granted to an account](#)  
[4718 System security access was removed from an account](#)  
[4719 System audit policy was changed](#)  
[4720 A user account was created](#)  
[4725 A user account was disabled](#)  
[4726 A user account was deleted](#)  
[4727 A security-enabled global group was created](#)  
[4728 A member was added to a security-enabled global group](#)  
[4729 A member was removed from a security-enabled global group](#)  
[4730 A security-enabled global group was deleted](#)

## Windows Security Events

[4731 A security-enabled local group was created](#)  
[4732 A member was added to a security-enabled local group](#)  
[4733 A member was removed from a security-enabled local group](#)  
[4734 A security-enabled local group was deleted](#)  
[4735 A security-enabled local group was changed](#)  
[4737 A security-enabled global group was changed](#)  
[4738 A user account was changed](#)  
[4739 Domain Policy was changed](#)  
[4754 A security-enabled universal group was created](#)  
[4755 A security-enabled universal group was changed](#)  
[4756 A member was added to a security-enabled universal group](#)  
[4757 A member was removed from a security-enabled universal group](#)  
[4758 A security-enabled universal group was deleted](#)  
[4764 A groups type was changed](#)  
[4794 An attempt was made to set the Directory Services Restore Mode administrator password](#)  
[4817 Auditing settings on object were changed.](#)  
[4819 Central Access Policies on the machine have been changed](#)  
[4865 A trusted forest information entry was added](#)  
[4866 A trusted forest information entry was removed](#)  
[4867 A trusted forest information entry was modified](#)  
[4906 The CrashOnAuditFail value has changed](#)  
[4908 Special Groups Logon table modified](#)  
[4911 Resource attributes of the object were changed](#)  
[4912 Per User Audit Policy was changed](#)  
[4913 Central Access Policy on the object was changed](#)  
[4932 Synchronization of a replica of an Active Directory naming context has begun](#)  
[5136 A directory service object was modified](#)  
[5137 A directory service object was created](#)  
[5141 A directory service object was deleted](#)  
[6145 One or more errors occurred while processing security policy in the group policy objects](#)






The Splunk App for LOGbinder







Solution comprises

- How do we pull this off for free?
  - Get Splunk Light
    - 500 MB a day free
  - From LOGbinder
    - Splunk App for LOGbinder
      - Free
  - Supercharger for Windows Event collection
    - Free for managing domain controllers



# Challenges

- Challenges with Windows security log
  - Logs are cryptic
  - Duplicate events
    - Users, group policy changes
  - Lots of events
- It's expensive, to use the free Splunk you can't be indexing noise



# Splunk Challenges

```

EventCode=4720
EventType=0
Type=Information
ComputerName=lab-0c2-50.lab.local
TaskCategory=User Account Management
OpCode=Info
RecordNumber=30821144
Keywords=Audit Success
Message=A user account was created.
  
```

```

Subject:
  Security ID: S-1-5-21-311908031-1195731464-1505490484-1805
  Account Name: rsmith
  Account Domain: LAB
  Logon ID: 0x3a76120e
  
```

```

New Account:
  Security ID: S-1-5-21-311908031-1195731464-1505490484-2331
  Account Name: cmartin
  Account Domain: LAB
  
```

```

Attributes:
  SAM Account Name: cmartin
  Display Name: Chris Martin
  User Principal Name: cmartin@lab.local
  Home Directory: -
  
```

~~Splunk native parsing~~



```

 Account_Name rsmith
 cmartin
  
```

With our app!



<input type="checkbox"/>	SourceName	Microsoft Windows security auditing.
<input type="checkbox"/>	SubjectAccountDomain	LAB
<input type="checkbox"/>	SubjectAccountName	rsmith
<input type="checkbox"/>	SubjectLogonID	0x3a76120e
<input type="checkbox"/>	SubjectSecurityID	S-1-5-21-311908031-1195731464-1505490484-1805
<input type="checkbox"/>	TargetAccountDomain	LAB
<input type="checkbox"/>	TargetAccountName	cmartin
<input type="checkbox"/>	TargetSecurityID	S-1-5-21-311908031-1195731464-1505490484-2331
<input type="checkbox"/>	TaskCategory	User Account Management

And it's at search time not at indexing! So your existing logs work.



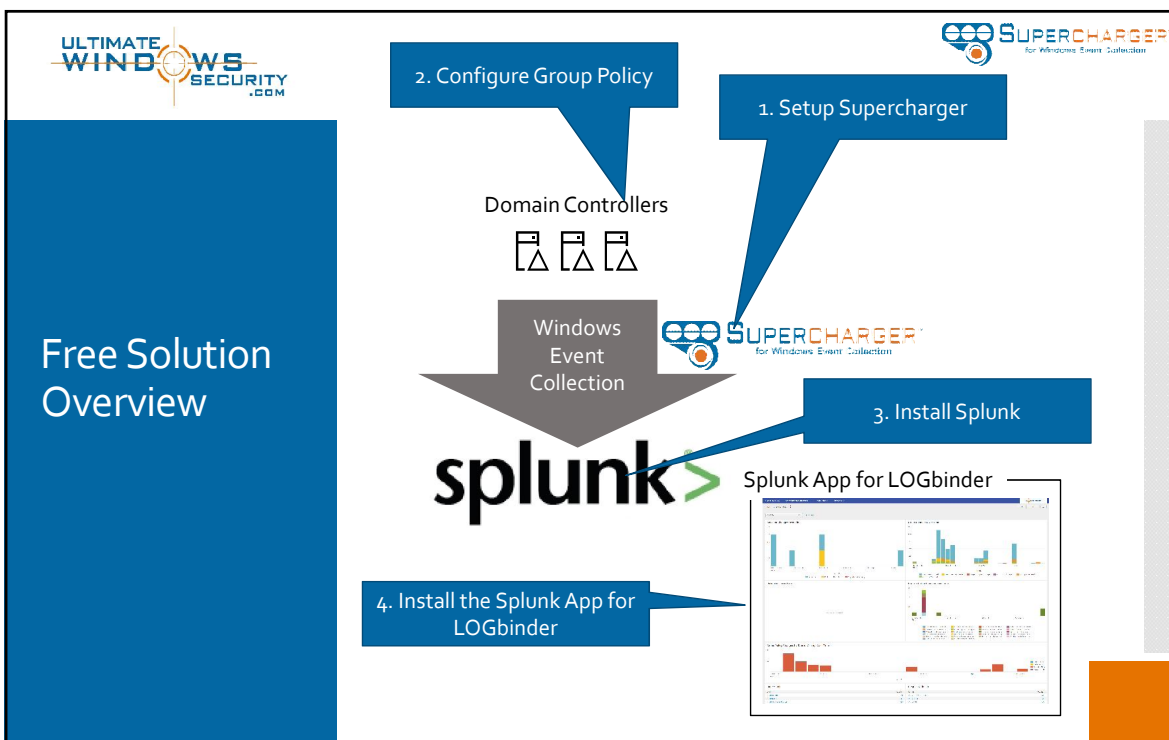
## WEC filtering at the source

- Domain controller security logs are huge
- How do you get just significant AD change events into Splunk and stay under the 500MB a day limit?
- Windows Event Collection
  - Xpath filtering at the source
  - Supercharger has a built-in filter for this very purpose
  - On our domain controllers only 0.1% events are actually forwarded to Splunk



## Splunk and Windows challenges

- How to distinguish events from domain controllers from other member servers?
  - Nobody wants to maintain a list of DCs
  - Our app builds a list of domain controllers automatically from event ID 4932
- How deal with repetitive events?
  - Group By
  - "Transactions"





**How to do it**

ULTIMATE WINDOWS SECURITY .COM

SUPERCHARGER<sup>™</sup>  
for Windows Event Collection

- Step by step instructions
  - <https://support.logbinder.com/Supercharger/50135/8-Install-Supercharger-with-Splunk-Light-and-the-Splunk-App-for-LOGbinder>
- Download Splunk Light
  - [https://www.splunk.com/en\\_us/download/splunk-light.html](https://www.splunk.com/en_us/download/splunk-light.html)
- Download Supercharger
  - <https://www.logbinder.com/Form/SCDownload>
- Download Splunk App for LOGbinder
  - <https://www.logbinder.com/Form/SplunkDownload>
- Get help at
  - <https://forum.logbinder.com/>
  - Look for the forum: Splunk App for LOGbinder







## Bottom line

- Everyone can monitor important AD changes using free technology
- This project demonstrates the power of Windows Event Collection
  - Especially Xpath filters at the source
- Domain controllers are just the beginning with what you can accomplish with Supercharger for Windows Event Collection
  - <https://www.logbinder.com/Products/Supercharger/>

© 2017 Monterey Technology Group Inc.



## Bottom line

- Our Splunk App also analyzes events from
  - LOGbinder for Exchange
    - Non-owner mailbox auditing
    - Privileged Access
  - LOGbinder for SharePoint
    - End-user activity
    - Privileged Access
  - LOGbinder for SQL Server
    - Zero-touch
    - Privileged Access
    - Database operations
- <https://www.logbinder.com/Products/>

© 2017 Monterey Technology Group Inc.