ULTIMATE WINDOWS SECURITY .COM ™

Monitoring Group Membership Changes in Active Directory

Sponsored by

solarwinds

ULTIMATE WINDOWS SECURITY .COM

solarwinds

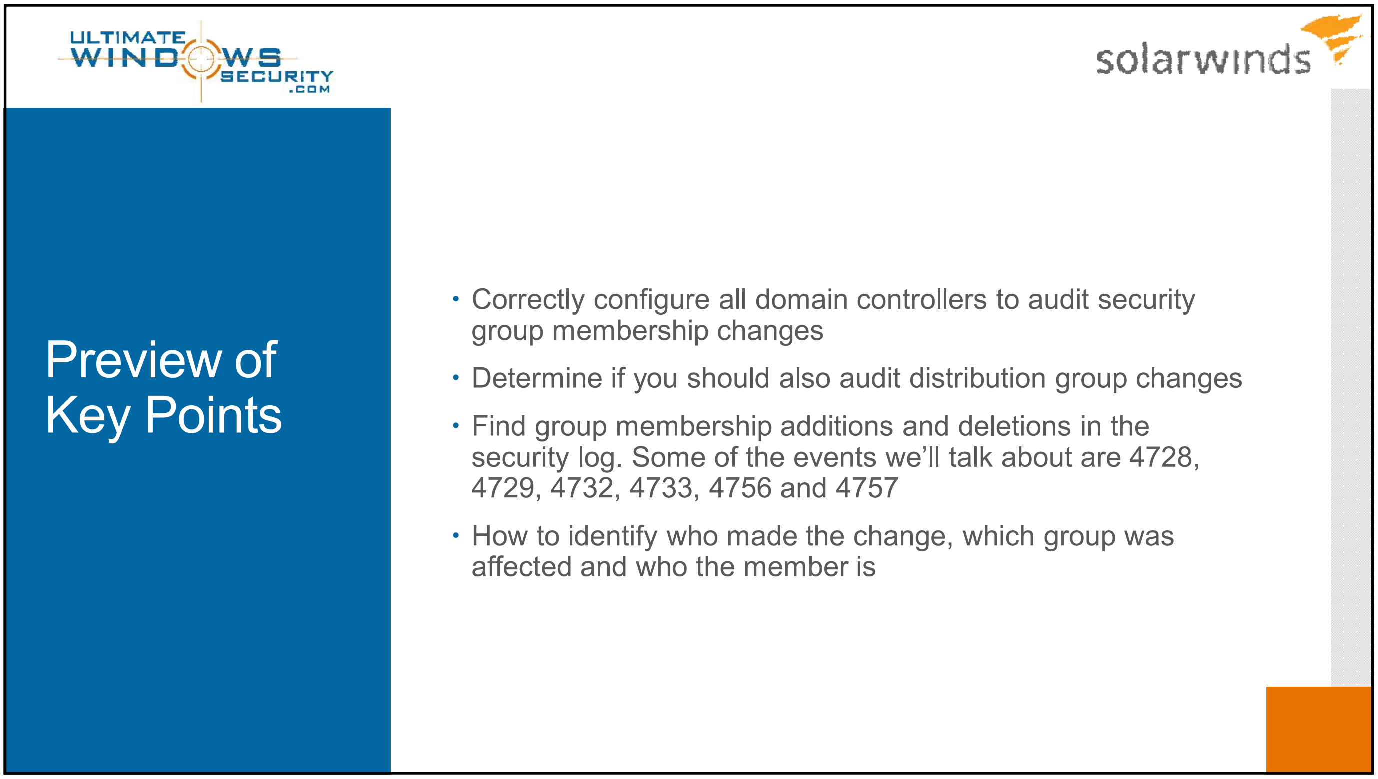
Thanks to

- Made possible by

solarwinds

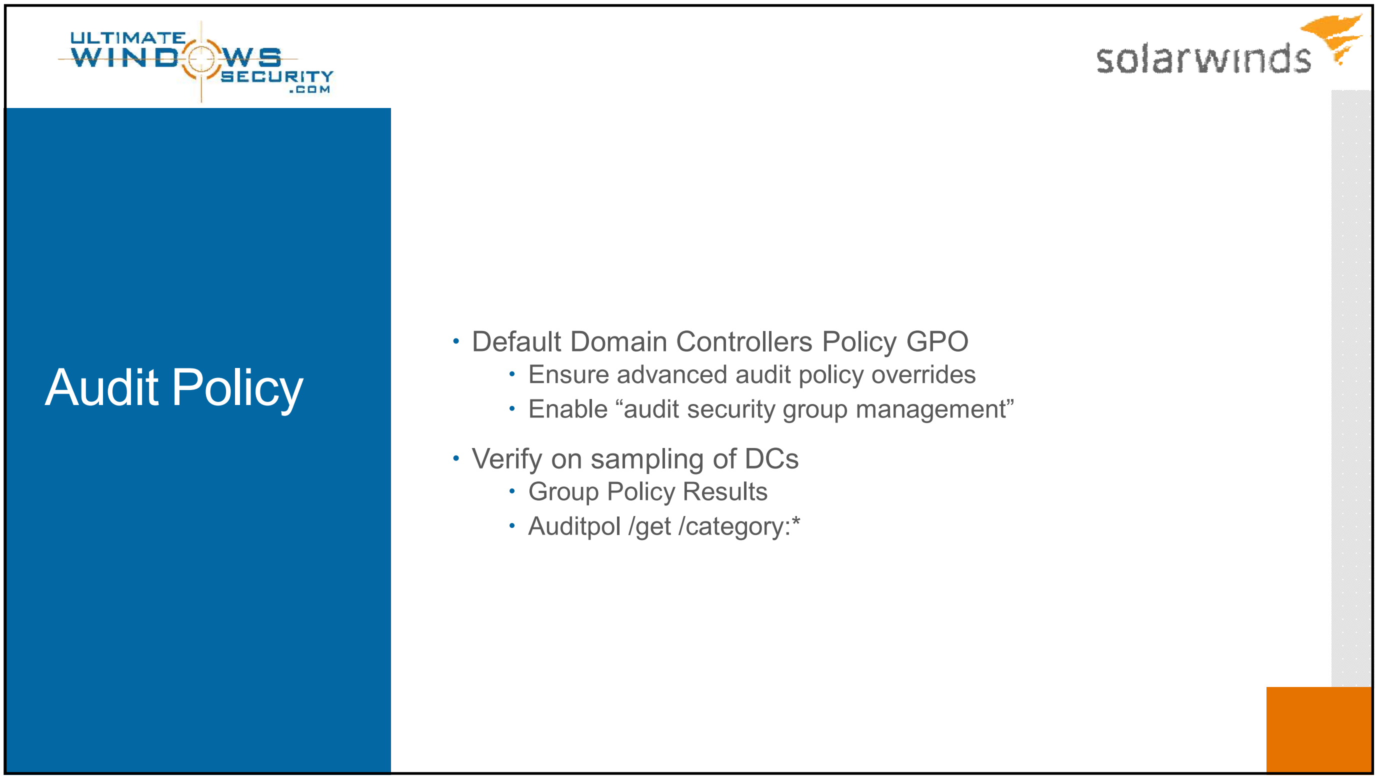
LOG & EVENT MANAGER

www.solarwinds.com



Preview of Key Points

- Correctly configure all domain controllers to audit security group membership changes
- Determine if you should also audit distribution group changes
- Find group membership additions and deletions in the security log. Some of the events we'll talk about are 4728, 4729, 4732, 4733, 4756 and 4757
- How to identify who made the change, which group was affected and who the member is



Audit Policy

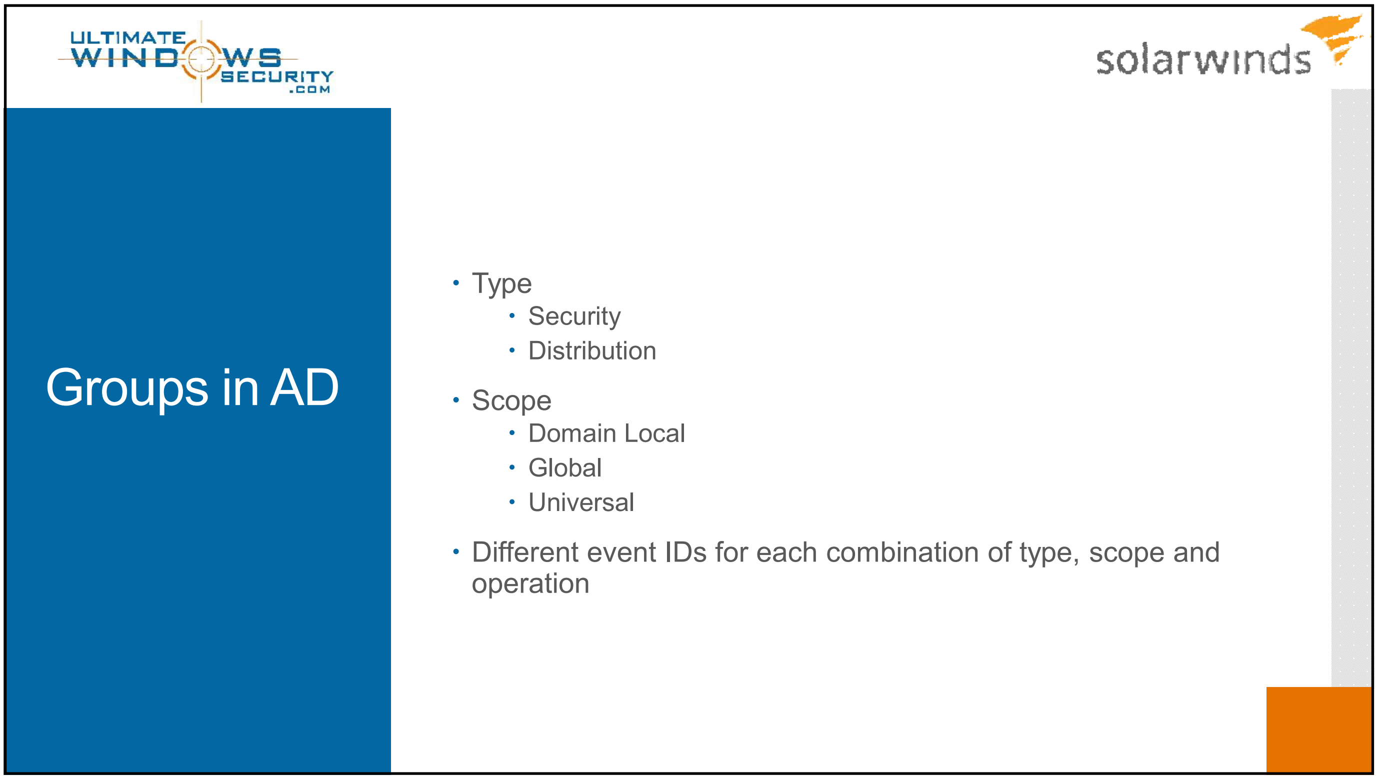
- Default Domain Controllers Policy GPO
  - Ensure advanced audit policy overrides
  - Enable "audit security group management"
- Verify on sampling of DCs
  - Group Policy Results
  - Auditpol /get /category:*

Groups in AD

- 2 types of groups
  - Security
    - Use for permissions and rights
    - Called “security enabled” in security log
  - Distribution
    - Used in Exchange
    - Called “security disabled” in security log
- Different audit subcategories for each type of group

Audit Policy

- Audit distribution group changes?
  - Do you use distribution groups in Exchange to route confidential email?

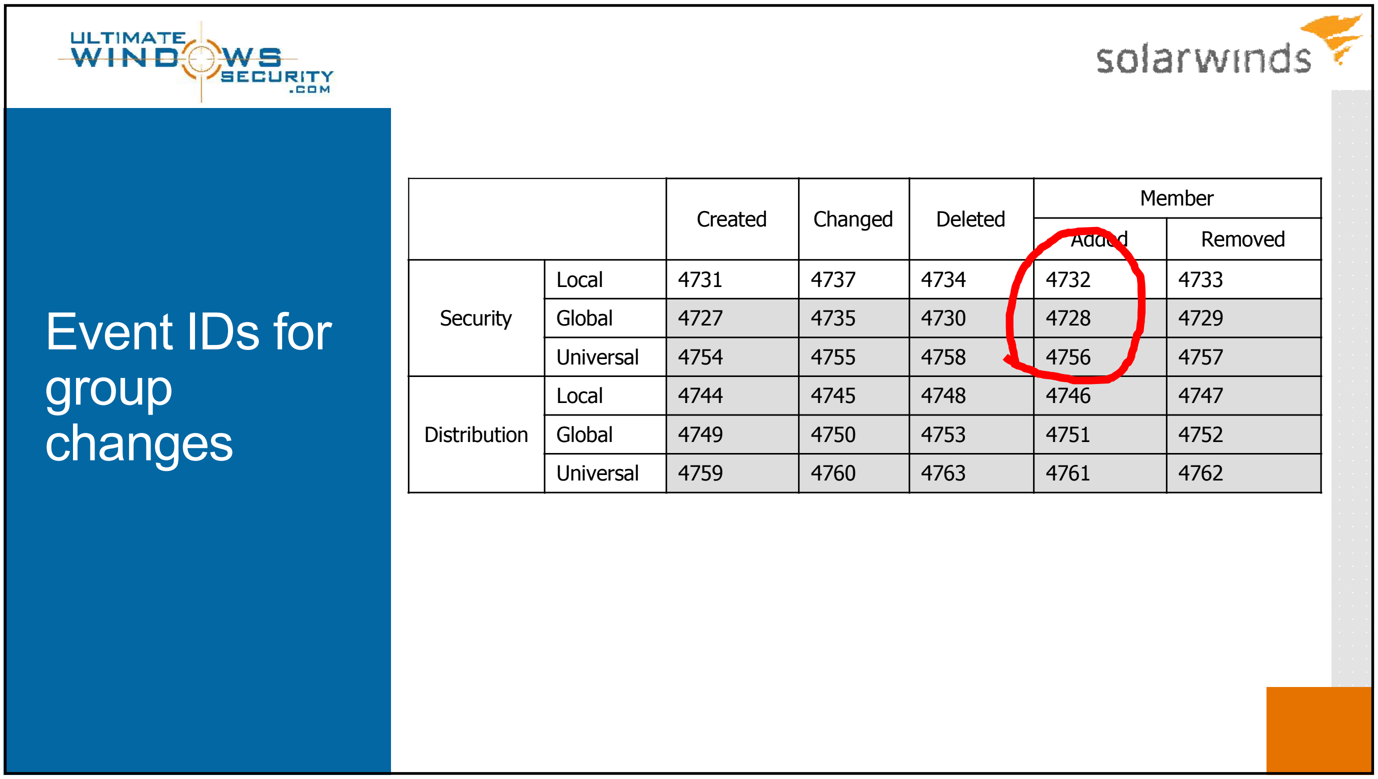


ULTIMATE WINDOWS SECURITY .COM

solarwinds

Groups in AD

- Type
  - Security
  - Distribution
- Scope
  - Domain Local
  - Global
  - Universal
- Different event IDs for each combination of type, scope and operation

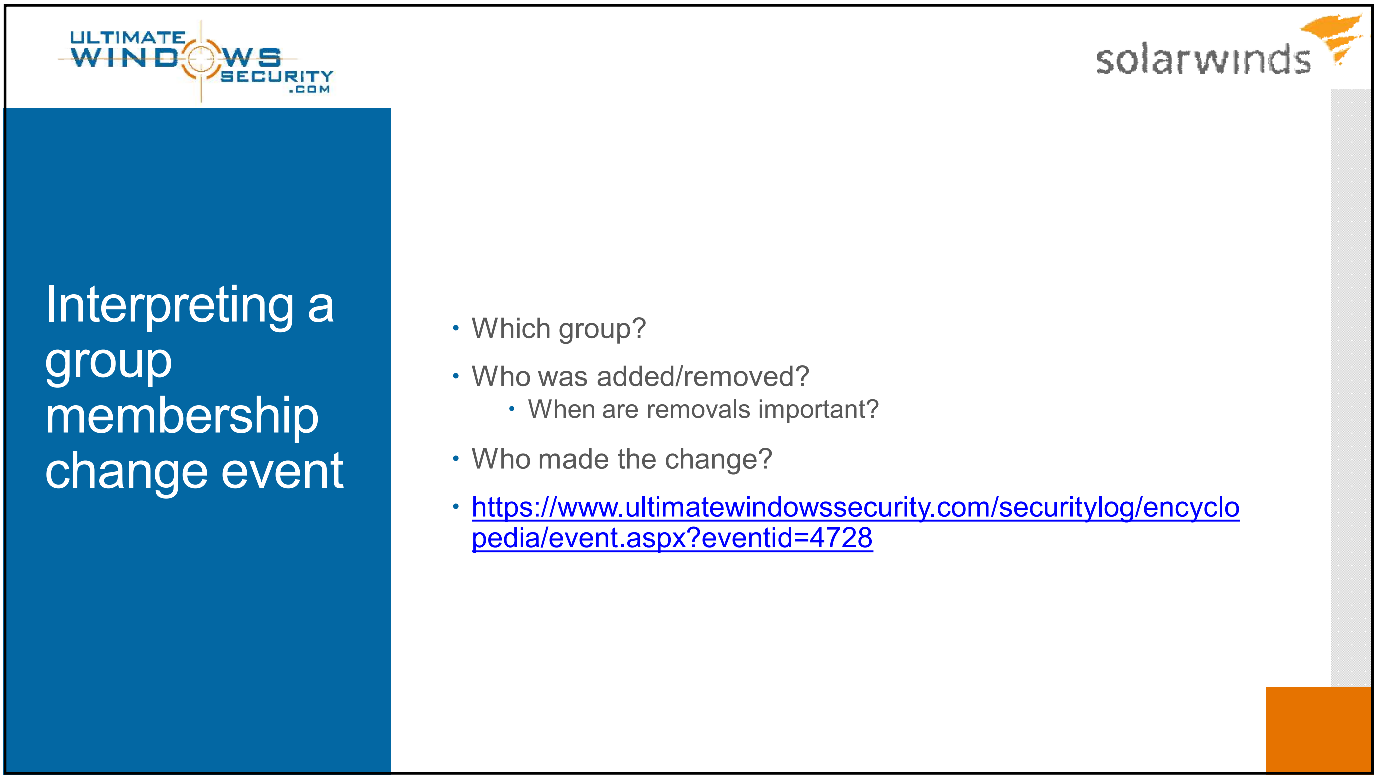


ULTIMATE WINDOWS SECURITY .COM

solarwinds

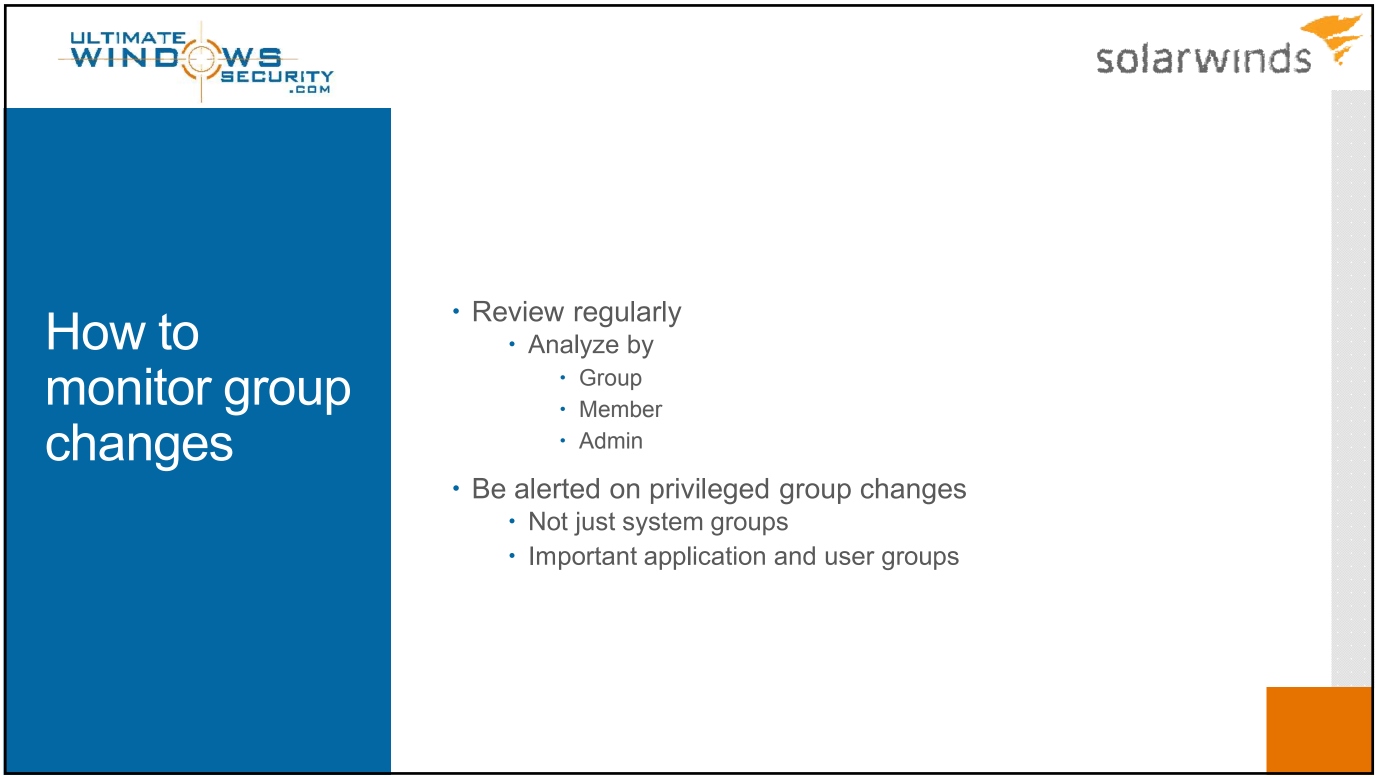
Event IDs for group changes

		Created	Changed	Deleted	Member	
					Added	Removed
Security	Local	4731	4737	4734	4732	4733
	Global	4727	4735	4730	4728	4729
	Universal	4754	4755	4758	4756	4757
Distribution	Local	4744	4745	4748	4746	4747
	Global	4749	4750	4753	4751	4752
	Universal	4759	4760	4763	4761	4762



Interpreting a group membership change event

- Which group?
- Who was added/removed?
  - When are removals important?
- Who made the change?
- https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventid=4728



How to monitor group changes

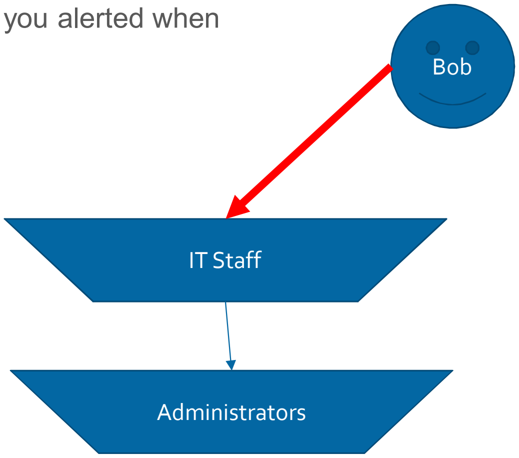
- Review regularly
  - Analyze by
    - Group
    - Member
    - Admin
- Be alerted on privileged group changes
  - Not just system groups
  - Important application and user groups

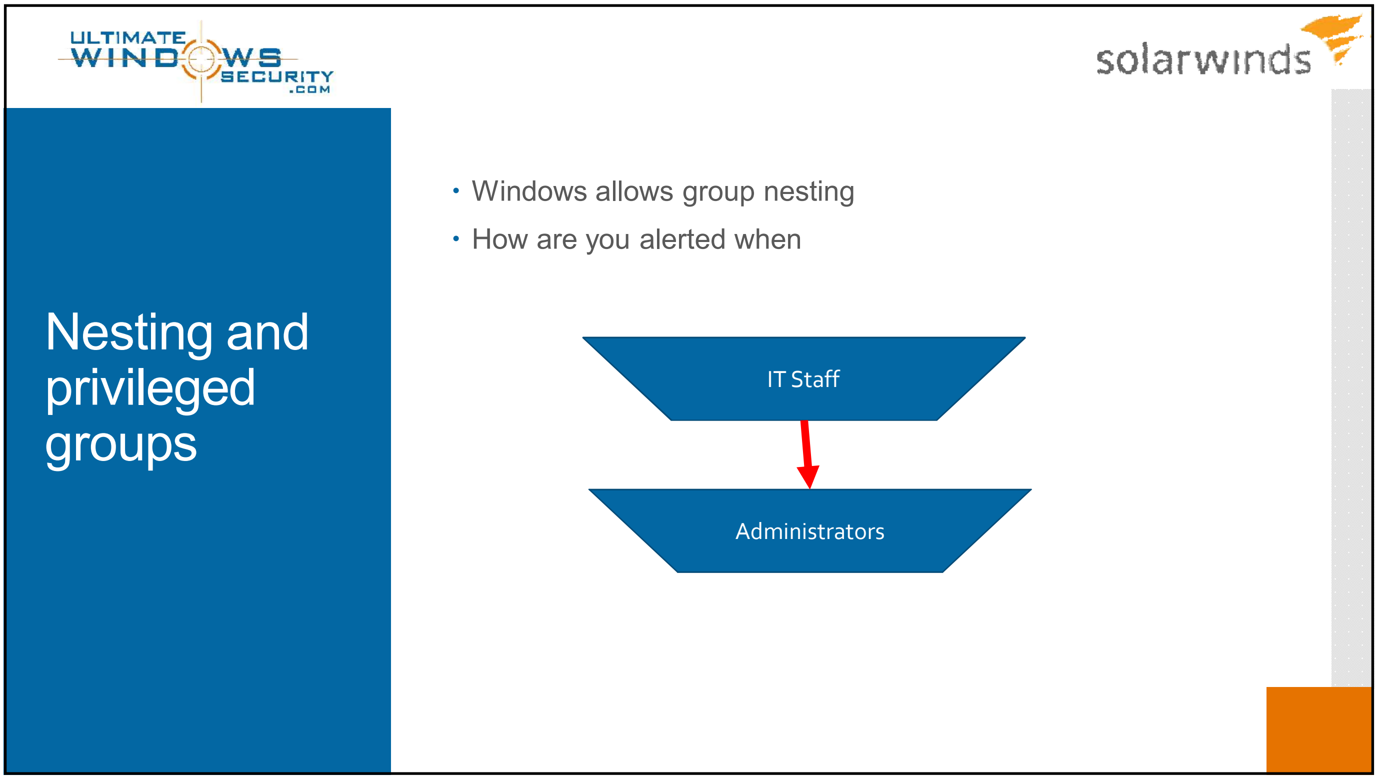
Custom groups

- How to alert on custom privileged groups?
  - Naming convention
  - Static list

Nesting and privileged groups

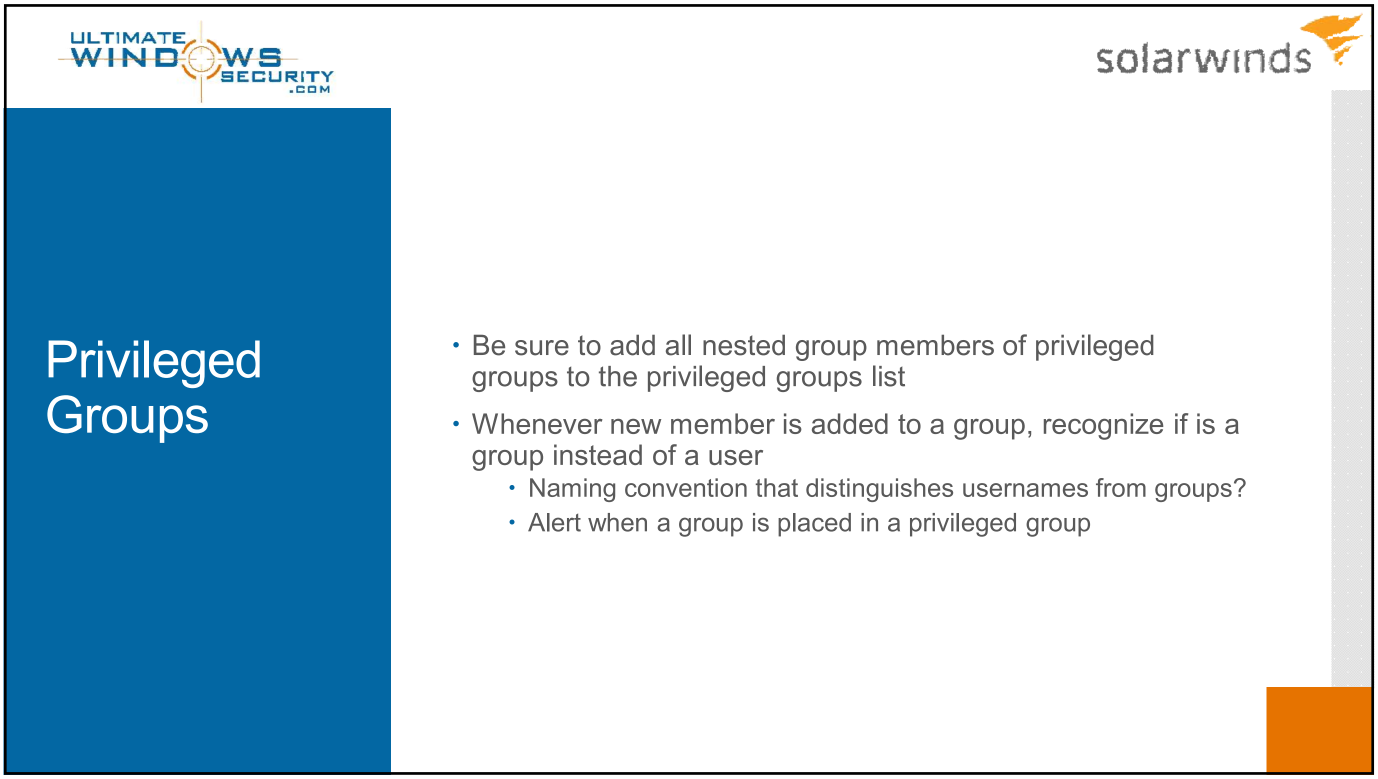
- Windows allows group nesting
- How are you alerted when





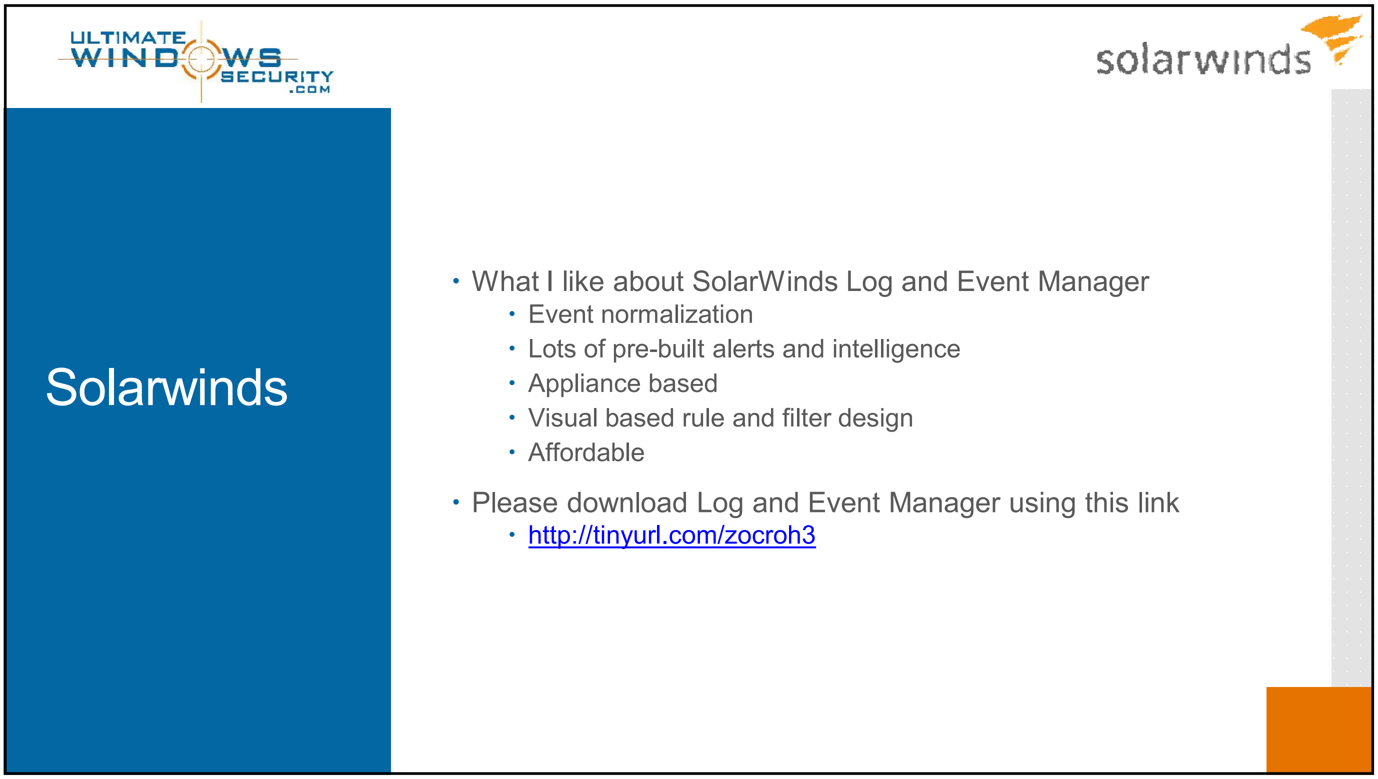
Nesting and privileged groups

- Windows allows group nesting
- How are you alerted when



Privileged Groups

- Be sure to add all nested group members of privileged groups to the privileged groups list
- Whenever new member is added to a group, recognize if is a group instead of a user
  - Naming convention that distinguishes usernames from groups?
  - Alert when a group is placed in a privileged group



Solarwinds

- What I like about SolarWinds Log and Event Manager
  - Event normalization
  - Lots of pre-built alerts and intelligence
  - Appliance based
  - Visual based rule and filter design
  - Affordable
- Please download Log and Event Manager using this link
  - http://tinyurl.com/zocroh3