# Analyzing Logon Failures in the Windows Security Log

Sponsored by

solarwinds

## Thanks to

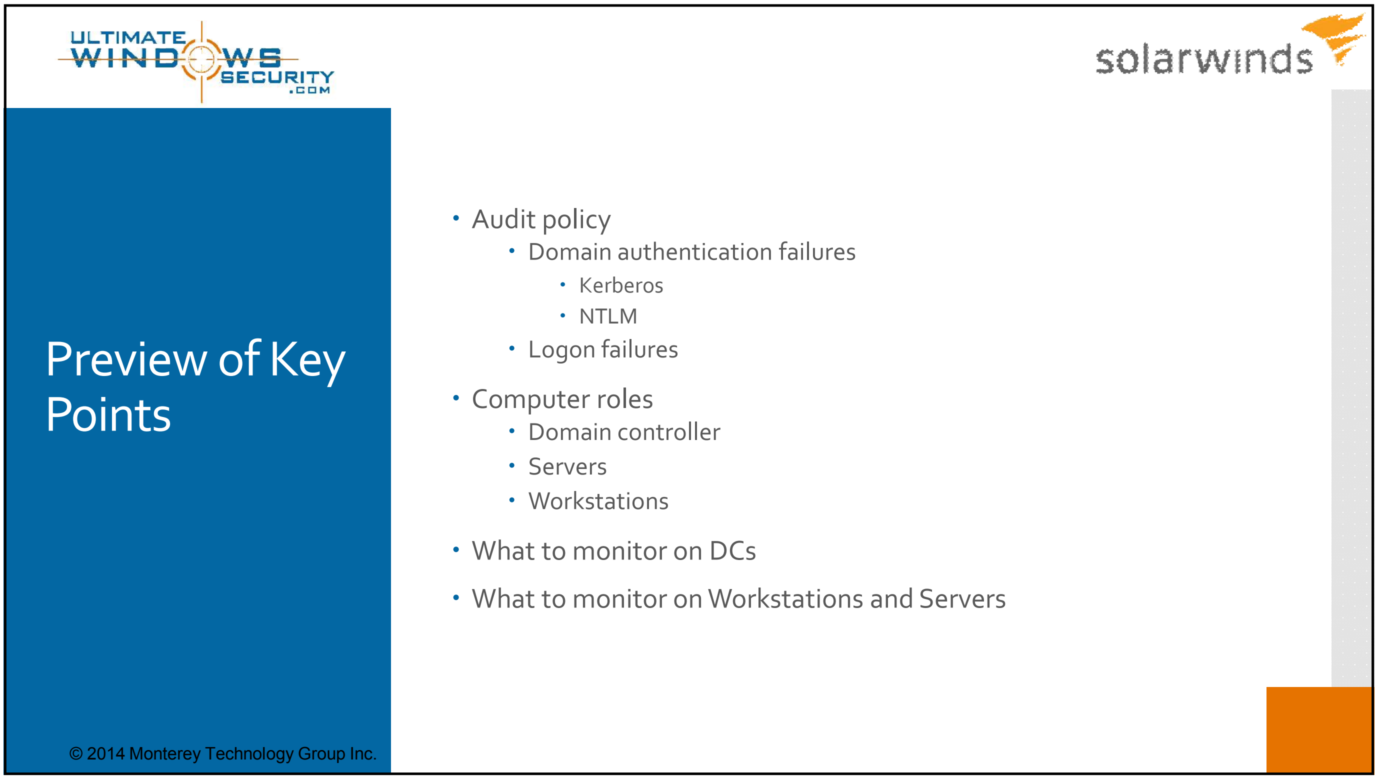
- Made possible by

solarwinds

LOG & EVENT MANAGER

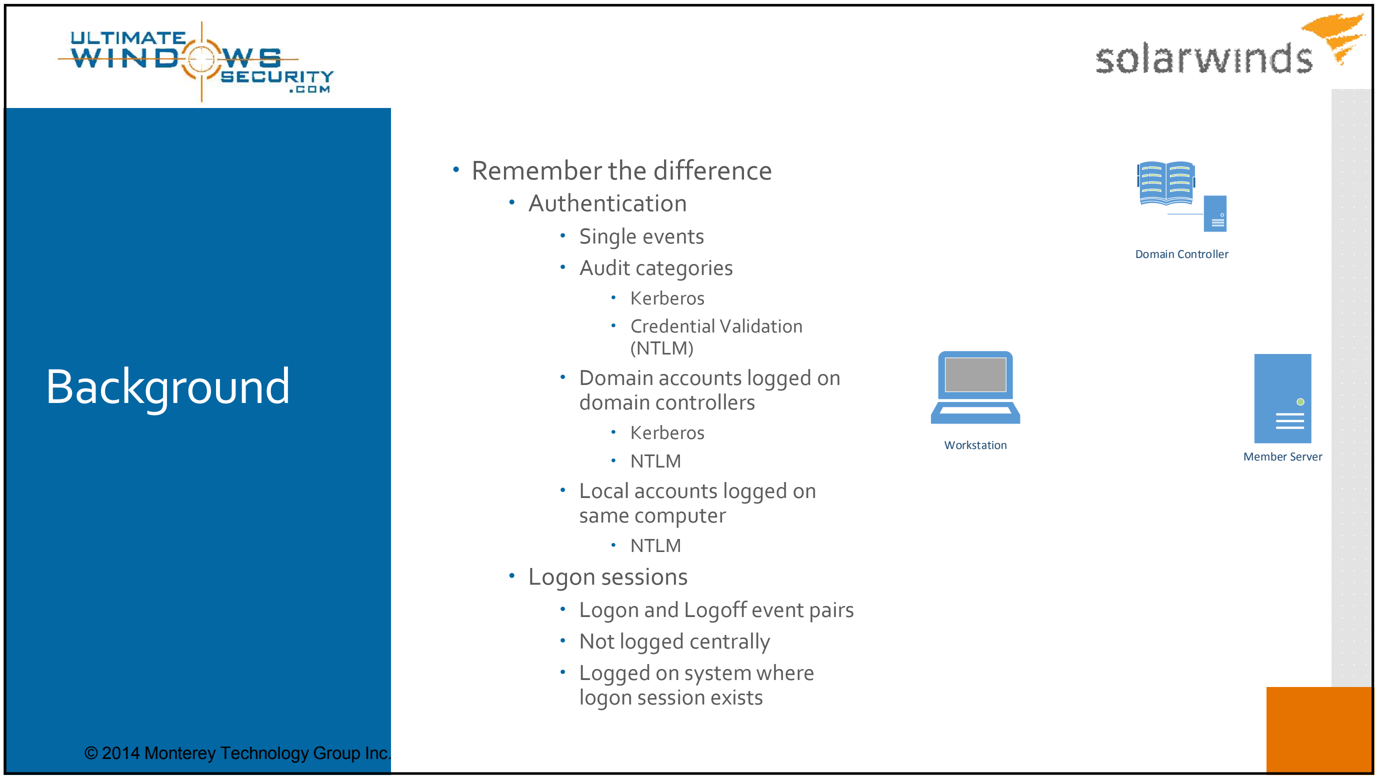
www.solarwinds.com

Nicole Pauls, Director of Product Management



## Preview of Key Points

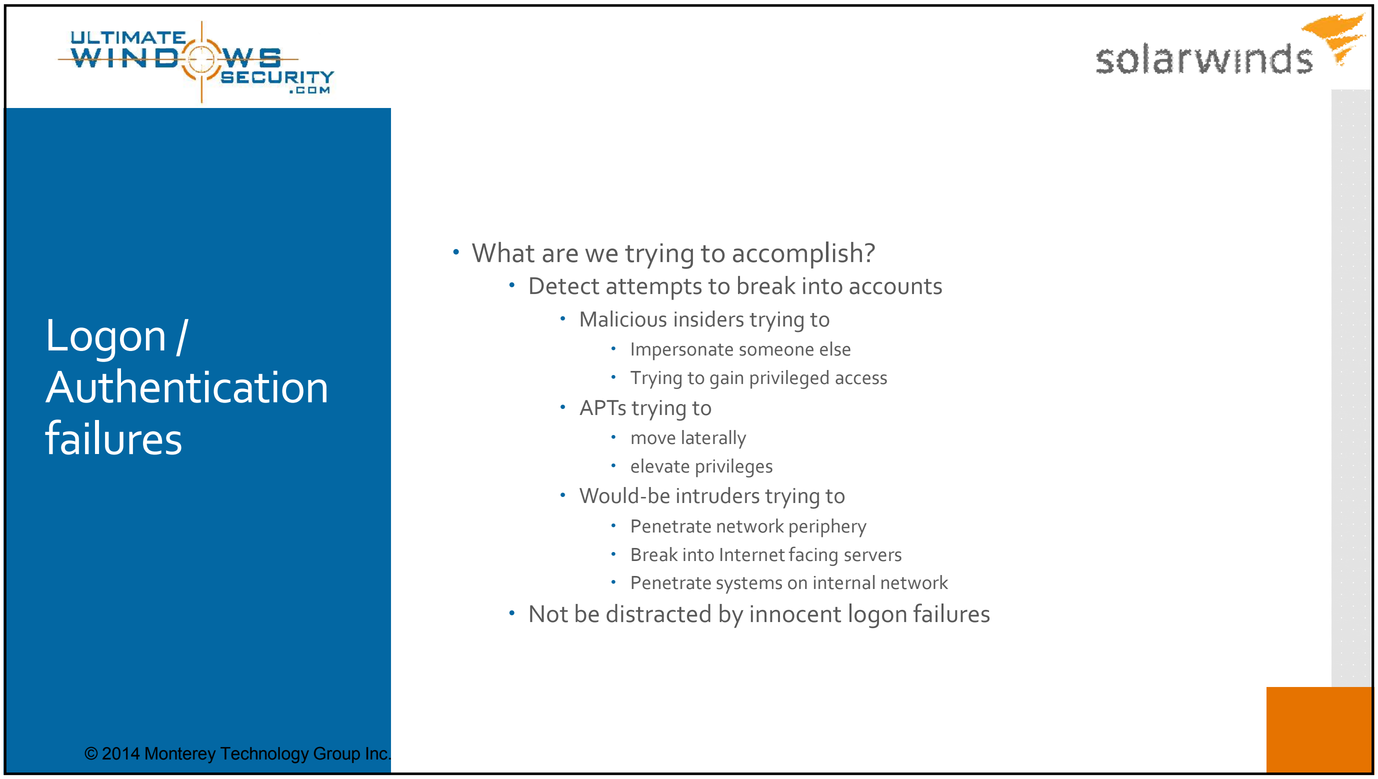
- Audit policy
  - Domain authentication failures
    - Kerberos
    - NTLM
  - Logon failures
- Computer roles
  - Domain controller
  - Servers
  - Workstations
- What to monitor on DCs
- What to monitor on Workstations and Servers



## Background

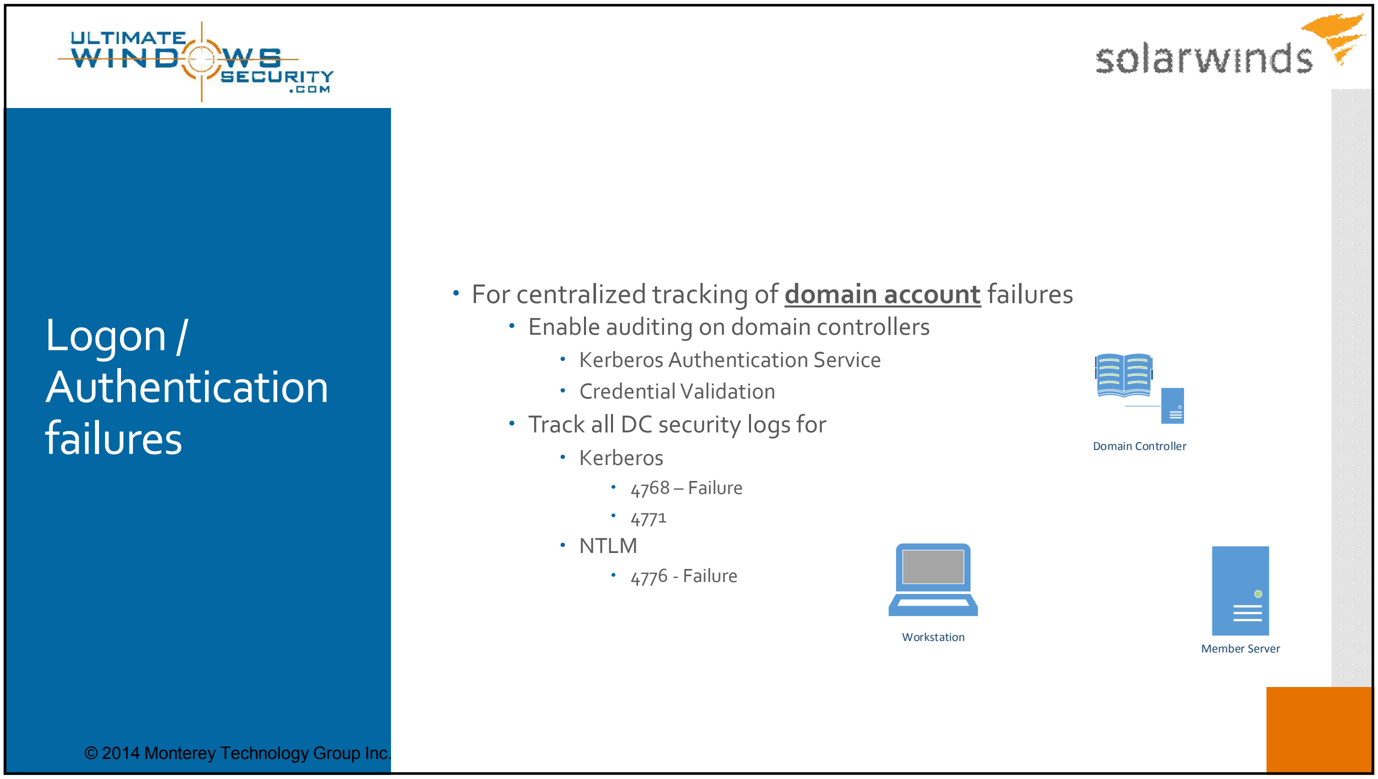
- Remember the difference
  - Authentication
    - Single events
    - Audit categories
      - Kerberos
      - Credential Validation (NTLM)
    - Domain accounts logged on domain controllers
      - Kerberos
      - NTLM
    - Local accounts logged on same computer
      - NTLM
  - Logon sessions
    - Logon and Logoff event pairs
    - Not logged centrally
    - Logged on system where logon session exists

Domain Controller
Workstation
Member Server



## Logon / Authentication failures

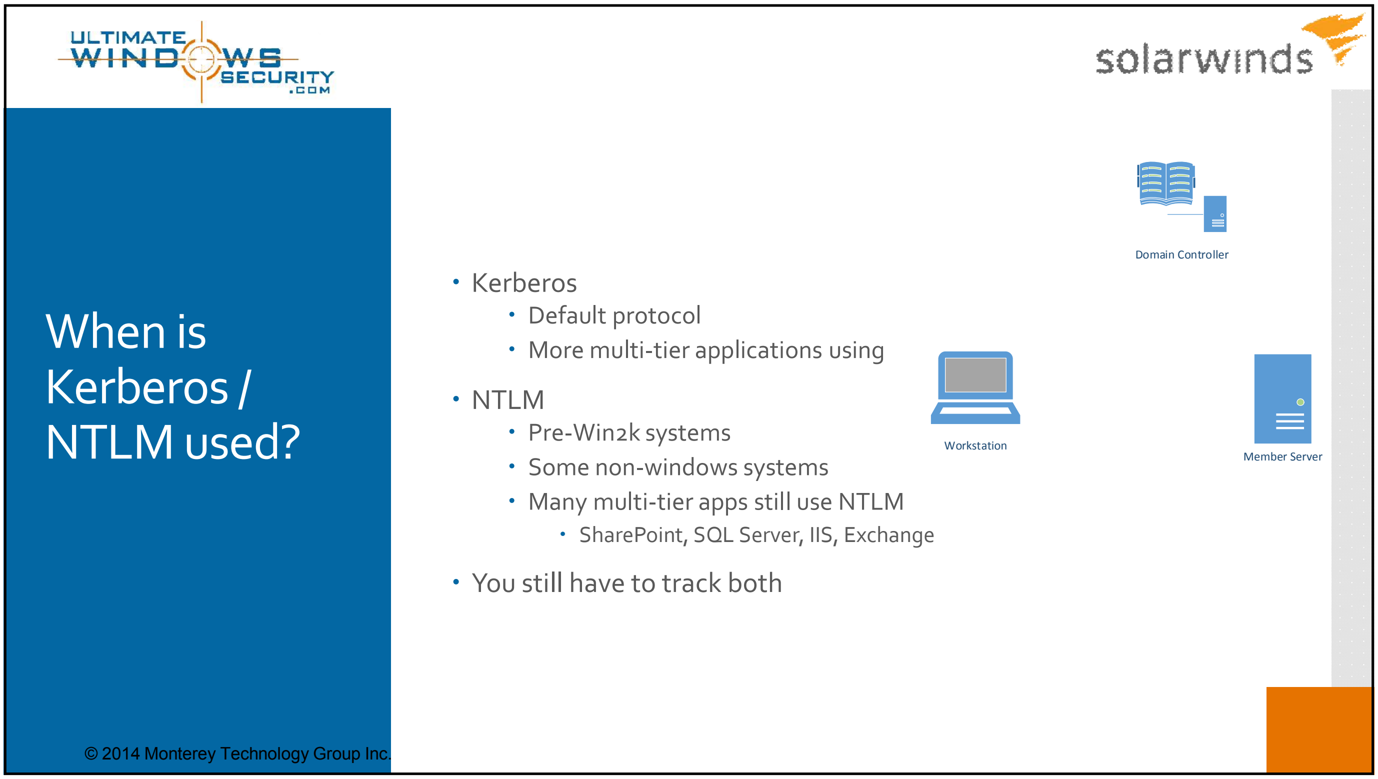
- What are we trying to accomplish?
  - Detect attempts to break into accounts
    - Malicious insiders trying to
      - Impersonate someone else
      - Trying to gain privileged access
    - APTs trying to
      - move laterally
      - elevate privileges
    - Would-be intruders trying to
      - Penetrate network periphery
      - Break into Internet facing servers
      - Penetrate systems on internal network
  - Not be distracted by innocent logon failures



## Logon / Authentication failures

- For centralized tracking of **domain account** failures
  - Enable auditing on domain controllers
    - Kerberos Authentication Service
    - Credential Validation
  - Track all DC security logs for
    - Kerberos
      - 4768 – Failure
      - 4771
    - NTLM
      - 4776 - Failure

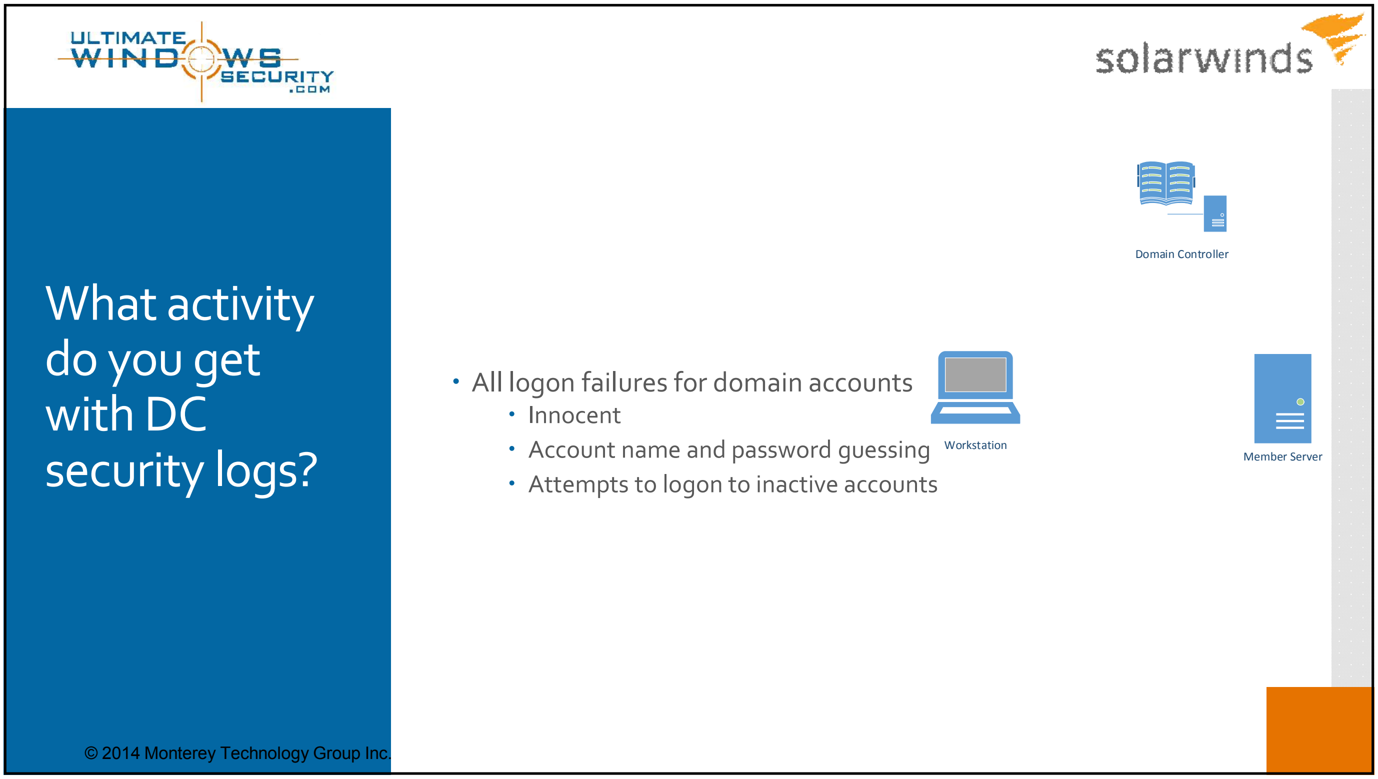
Domain Controller
Workstation
Member Server



# When is Kerberos / NTLM used?

- Kerberos
  - Default protocol
  - More multi-tier applications using
- NTLM
  - Pre-Win2k systems
  - Some non-windows systems
  - Many multi-tier apps still use NTLM
    - SharePoint, SQL Server, IIS, Exchange
- You still have to track both

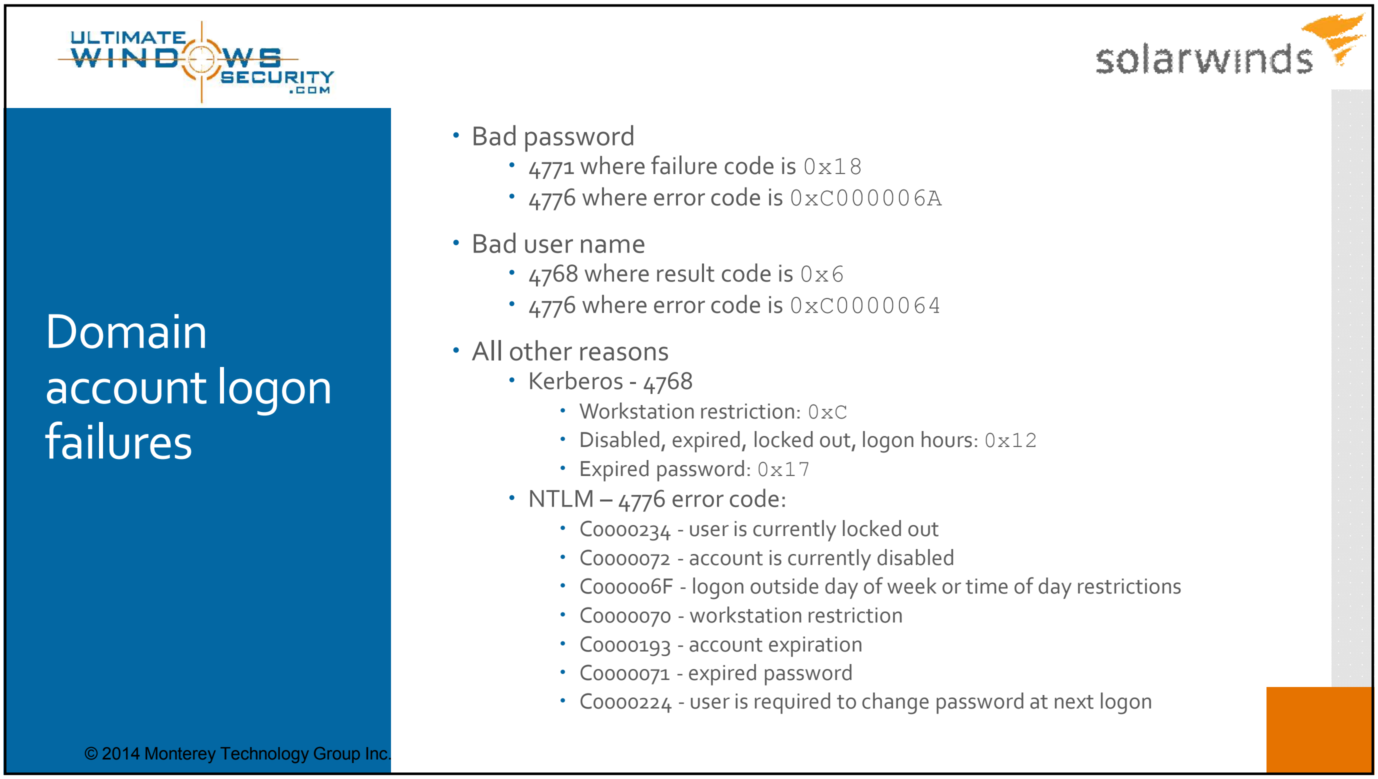
Domain Controller
Workstation
Member Server



# What activity do you get with DC security logs?

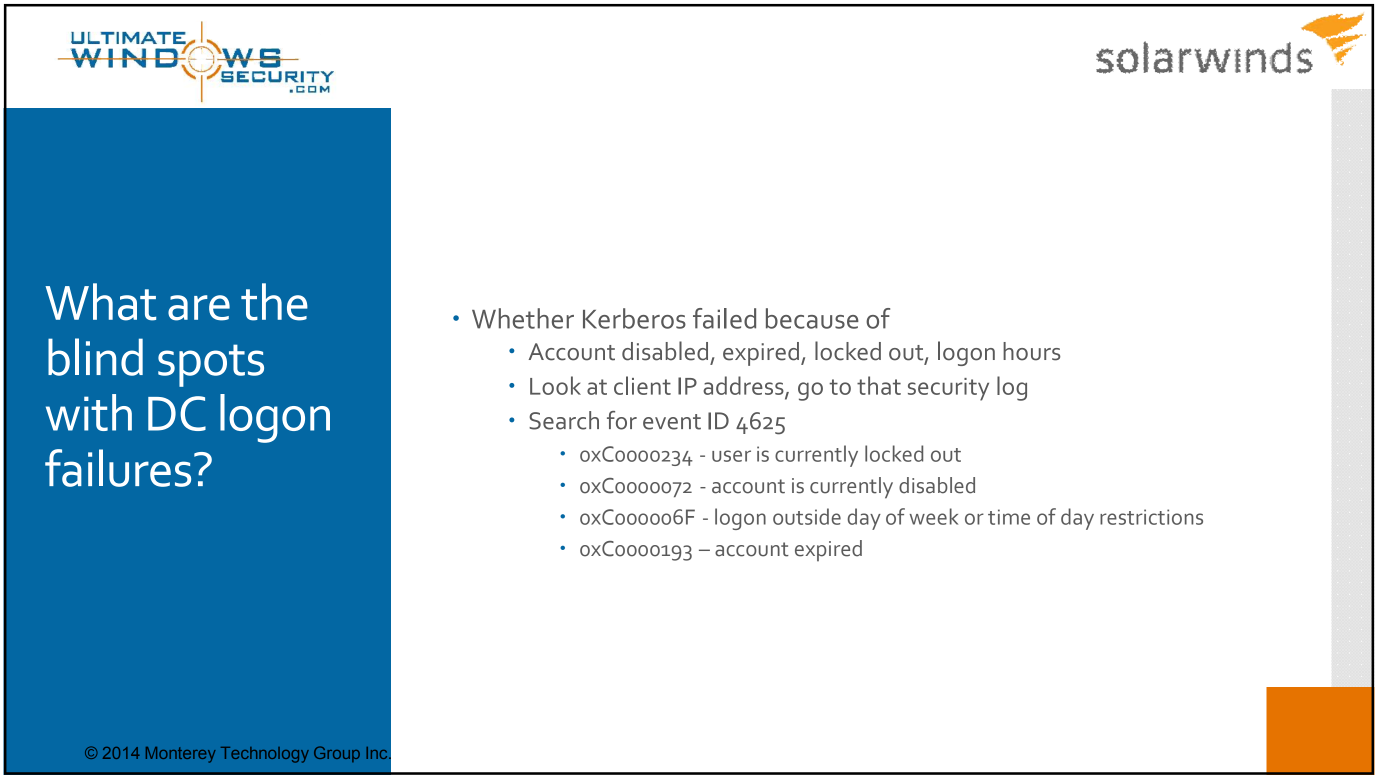
- All logon failures for domain accounts
  - Innocent
  - Account name and password guessing
  - Attempts to logon to inactive accounts

Domain Controller
Workstation
Member Server



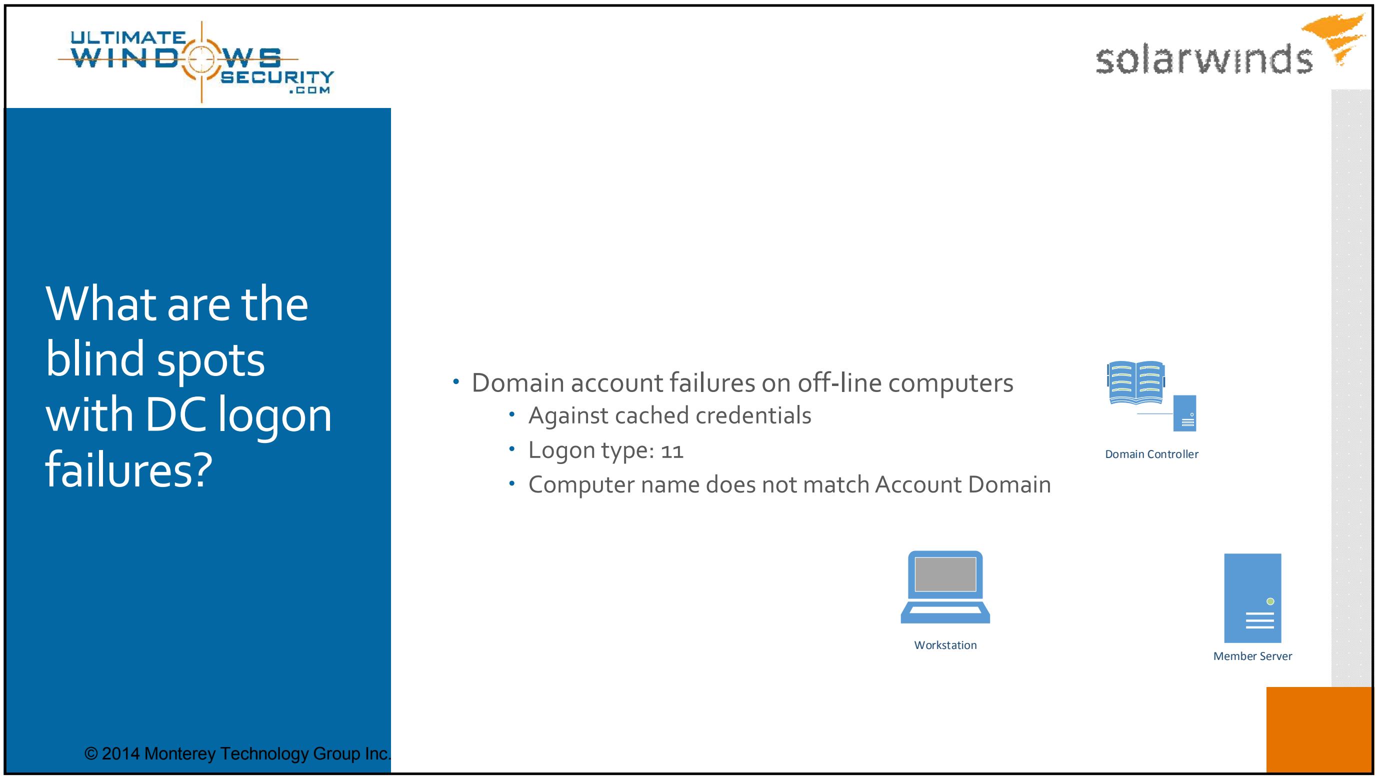
## Domain account logon failures

- Bad password
  - 4771 where failure code is `0x18`
  - 4776 where error code is `0xC000006A`
- Bad user name
  - 4768 where result code is `0x6`
  - 4776 where error code is `0xC0000064`
- All other reasons
  - Kerberos - 4768
    - Workstation restriction: `0xC`
    - Disabled, expired, locked out, logon hours: `0x12`
    - Expired password: `0x17`
  - NTLM – 4776 error code:
    - C0000234 - user is currently locked out
    - C0000072 - account is currently disabled
    - C000006F - logon outside day of week or time of day restrictions
    - C0000070 - workstation restriction
    - C0000193 - account expiration
    - C0000071 - expired password
    - C0000224 - user is required to change password at next logon



## What are the blind spots with DC logon failures?

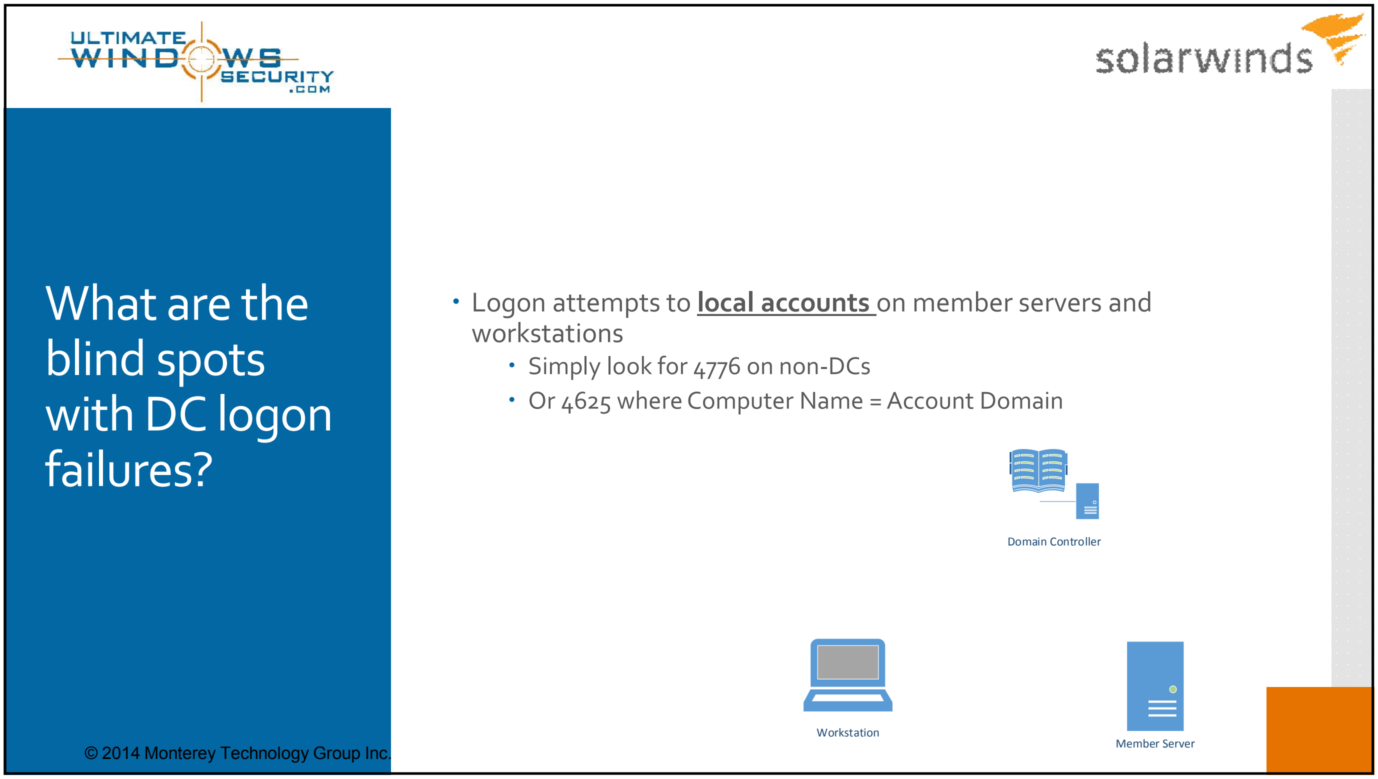
- Whether Kerberos failed because of
  - Account disabled, expired, locked out, logon hours
  - Look at client IP address, go to that security log
  - Search for event ID 4625
    - 0xC0000234 - user is currently locked out
    - 0xC0000072 - account is currently disabled
    - 0xC000006F - logon outside day of week or time of day restrictions
    - 0xC0000193 – account expired



## What are the blind spots with DC logon failures?

- Domain account failures on off-line computers
  - Against cached credentials
  - Logon type: 11
  - Computer name does not match Account Domain

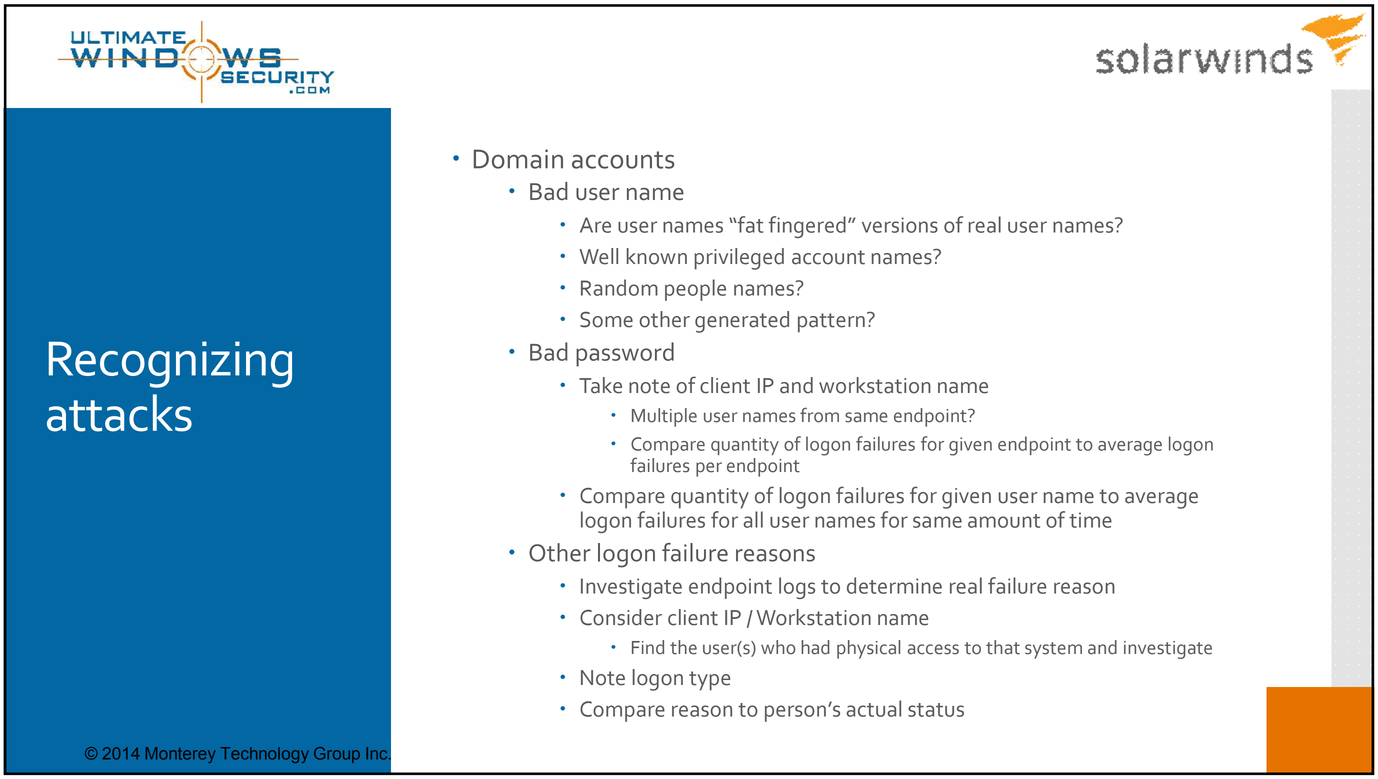
Domain Controller
Workstation
Member Server



## What are the blind spots with DC logon failures?

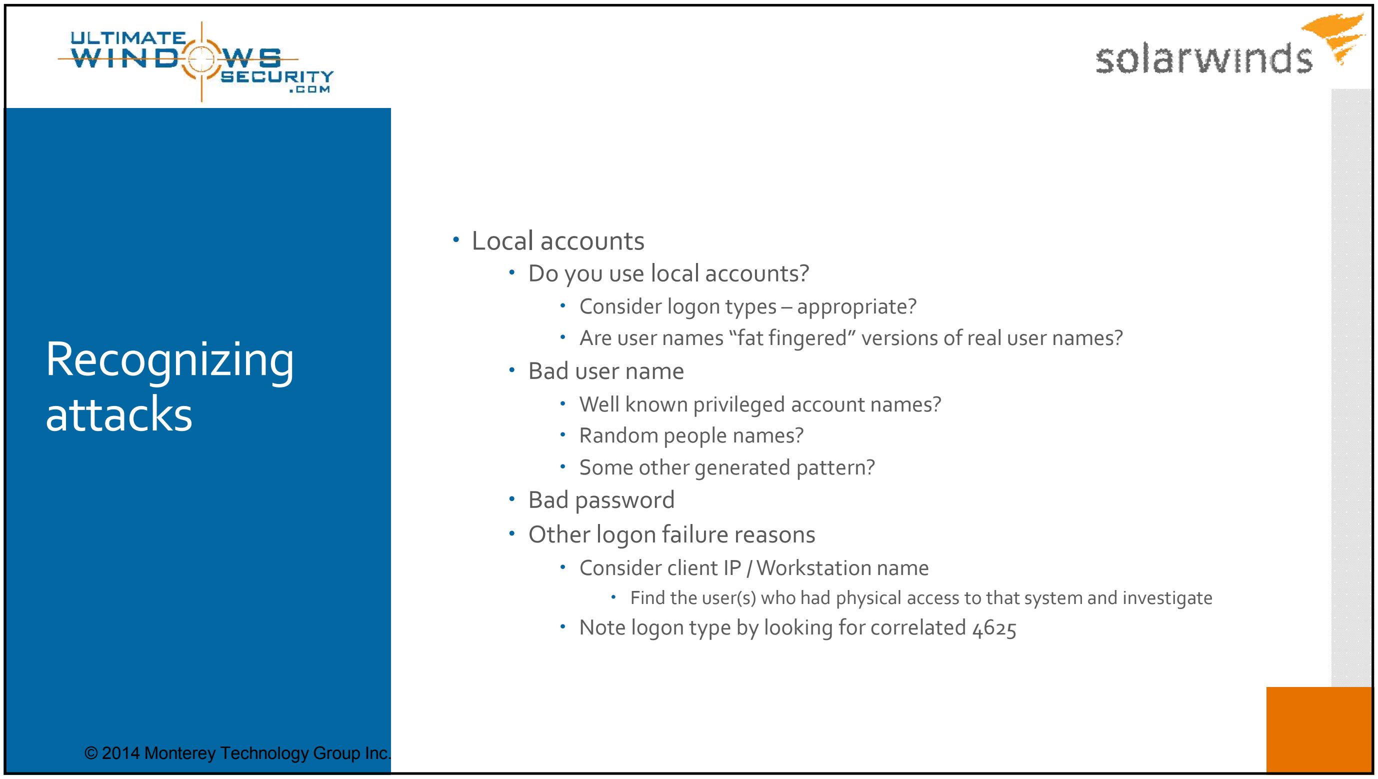
- Logon attempts to **local accounts** on member servers and workstations
  - Simply look for 4776 on non-DCs
  - Or 4625 where Computer Name = Account Domain

Domain Controller
Workstation
Member Server



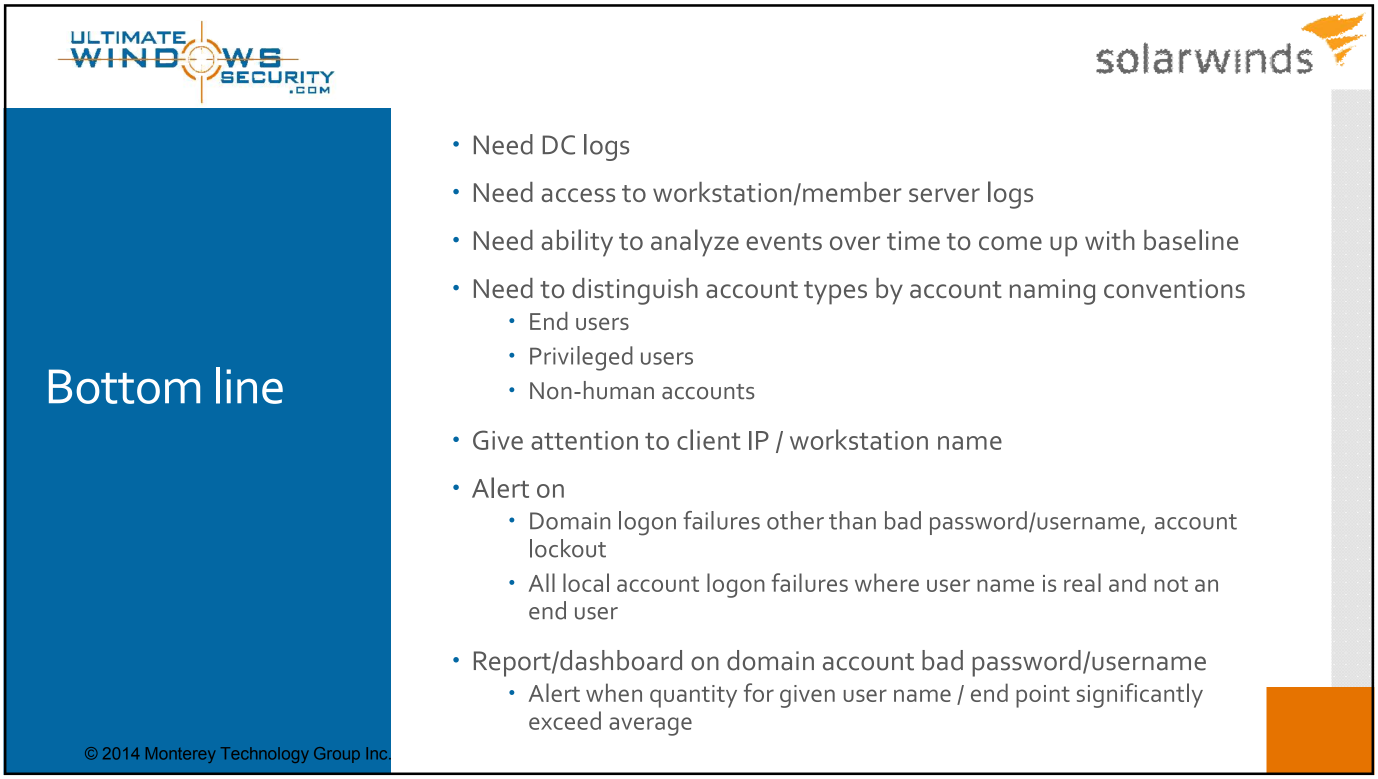
## Recognizing attacks

- Domain accounts
  - Bad user name
    - Are user names "fat fingered" versions of real user names?
    - Well known privileged account names?
    - Random people names?
    - Some other generated pattern?
  - Bad password
    - Take note of client IP and workstation name
      - Multiple user names from same endpoint?
      - Compare quantity of logon failures for given endpoint to average logon failures per endpoint
    - Compare quantity of logon failures for given user name to average logon failures for all user names for same amount of time
  - Other logon failure reasons
    - Investigate endpoint logs to determine real failure reason
    - Consider client IP / Workstation name
      - Find the user(s) who had physical access to that system and investigate
    - Note logon type
    - Compare reason to person's actual status



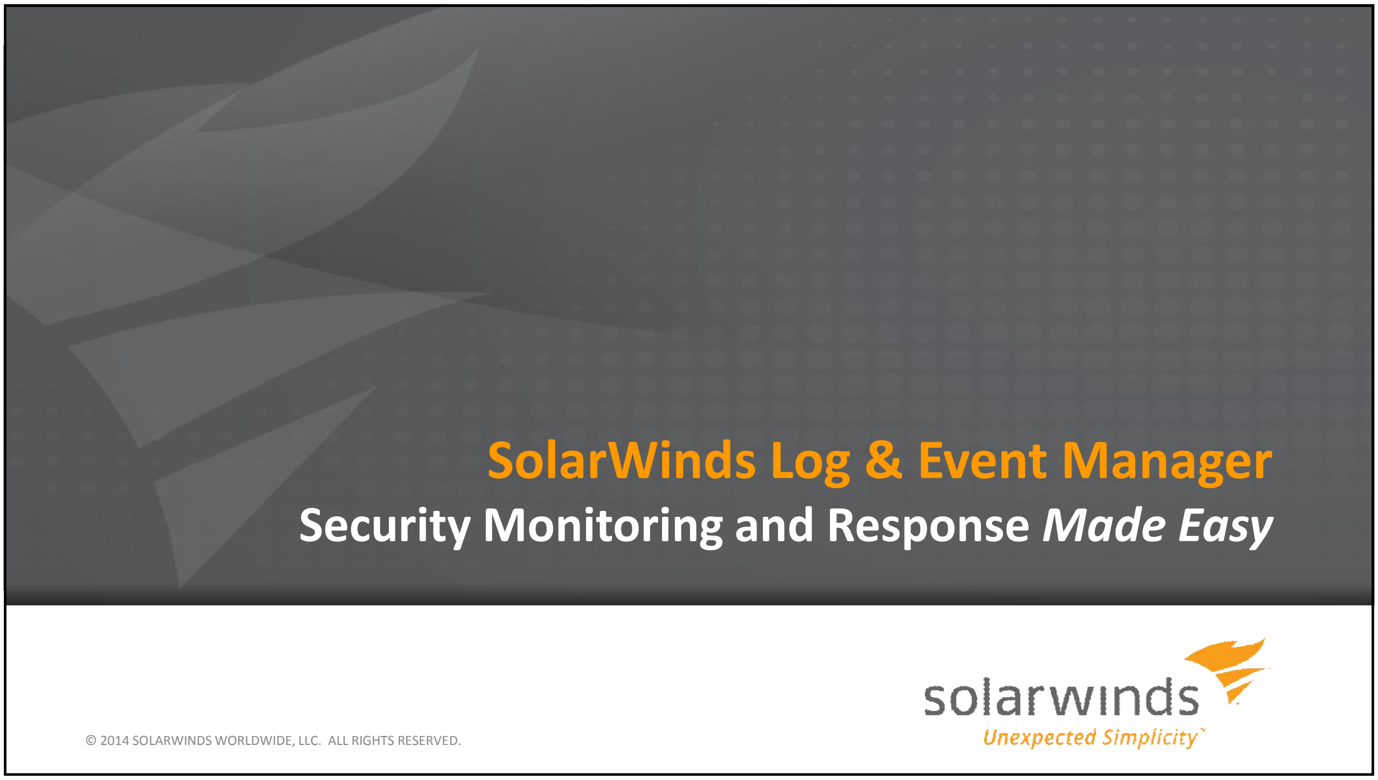
## Recognizing attacks

- Local accounts
  - Do you use local accounts?
    - Consider logon types – appropriate?
    - Are user names "fat fingered" versions of real user names?
  - Bad user name
    - Well known privileged account names?
    - Random people names?
    - Some other generated pattern?
  - Bad password
  - Other logon failure reasons
    - Consider client IP / Workstation name
      - Find the user(s) who had physical access to that system and investigate
    - Note logon type by looking for correlated 4625



## Bottom line

- Need DC logs
- Need access to workstation/member server logs
- Need ability to analyze events over time to come up with baseline
- Need to distinguish account types by account naming conventions
  - End users
  - Privileged users
  - Non-human accounts
- Give attention to client IP / workstation name
- Alert on
  - Domain logon failures other than bad password/username, account lockout
  - All local account logon failures where user name is real and not an end user
- Report/dashboard on domain account bad password/username
  - Alert when quantity for given user name / end point significantly exceed average



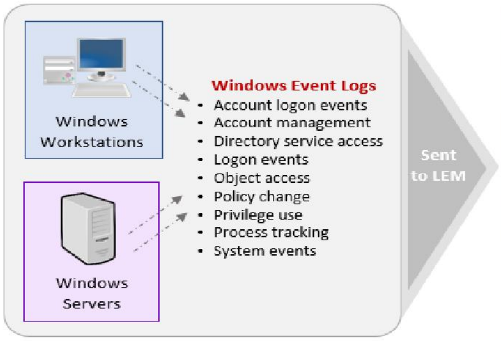
## SolarWinds Log & Event Manager

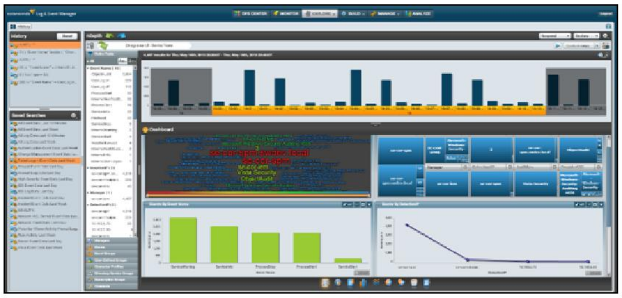
**Security Monitoring and Response *Made Easy***

solarwinds
Unexpected Simplicity

## Find the Needle in the Haystack – *Fast!*

**SolarWinds Log & Event Manager** goes far beyond log collection and analysis by providing **real-time, multi-dimensional event correlation combined with automated response capabilities** to **immediately identify and stop threats *before* the damage is done.**





SolarWinds Log & Event Manager Collects & Correlates Windows Server and Workstation Logs in Real Time

Over **700 built-in correlation rules** for **visibility right out of the box**

solarwinds

## Turning Unruly Log Data into Useable, Actionable Intelligence

**SolarWinds Log & Event Manager** gives you **the actionable intelligence you need, *when you need it***, to stay ahead of advanced threats and other vital network issues.

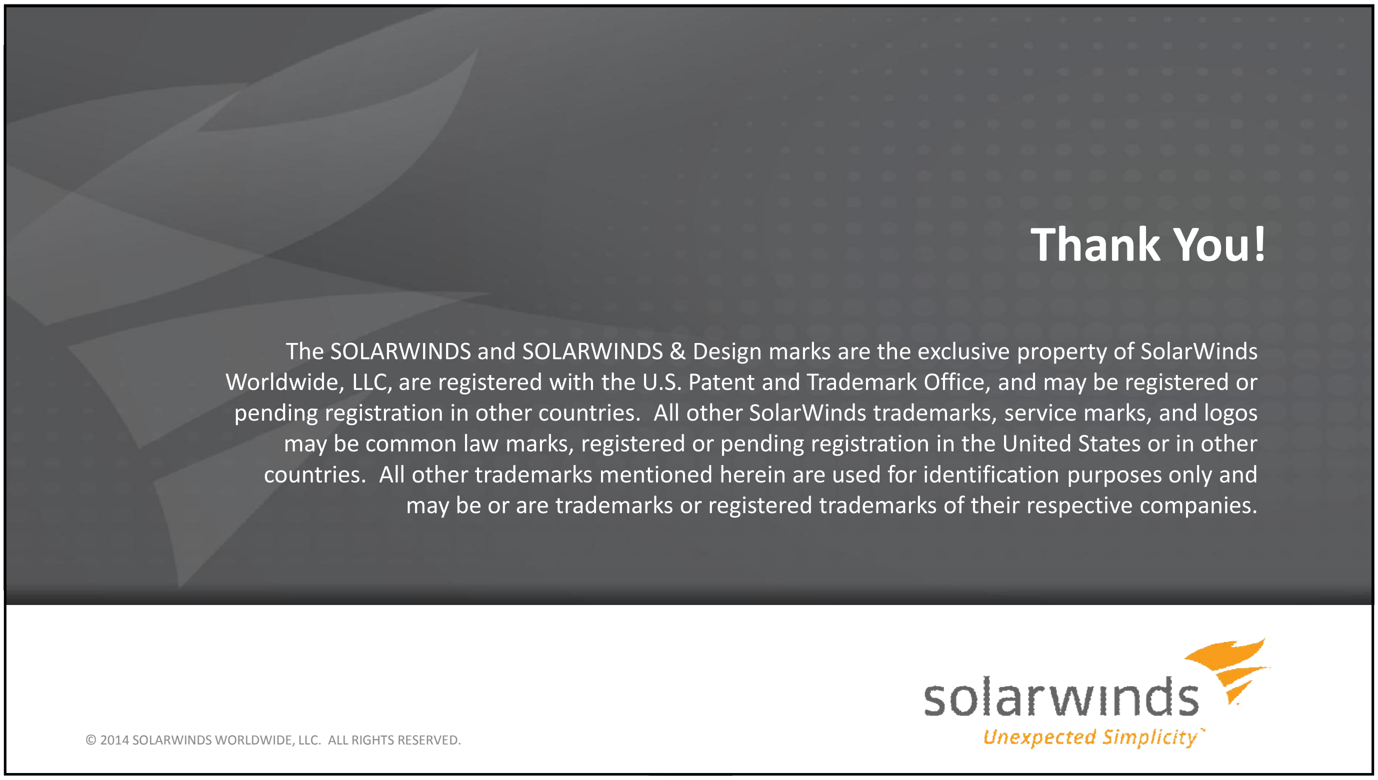
- ✓ Collect, aggregate, normalize, and classify log data from across your IT infrastructure
- ✓ Correlate events across devices and disparate systems to detect and stop multi-faceted attacks
- ✓ Get real-time, detailed visibility into security, compliance, and operational issues
- ✓ Leverage Built-in Active Responses for automated threat remediation and incident response
- ✓ Explore data visually through an intuitive search interface for fast and easy forensics
- ✓ Consolidate, compress, and securely store log data for compliance and auditing
- ✓ Generate and schedule reports using hundreds of customizable, out-of-the-box templates

**LEARN MORE**

**SolarWinds Log & Event Manager – *Product Info and Online Demo***

http://www.solarwinds.com/log-event-manager.aspx

solarwinds



# Thank You!

The SOLARWINDS and SOLARWINDS & Design marks are the exclusive property of SolarWinds Worldwide, LLC, are registered with the U.S. Patent and Trademark Office, and may be registered or pending registration in other countries. All other SolarWinds trademarks, service marks, and logos may be common law marks, registered or pending registration in the United States or in other countries. All other trademarks mentioned herein are used for identification purposes only and may be or are trademarks or registered trademarks of their respective companies.

solarwinds
Unexpected Simplicity