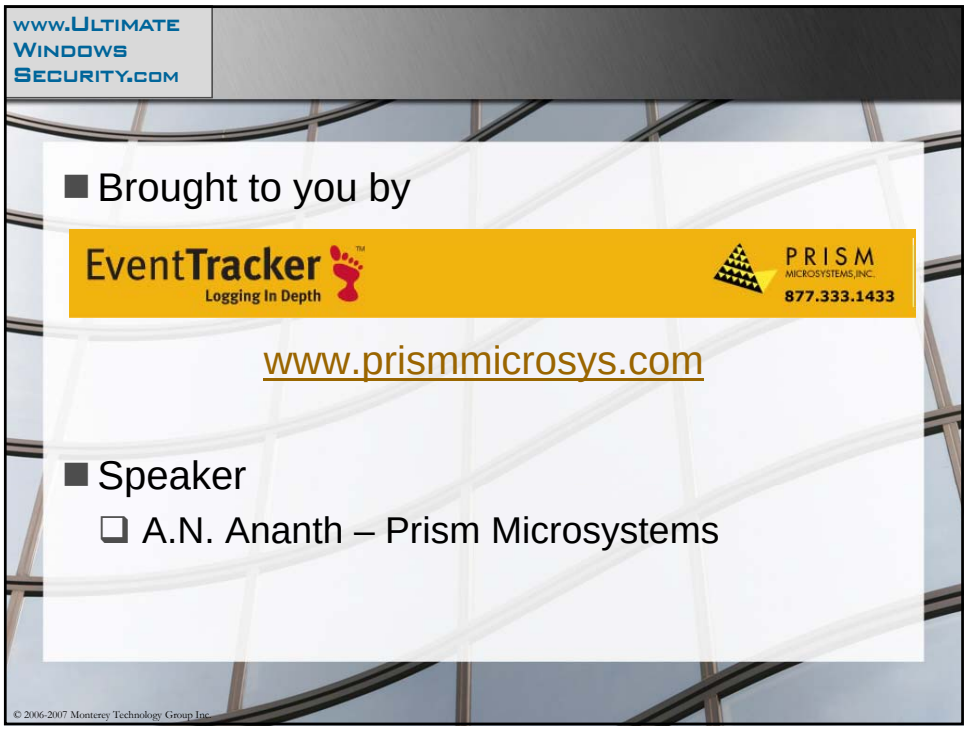


www.UltimateWindowsSecurity.com

Key Points

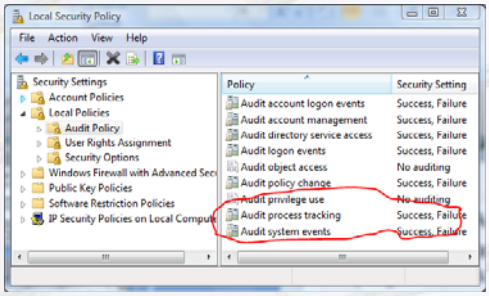
- Auditing Program Execution with the Security Log
  - Audit setup
  - Event IDs
  - Putting knowledge to work
    - What programs did this user execute?
    - How long did the program run?
    - Detect new programs run for the first time
    - What are all the unique programs executed on this server over a period of time?
    - How to recognize new malware

3

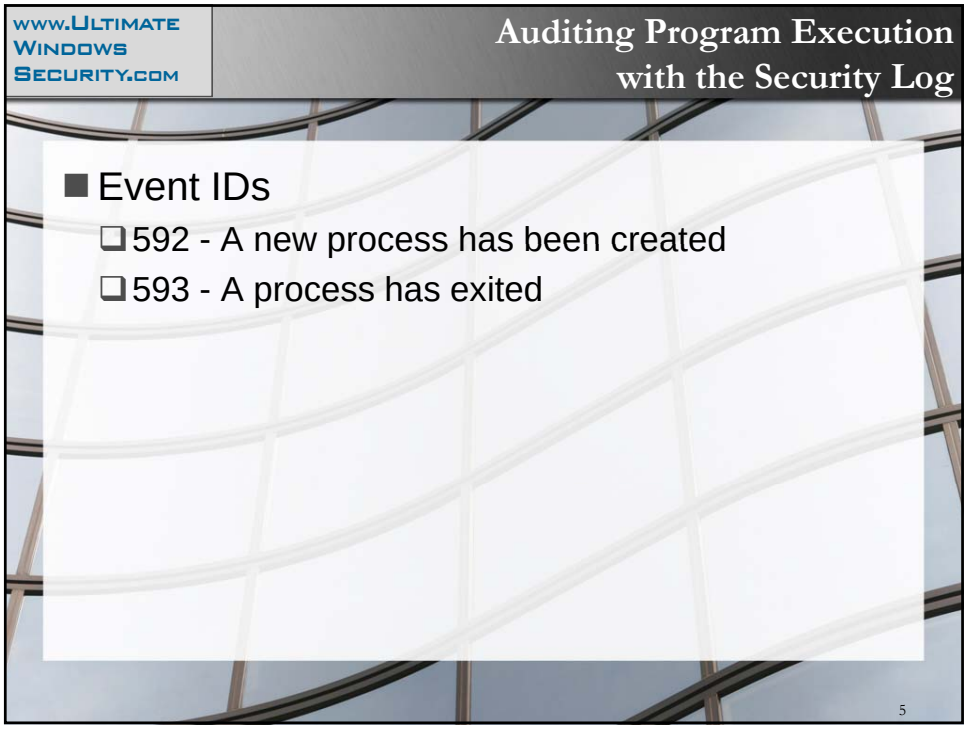
www.UltimateWindowsSecurity.com

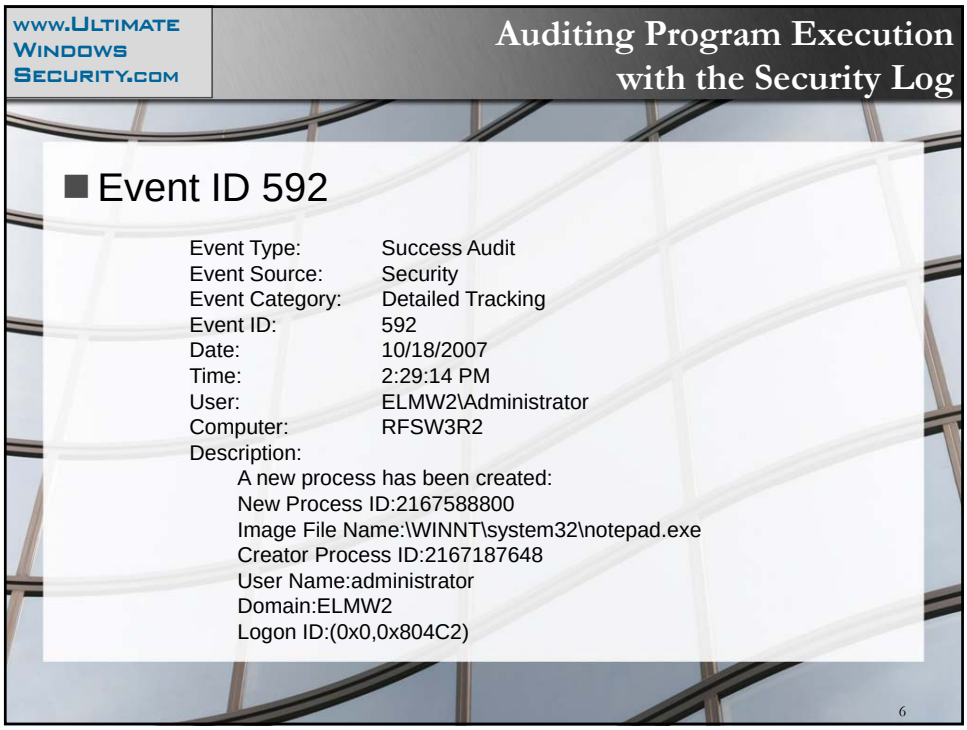
Auditing Program Execution with the Security Log

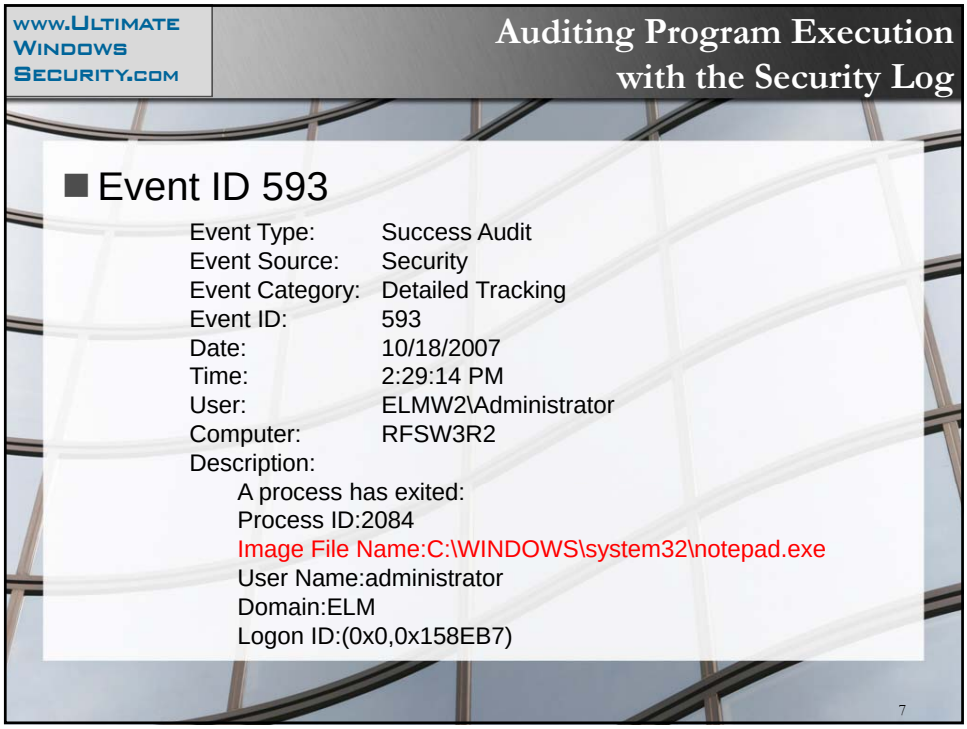
- Setup
  - Just enable “Audit process tracking”
  - On all computers where you want to track program execution

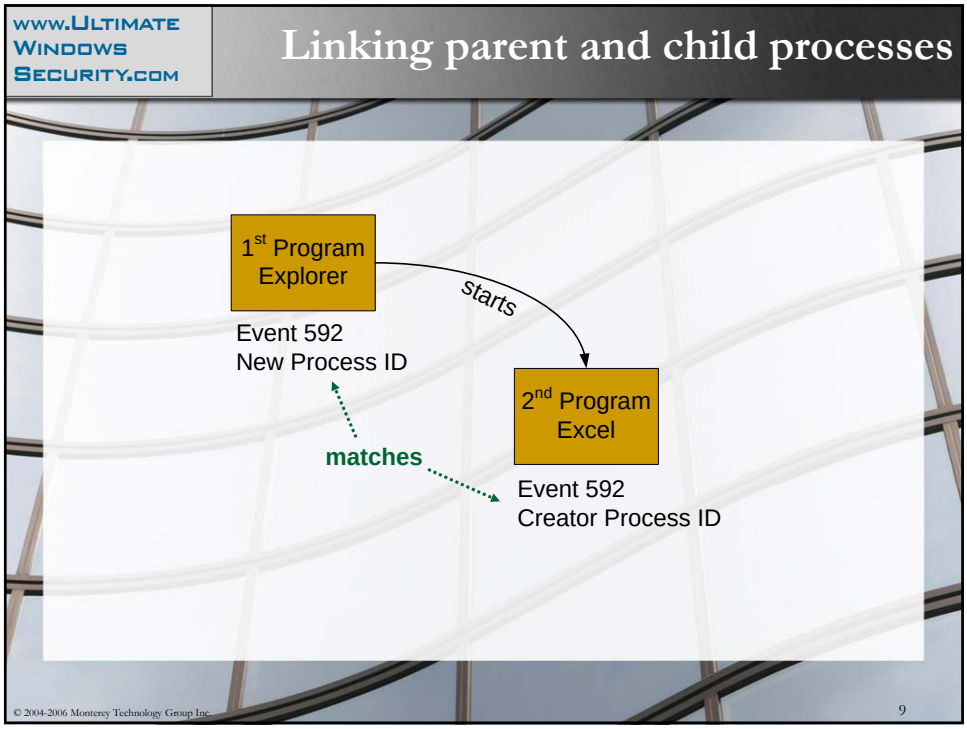


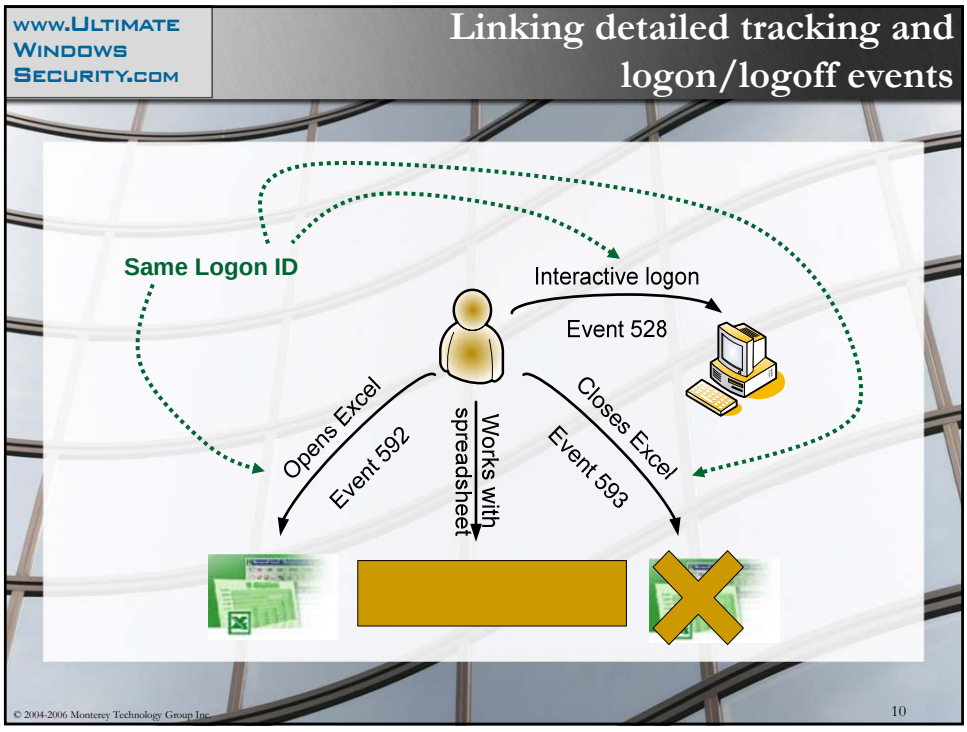
4

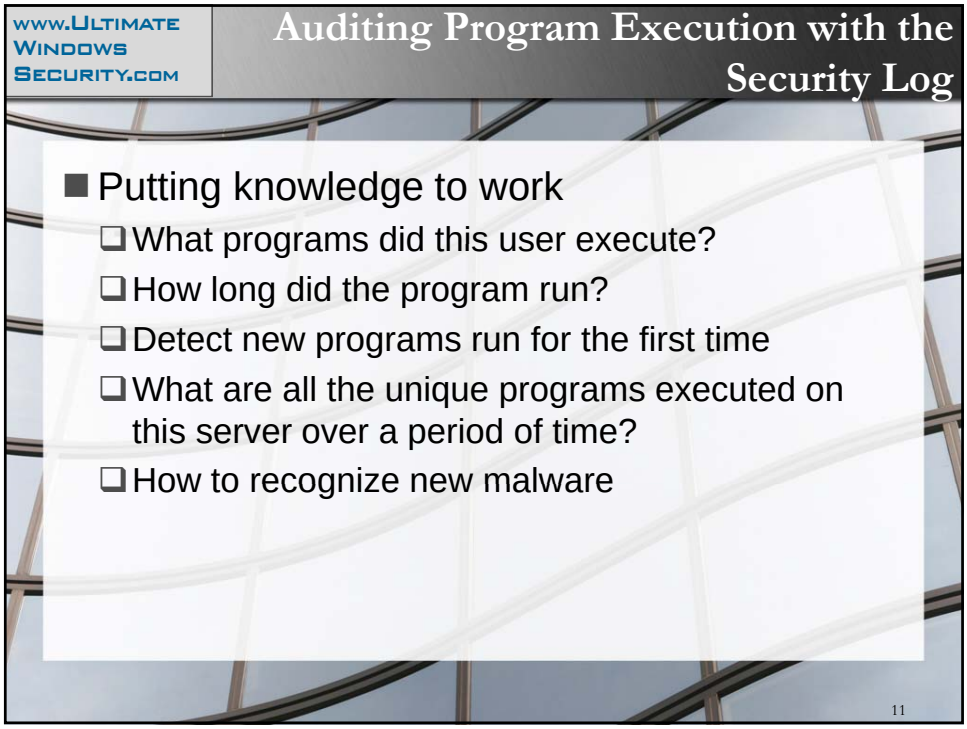


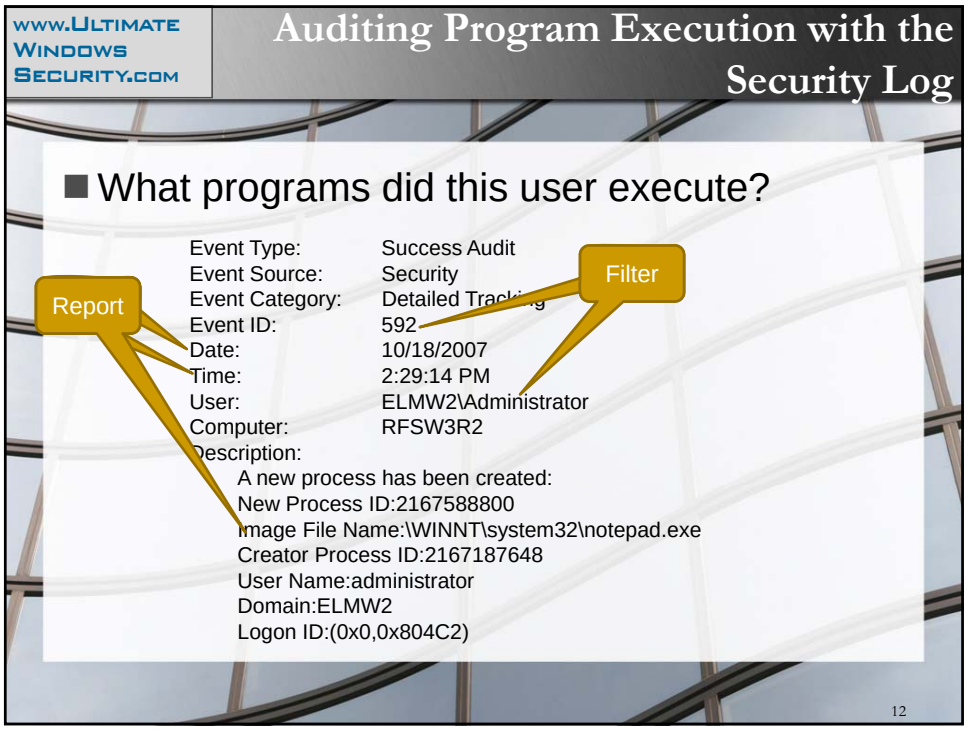





www.UltimateWindowsSecurity.com
Linking parent and child processes
1st Program Explorer
starts
Event 592
New Process ID
2nd Program Excel
matches
Event 592
Creator Process ID
© 2004-2006 Monterey Technology Group Inc.
9


www.UltimateWindowsSecurity.com
Linking detailed tracking and logon/logoff events
Same Logon ID
Interactive logon
Event 528
Opens Excel
Event 592
Works with spreadsheet
Closes Excel
Event 593
© 2004-2006 Monterey Technology Group Inc.
10

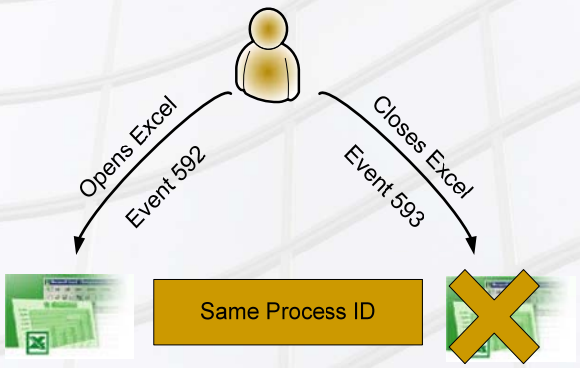




www.UltimateWindowsSecurity.com

Auditing Program Execution with the Security Log

- How long did the program run?



13

www.UltimateWindowsSecurity.com

Auditing Program Execution with the Security Log

- Putting knowledge to work
  - What are all the unique programs executed on this server over a period of time?
    - Collect 592s over period of time
    - Get a distinct list of image filenames from 592s

14