Application Security Intelligence: The Next Frontier in Security Analytics - Bridge the Gap between Applications and SIEM

Sponsored by

LOGbinder

© 2014 Monterey Technology Group Inc.

Thanks to

- Made possible by

LOGbinder
Application Security Intelligence for your SIEM

www.logbinder.com

© 2014 Monterey Technology Group Inc.

Preview of Key Points

- The critical need for application security intelligence
- Top 3 applications
  - SharePoint
  - SQL Server
  - Exchange
- What activity should you audit?
- How does each application's internal auditing work?
- How do you get those events into your SIEM?

© 2014 Monterey Technology Group Inc.

The critical need for application security intelligence

What are most organization's monitoring with their SIEM?

Network	Active Directory	Windows
SQL Server	Exchange	SharePoint
Lync	SAP	Line of Business Apps
	Cloud Apps	

What is the ultimate goal of most attackers?

Where does information reside?

At which level of the stack is information most easily understood?

Which people in an organization are targeted the most?

What level of the stack do end users have access to?

© 2014 Monterey Technology Group Inc.

ULTIMATE WINDOWS SECURITY .COM

LOGbinder

Without application security intelligence…

© 2014 Monterey Technology Group Inc.

ULTIMATE WINDOWS SECURITY .COM

LOGbinder

Real world scenarios

- Information grab
- Reading VIP mailbox
- Querying entire customer payment information table

© 2014 Monterey Technology Group Inc.

The information grab

- Edward, and engineering QC analyst, downloads 1000 product design documents from a SharePoint document library
- Operating system logs?
  - Blind
- IIS logs
  - 1000 files sounds like a lot of events until you look at IIS logs on a SharePoint Server
- Network
  - Using https?
    - Blind
  - HTTP?
    - Are you really going to capture every packet to/from every server with confidential/sensitive/regulated information in your organization?

© 2014 Monterey Technology Group Inc.

Reading VIP mailbox

- Network logs
  - Blind to https
- Operating system logs
  - Blind
  - See user logon
- IIS logs
  - Uhh, let's just say there's a reason why Microsoft added a mailbox audit log to Exchange

© 2014 Monterey Technology Group Inc.

Querying entire customer payment information table

- Operating system log
  - Blind
- Network
  - Encrypted?
    - Blind
  - Not encrypted
    - Capture every packet to/from database server
    - Reconstruct SQL protocol
    - Parse SQL
  - But what if query performed via local session?
    - Blind

© 2014 Monterey Technology Group Inc.

The solution

- Each of these applications has a native but highly internalized audit log
- Each application can easily catch the previous scenarios and much more

© 2014 Monterey Technology Group Inc.

Exchange

- 2 audit logs
  - Mailbox audit log
    - For the express purpose of auditing non-owner access to mailboxes
  - Admin audit log
    - Full fidelity audit trail of privileged users

© 2014 Monterey Technology Group Inc.

SharePoint

- Auditing
  - Define what operations to perform on selected site collections or content types
    - View
    - Update
    - Delete
    - …
  - Audit security changes
    - Permissions
    - Groups
    - …

© 2014 Monterey Technology Group Inc.

SQL Server

- New audit log in SQL 2008
- Blows away SQL Trace / C2 Auditing
  - All or nothing proposition
- Define exactly
  - Which objects
    - Databases, tables, stored procedures
  - Which users
    - Users, groups
  - Which actions
    - Databases: backup, copy
    - Tables: Insert, Select
    - Stored procedure: execute
    - Security changes
      - Logins
      - Roles
      - Permissions

© 2014 Monterey Technology Group Inc.

One big caveat

- Can't directly get these audit events into your SIEM

© 2014 Monterey Technology Group Inc.

The gap

- Your SIEM might already be getting some logs from SharePoint or Exchange
- But not the audit logs
- Exchange
  - Comparing Exchanges 3 Audit Logs for Security and SIEM Integration
  - http://www.logbinder.com/Form/LBEXWhitepaperComp
- SharePoint
  - Comparing SharePoints 4 Audit Logs for Security and SIEM Integration
  - http://www.logbinder.com/Form/LB4LogsWP

© 2014 Monterey Technology Group Inc.

Bridge the gap

© 2014 Monterey Technology Group Inc.

ULTIMATE WINDOWS SECURITY .COM

LOGbinder

LOGbinder philosophy

- Prime Directive: Preserve audit log integrity
- Focus
- Least privilege
- Low impact

© 2014 Monterey Technology Group Inc.

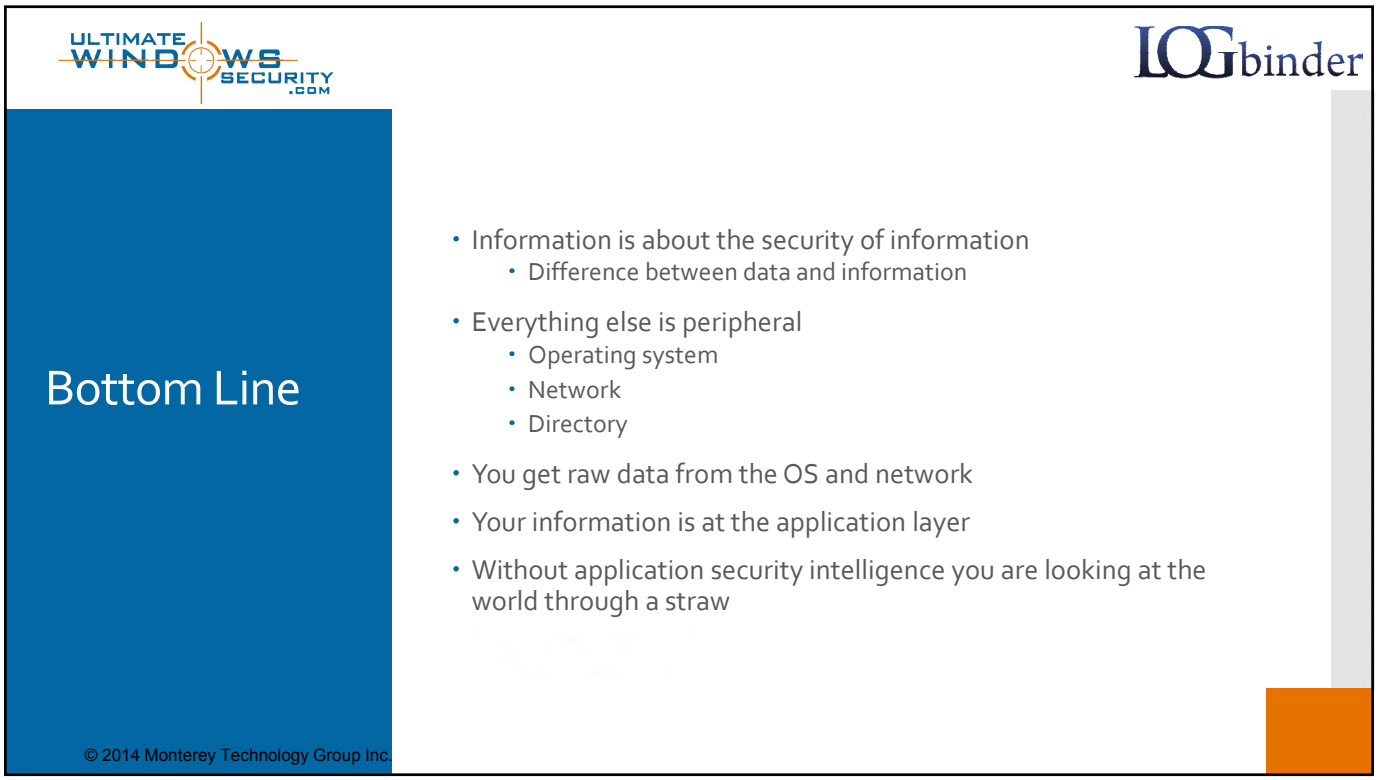
ULTIMATE WINDOWS SECURITY .COM

LOGbinder

LOGbinder

- Application Security Intelligence is knowing about:
  - Who is accessing confidential information
  - Who is modifying information that must be accurate
  - Entitlement changes and other security policy
  - Suspiciously large downloads or exports of information
  - Behavior suggestive of an exploring expedition

© 2014 Monterey Technology Group Inc.


ULTIMATE WINDOWS SECURITY .COM
LOGbinder
Bottom Line
• Information is about the security of information
  • Difference between data and information
• Everything else is peripheral
  • Operating system
  • Network
  • Directory
• You get raw data from the OS and network
• Your information is at the application layer
• Without application security intelligence you are looking at the world through a straw
© 2014 Monterey Technology Group Inc.