Case Study: University of Dayton and Novell® Identity & Security Solutions

Rick Wagner

Senior Product Manager, Security Management

rwagner@novell.com

Novell®

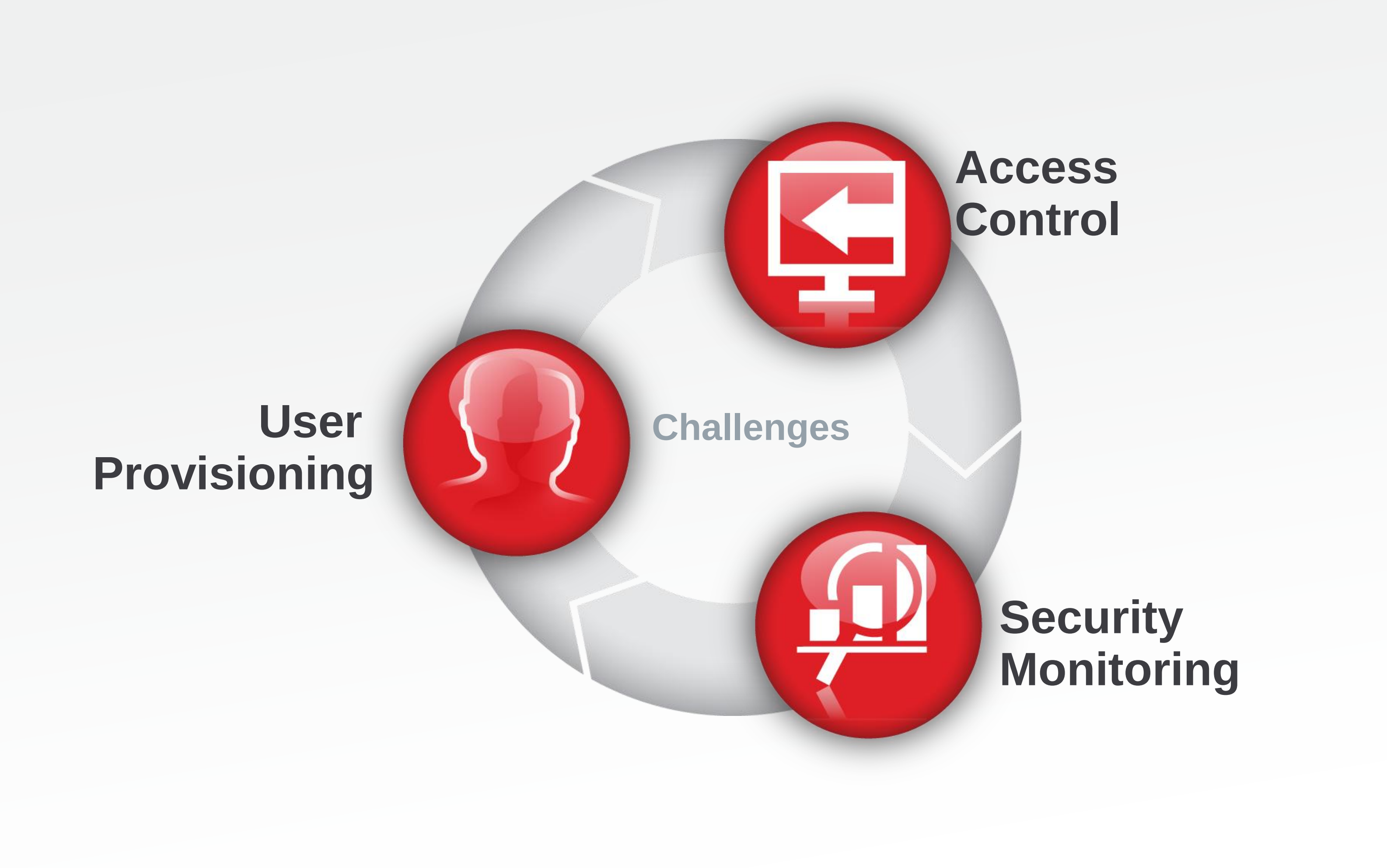
University of Dayton

- Recognized by US News and World Report as one of the 10 best Catholic Universities in the nation
- 12,0000 Students and 3,000 Faculty
- The Challenge:
    - "We had a huge pile of data and no way of getting to the few bits of data that were really important to us”
    - "We needed a way to not only analyze this data but also simplify ongoing report creation for PCI compliance. Previously we had to do a lot of manual work to produce reports.”

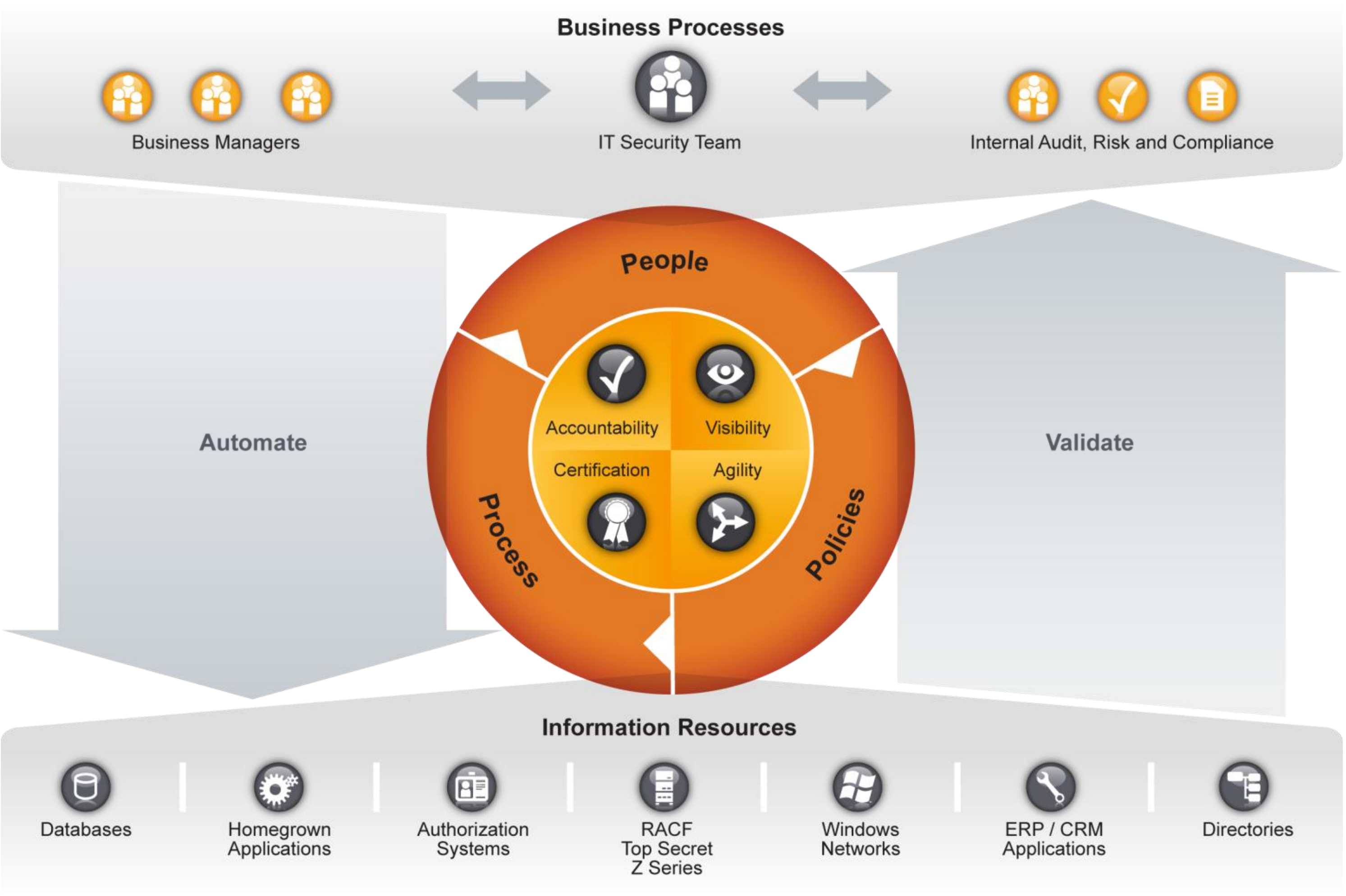
University of Dayton

- The Solution
  - Deployed Sentinel™ and Sentinel Log Manager Log Manager to detect and collect an average of three million security events a day simplifying the process of collecting, archiving and analyzing its log data.
  - “Novell Sentinel Log Manager allows us to take all the log information and look at it by any parameter. It brings meaning to the hundreds of security logs we receive.”
  - The University uses Sentinel™ to collect security-related events from its firewalls, intrusion detection systems, Novell eDirectory™, Novell Identity Manager and Novell Access Manager™.
  - "The real strength of Novell Sentinel, coupled with Novell Identity Manager, is the ability to clearly connect security events with individual identities, which is critical for achieving PCI compliance.”
  - "Novell Sentinel Log Manager does an amazing job at handling the huge volume of data we're throwing at it.”
  - "Within this year, the Novell solution will have easily paid for itself in reduced administrative time, not to mention our improved security posture."

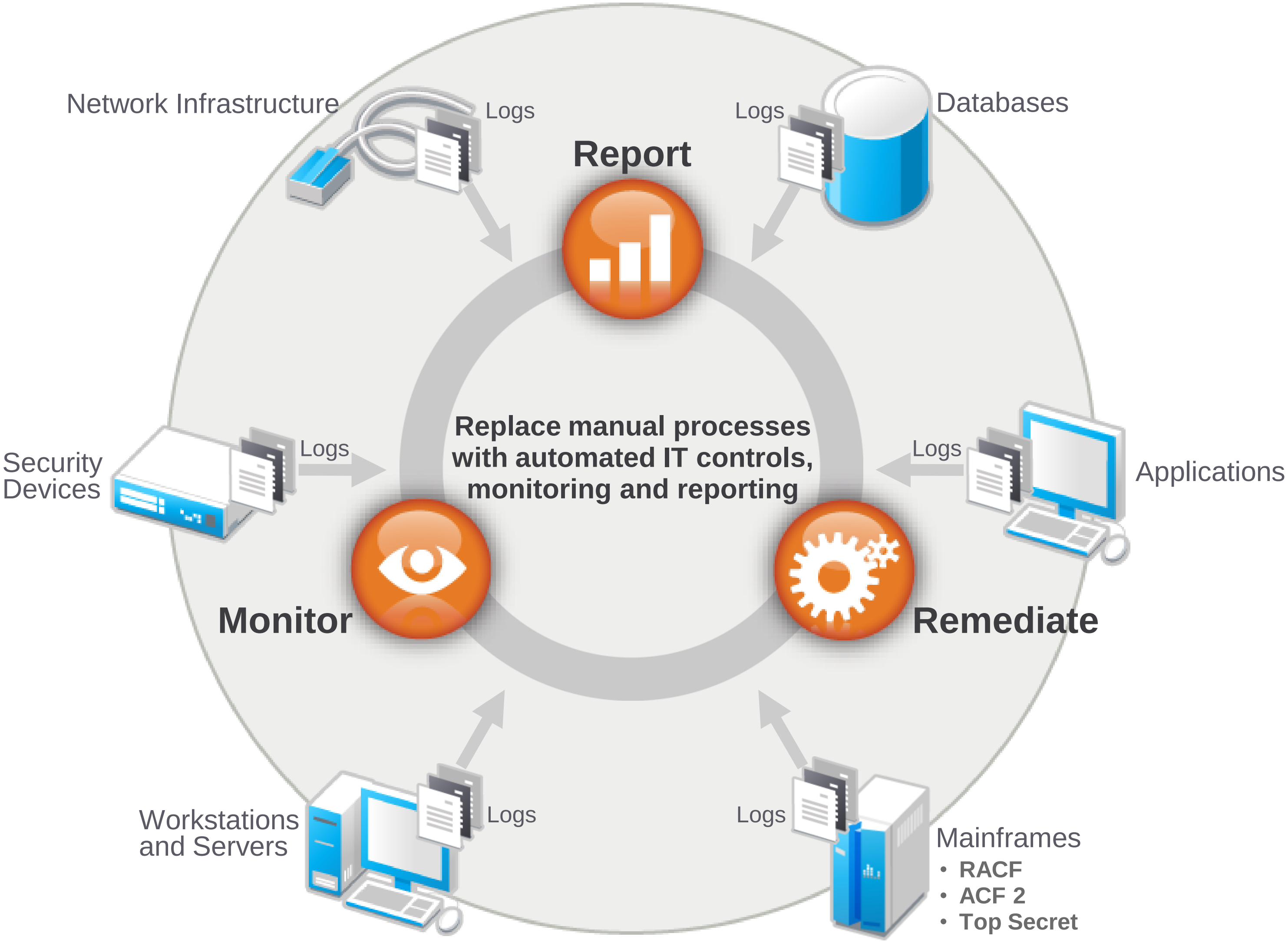
Integrated Approach to Security



Identity and Security Business View

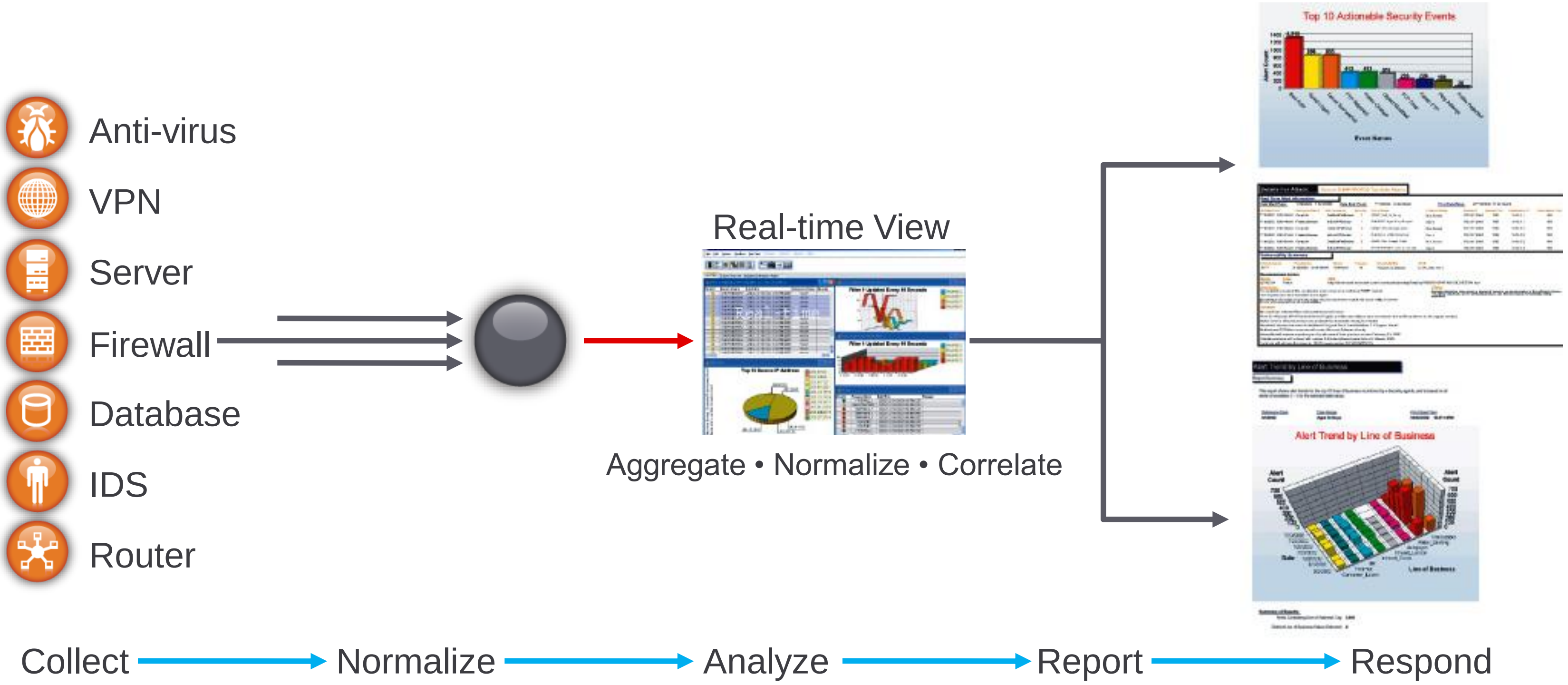


Novell® Sentinel™

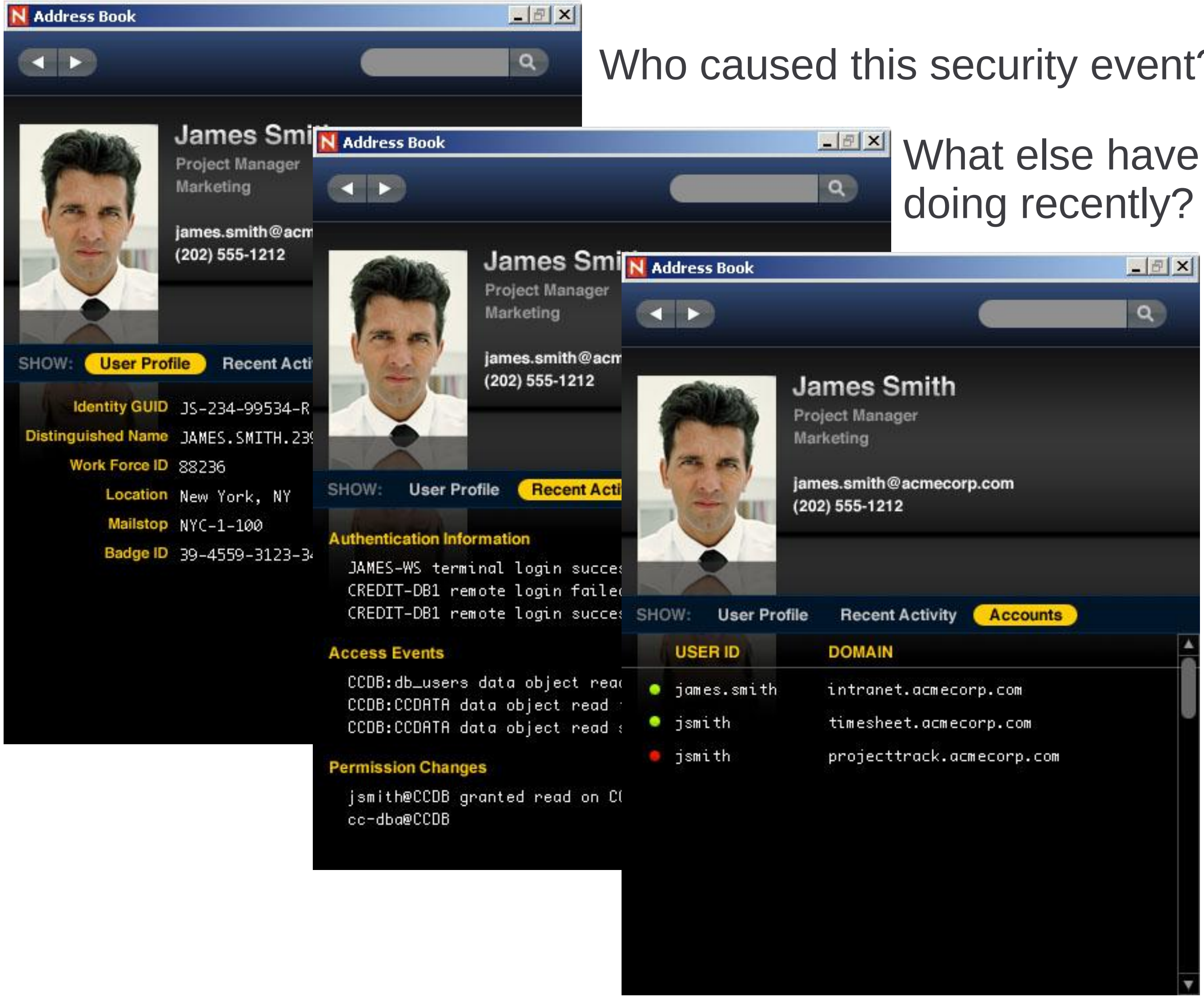


Sentinel™ Automates the Monitoring and Reporting of IT Controls

Collect and consolidate feeds from multi-vendor sensors
Normalize logs from across the enterprise seamlessly
Monitor and analyze for control violations in real time
Respond to violations … incident management tied to existing workflows
Report on the effectiveness of the control environment


Anti-virus
VPN
Server
Firewall
Database
IDS
Router
Real-time View
Aggregate • Normalize • Correlate
Top 10 Actionable Security Events
Alert Trend by Line of Business
Collect
Normalize
Analyze
Report
Respond

Real-time Identity Enriched Security Information



Address Book

James Smi

Project Manager
Marketing

james.smith@acm
(202) 555-1212

SHOW: User Profile Recent Acti

Identity GUID	JS-234-99534-R
Distinguished Name	JAMES.SMITH.23
Work Force ID	88236
Location	New York, NY
Mailstop	NYC-1-100
Badge ID	39-4559-3123-3

Who caused this security event?

Address Book

James Smi

Project Manager
Marketing

james.smith@acm
(202) 555-1212

SHOW: User Profile Recent Acti

Authentication Information

```
JAMES-WS terminal login succes
CREDIT-DB1 remote login failed
CREDIT-DB1 remote login succes
```

Access Events

```
CCDB:db_users data object read
CCDB:CCDATA data object read
CCDB:CCDATA data object read
```

Permission Changes

```
jsmith@CCDB granted read on C
cc-dba@CCDB
```

What else have they been doing recently?

Address Book

James Smith

Project Manager
Marketing

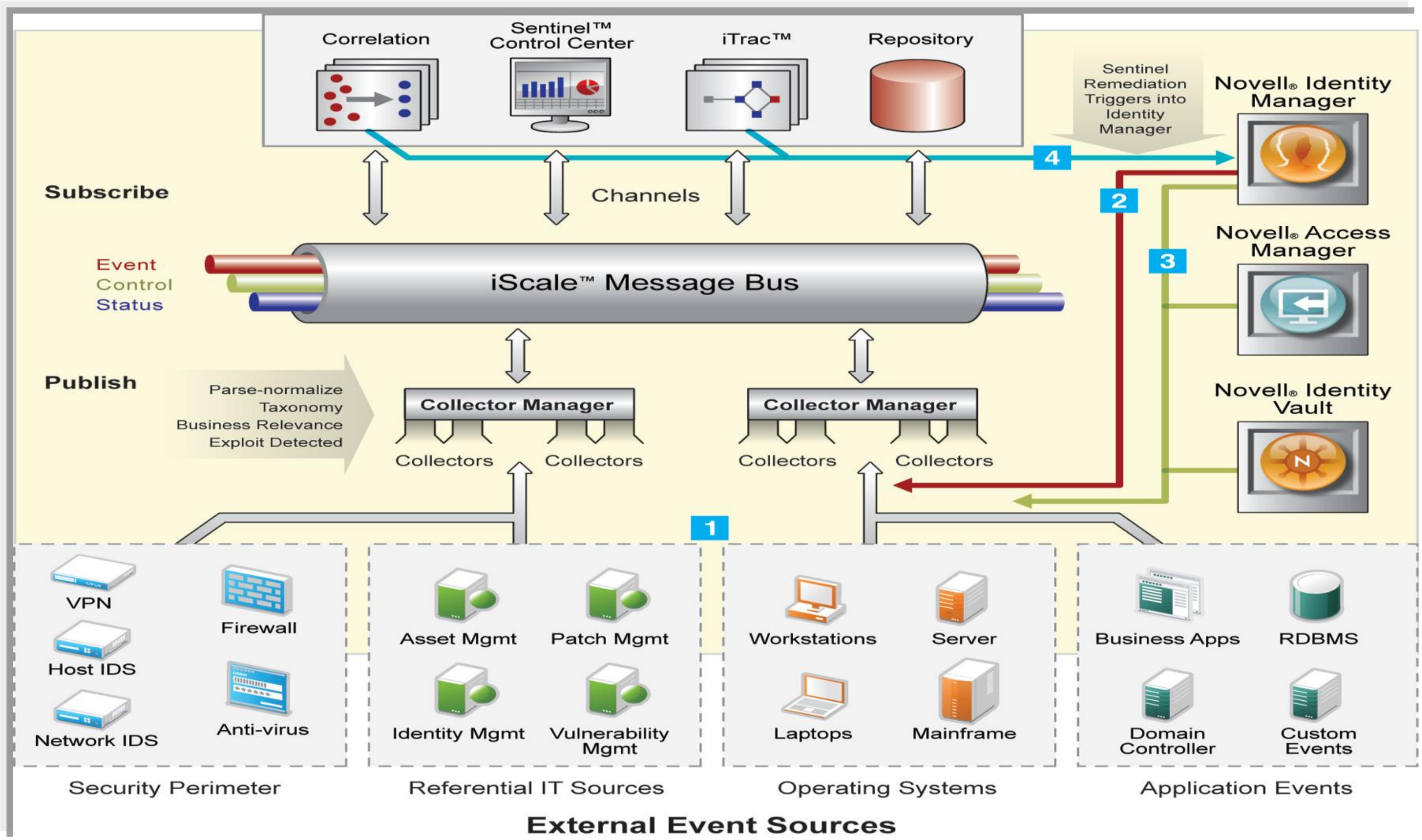
james.smith@acmecorp.com
(202) 555-1212

SHOW: User Profile Recent Activity Accounts

	USER ID	DOMAIN
●	james.smith	intranet.acmecorp.com
●	jsmith	timesheet.acmecorp.com
●	jsmith	projecttrack.acmecorp.com

What other accounts do they have throughout the enterprise?

Identity & Security Real Time Analysis



For Additional Information

- Novell Open Audio
  - http://www.novell.com/media/content/university-of-dayton-uses-sentinel-log-manager.html
- Success Story
  - http://www.novell.com/success/univ_dayton.html
- Sentinel Log Manager
  - http://www.novell.com/products/sentinel-log-manager/

Novell®

Unpublished Work of Novell, Inc. All Rights Reserved.

General Disclaimer

This document is not to be construed as a promise by any participating company to develop, deliver, or market a product. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. Novell, Inc. makes no representations or warranties with respect to the contents

of this document, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. The development, release, and timing of features or functionality described for Novell products remains at the sole discretion of Novell. Further, Novell, Inc. reserves the right to revise this document and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes. All Novell marks referenced in this presentation are trademarks or registered trademarks of Novell, Inc. in the United States and other countries. All third-party trademarks are the property of their respective owners.