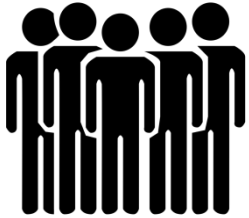


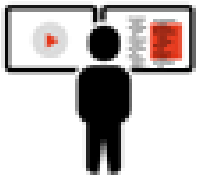
Agenda



Insider Threat
Problem



People-centric
Approach



ObserveIT
Solution

Insider Threat Management

Presented by:

Elad Tzur

observe **it**

Who is ObserveIT?

ObserveIT is the Global leader in
Insider Threat Management

Over 1,200 Customers Worldwide



- Boston, MA
- Founded 2006
- Bain Capital

CHALLENGE WITH ADDRESSING **INSIDER THREATS**

260,000+
members

LinkedIn  Group Partner

Information
Security



3 out of 4 InfoSec professionals say

**“It’s Hard to Distinguish
Abuse from Legitimate Use”**

People are the core of your business...



Business users

IT users

Contractors

...they are also responsible for 90% of security incidents*

Bad actors



MALICIOUS

- Good employee turning bad
- Joined with no malicious intent
- Authorized users doing unauthorized things

Careless users



NEGLIGENT

- Imposing risk carelessly
- Unaware of security policy
- Create lots of noise and alert fatigue

There is no patch for people

To reduce the likelihood of incidents, you must:

Detect early indicators of unauthorized behavior

- Abusing admin privileges
- Bypassing security controls
- Unnecessary access

Bad actors



Inform negligent users of security policy

- Using unauthorized cloud apps
- Responding to phishing attempts
- Accidental data leakage



Unwitting users

Bad actor



Insider attack chain

Tipping Point – Going from good to bad



- Uploading Files to an external cloud
- message to competitor
- Playing video games with lack of regard



Searching for Data

- Password harvesting
- Database Queries
- unauthorized access to co-workers computers



Capture and Hide the data

- Encrypt and rename file extensions
- password protected zip file



Data Exfiltration

Send zip file over Wetransfer – off hours transfers

Unwitting user



Human Error



Bad actor



Insider attack chain

Detect negligent behavior



Inform user of security policy

Unwitting user



Human Error

Enforce behavior change



Stop wasting resources

Before...
Event-centric

```
2012-10-11 03:54:28,578 INFO - Starting Backup Manager 5.0.0 build 18266
2012-10-11 03:54:29,422 WARN - Generating Self-Signed SSL Certificate (al
2012-10-11 03:54:29,781 WARN - Saved SSL Certificate (alias = cdp) to Key
2012-10-11 03:54:30,047 INFO - Operating System: windows Server 2008 R2
2012-10-11 03:54:30,047 INFO - Architecture: amd64
2012-10-11 03:54:30,047 INFO - OS Version: 6.1
2012-10-11 03:54:30,047 INFO - Processors Detected: 1
2012-10-11 03:54:30,063 INFO - Max Configured Heap Memory: 483.4 MB
2012-10-11 03:54:30,063 INFO - Total Physical Memory: 2.0 GB
2012-10-11 03:54:30,063 INFO - Free Physical Memory: 893.1 MB
2012-10-11 03:54:30,063 INFO - Database Service starting
2012-10-11 03:54:33,203 INFO - creating embedded database 10.8.2.2 - (118
2012-10-11 03:54:34,141 INFO - Database Service started
2012-10-11 03:54:34,141 INFO - Object-Relational Mapping Service starting
2012-10-11 03:54:56,126 ERROR - Unsuccessful: create index stateIndex on R
2012-10-11 03:54:56,126 ERROR - Index 'STATEINDEX' already exists in Schem
2012-10-11 03:55:01,157 INFO - Object-Relational Mapping Service started
2012-10-11 03:55:01,157 INFO - Message Event Service wrapper starting
2012-10-11 03:55:04,626 INFO - Message Event Service wrapper started
2012-10-11 03:55:04,626 INFO - Event Service wrapper starting
2012-10-11 03:55:04,861 INFO - Event Service wrapper started
```

Only notice 25% of Insider Threats*

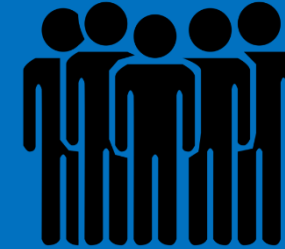
- Infinite amount of events to interpret
- Based on log files (must infer conclusions)
- Individual discrete incidents
- Classified by severity

Thousands of hours

*CERT Insider Threat Center

Much more efficient

...After
People-centric



100% visibility of Insider Threats

- Limited to the number of employees
- Based on people's actions (self-evident)
- All incidents roll up to users
- Prioritized by risk scoring

Less than one FTE

People-centric approach

People: 100,000

Deter

Deterrence will eliminate
90% of risky users

People: 10,000

Detect

On average, 10% of users
will be risky

People: 1000

Act

Less than 1% will be high-risk
and need investigation

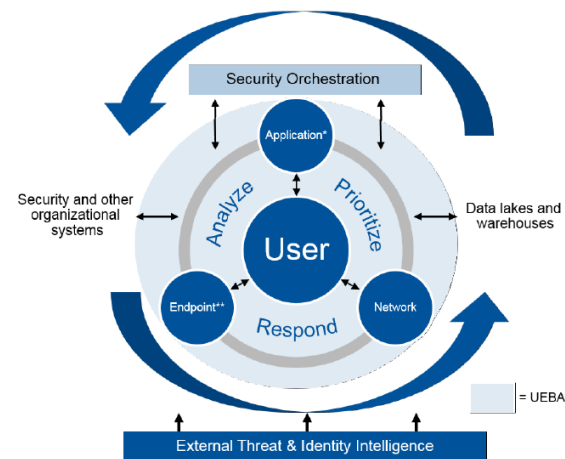
People: 50

GARTNER MARKET REVIEW: USER & ENTITY BEHAVIOR ANALYTICS

“most enterprises spend a majority of their security budget on prevention measures, such as firewalls, strong user authentication, intrusion prevention, antivirus systems and the like.

Successful hackers have figured out how to beat these prevention systems. In addition, the attackers are often not detected once they intrude on a network, since many monitoring systems generate so many false alarms that intrusion alerts often remain unnoticed.

Most recent breaches involved hackers taking over existing user accounts, activities that UEBA systems are designed to detect.” (Gartner, 2015)



* Includes cloud, mobile and other on-premises applications

** Includes managed and unmanaged endpoints

REGULATIONS ARE COMING

- General Data Protection Regulation (GDPR) – Aims to become effective in 2016
- European Central Bank (ECB) & European Bank Authority (EBA) – New security regulations on Insider threat
- European Union Agency for Network and Information Security (ENISA) – New Guidelines for Security & Privacy
- European Commission (EC) – Regulation for Internet Payments (Logging all inside activities)

USER RISK DASHBOARD



OVERALL RISK Time period: 8/19/15 12:00 AM - 9/18/15 12:29 PM

USER RISK SUMMARY

| Risk Level | Count |
|------------|-------|
| Critical | 7 |
| High | 16 |
| Medium | 36 |
| Low | 16 |

75 RISKY USERS

+3 NEW USERS IN RISK

TOP RISK APPLICATIONS

- 3 | /usr/bin/sudo
- 14 | Windows Explorer
- 7 | eu3.salesforce.com
- 1 | cs20.salesforce.com
- 2 | outlook.office365.com

TOP RISK ALERTS

- 10 | Free Cloud Storage Access
- 2 | Audit log tampering detecte...
- 1 | Suspicious Hacking Tools
- 1 | Export Top Clients by Financ...
- 10 | Cloud File Sharing

RISKY USERS (3)

Risk level: Critical High Medium Low

★ Page 1 of 1

Mary Smith

Virtualization / Linux Systems Administrator

100 +100

RISKY APPLICATIONS

- 82% /usr/bin/sudo
- 18% /bin/ping

ALERTS

- 4 | Audit log tampering detected - CANNED (Unix), 2 | Backdoor detected - Create a local user with a duplicated user ID - CANNED (Unix), 2 | Backdoor detected - Create a local user with a duplicated user ID - CANNED (Unix), 1 | Malicious privilege elevation - Root shell access by a non-standard application - CANNED (Unix)

Investigate

Robert Miller

Wealth Management Advisor

100 +100

RISKY APPLICATIONS

- 55% cs20.salesforce.com
- 27% ObserveIT Marking Tool
- 9% drive.google.com

ALERTS

- 2 | Export Top Clients by Financial Value Report
- 1 | Export Top Clients by Financial Value Report
- 3 | Cloud storage access - CANNED (Windows)

Investigate

James Brown

Senior Network & Systems Administrator

90 +90

RISKY APPLICATIONS

- 100% outlook.office365.com

ALERTS

- 1 | Unauthorized Office 365 mailbox snooping - Accessing another user mailbox - CANNED (windows)

Investigate

KNOW WHICH USERS ARE PUTTING YOUR BUSINESS AT RISK AND WHY

ObserveIT Solution



DETER

- Inform and enforce security policy
- Eliminate alert fatigue and noise
- Notify users that they are being recorded



DETECT

- No baselining required (to define “normal”)
- Canned alerts and packaged analytics for known risks
- Immediate detection of insider threats



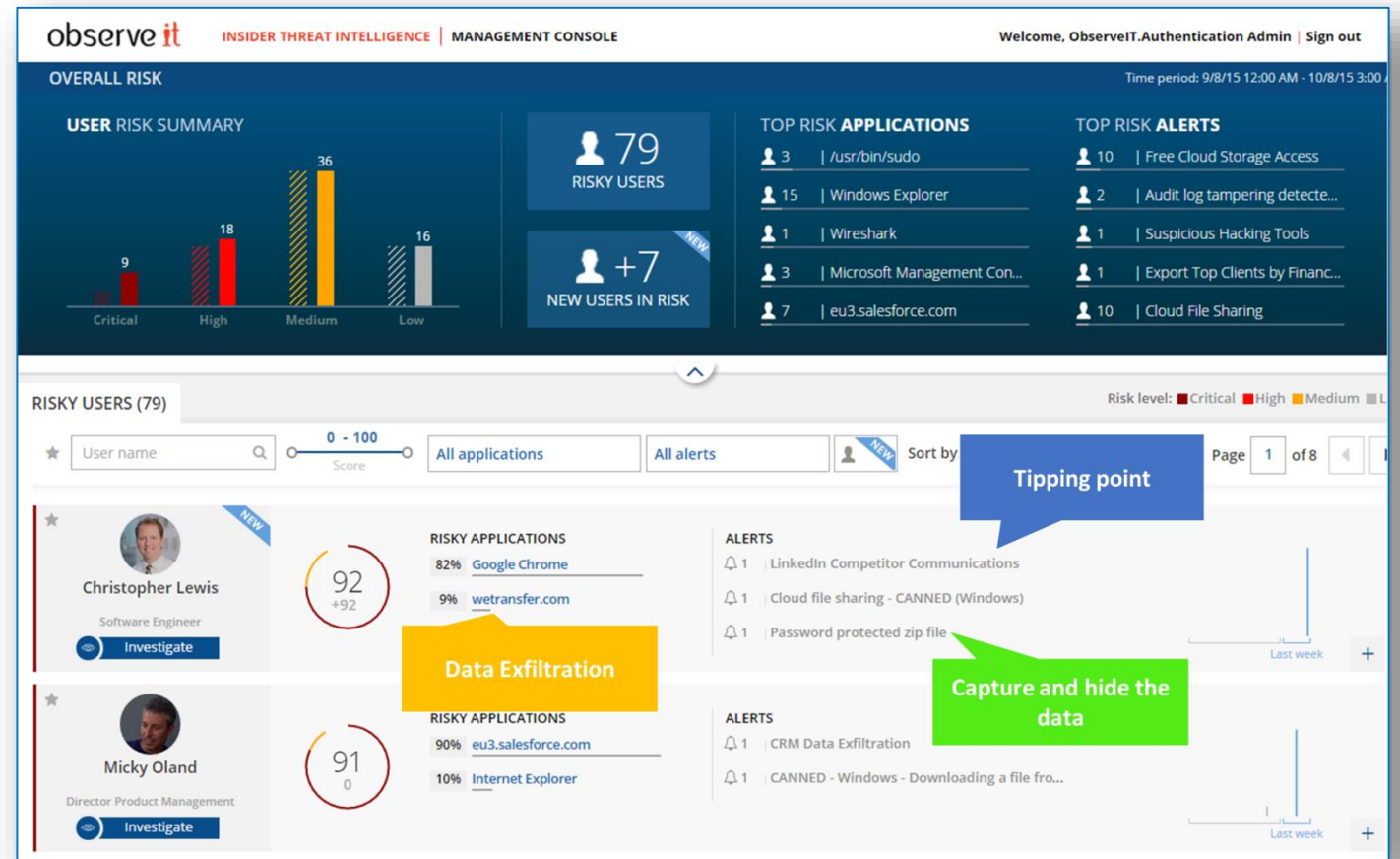
INVESTIGATE

- Simple, easy to view playback and metadata
- See who is doing what with visual forensics
- Assess malicious intent with irrefutable evidence



PREVENT

- Immediate “Circuit Breaker” to unauthorized sessions
- Block and control risky activity
- Instant messaging to live sessions





- Activities
 - Applications
 - Inventory
 - Software
 - Search
 - Messages
- Latest Sessions
- | | |
|----------------|--------|
| SNOOPY-NB | Snoopy |
| PRODSQL | brad |
| CTRX04-PA | james |
| KATIE-PC | brad |
| rhel-prod-3 | brad |
| JAMES-PC | ayelet |
| ubun-apache... | dima |
| solrs-dev-4 | brad |
- Quick Help
- Installation Guide
 - User Guide
 - Configuration Guide

Activities

Activity View

Server: [] ... Go [Server statistics](#) [Print this information](#)

Period: Last 5 Start Date: Mar 13 2014 End Date: Mar 21 2014

Filter by login/user: -All-

1 - 2 of 2 1

| Session | Duration | Login | User | Server | Client | Slides | Video |
|---------|-------------------|--------|------|-----------|---------|--------|-------|
| | 7:39 AM - 7:47 AM | Snoopy | n/a | SNOOPY-NB | (local) | 24 | |
| | 7:32 AM - 7:42 AM | Snoopy | n/a | SNOOPY-NB | (local) | 28 | |

[Add Comment](#) [Print this information](#) [Print detailed information](#)

Comment: abc User: Guest Comment Time: 2/21/2014 3:40 AM

ObserveITAgent

Untitled - Notepad (3)

LB-800E - Microsoft Word

ObserveIT - Login Page - ObserveIT - Login Page

http://demo.observeit.com/ObserveIT/FormLoginAuth.aspx?ReturnUrl=%2fo

Gistda

Save As (2)

Program Manager (3)

ObserveIT

ObserveIT - Demo server - Notepad

ObserveIT - Server Diary - Activities - ObserveIT - Login Page (3)

Resource

http://demo.observeit.com/ObserveIT/SlideViewer.aspx?SessionID=8fe1ae48-4921-44c...

Session alert summary

Session activity alerts

Investigate
Who did What

| Time | Status | | Login | User | Server | Video |
|---|--------|-----------------------------|-------------|------|--------------------------------------|--|
| 8/02/2016 | | | | | | |
| 1:09 PM | New | Active Directory Management | ilan | n/a | OITSRV | |
| Blocking Message User feedback: fff | | | | | | |
| Who? | | oit-lab.local\ilan | | | | View rule details |
| Did What? | | Opened window | | | Active Directory Users and Computers | |
| On Which Computer? | | OITSRV | | | | |
| From Which Client? | | OIT-ILAN-LAP (10.1.100.12) | | | | |
| When? | | Monday, 8/02/2016 1:09 PM | | | | View session of 10122444 |
| 9:55 AM | New | Remote Desktop Connection | Administ... | ilan | OITSRV | |
| 9:55 AM | New | Remote Desktop Connection | Administ... | ilan | OITSRV | |

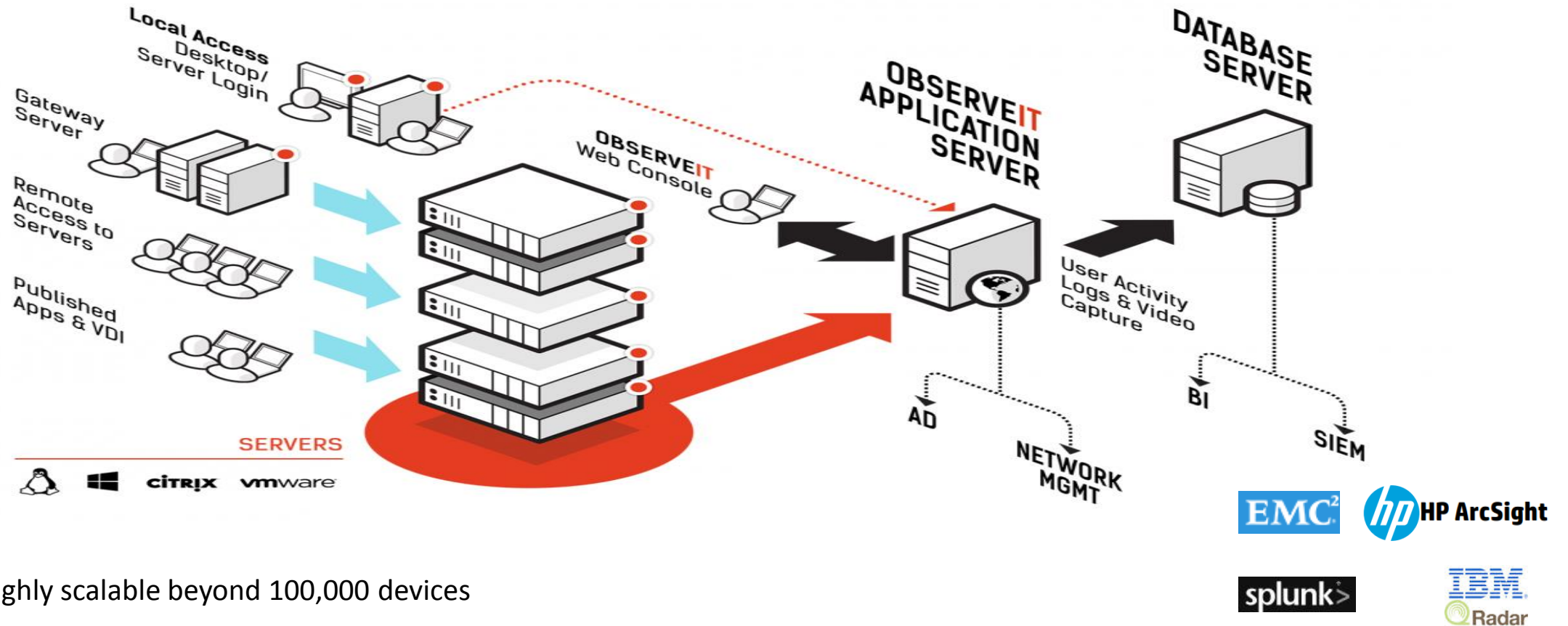
FILED-LEVEL APPLICATION MONITORING

Turn on Mark Mode to choose an element that should be monitored

| Element Name | Application/Website | Interaction | IE | Chrome | Firefox | Win |
|--|---------------------|-------------|----|--------|---------|-----|
| <input type="checkbox"/> Contact Name | eu3.salesforce.com | Displayed | ✓ | | | |
| <input type="checkbox"/> Contact Phone | eu3.salesforce.com | Displayed | ✓ | | | |
| <input type="checkbox"/> Contact Email | eu3.salesforce.com | Displayed | ✓ | | | |

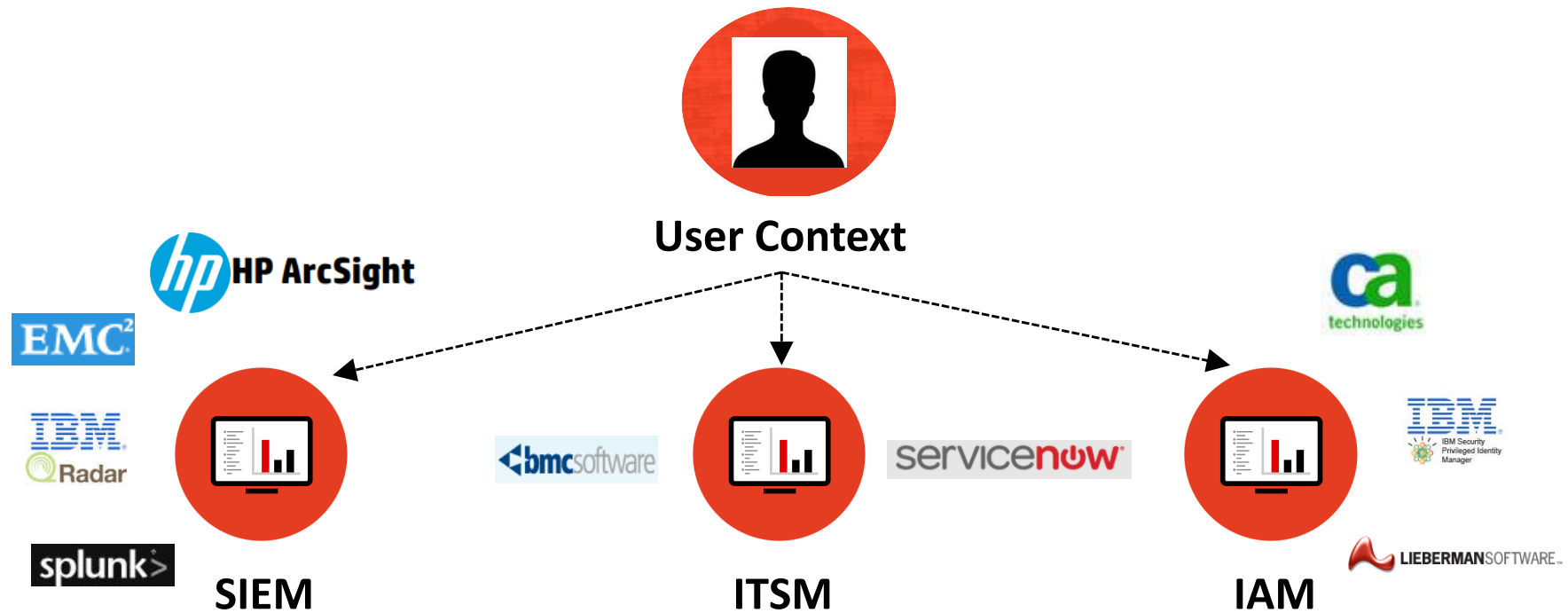
MARKING TOOL:
DISTINGUISH ABUSIVE BEHAVIOR
FROM NORMAL USER ACTIVITY

ObserveIT Deployment



- Highly scalable beyond 100,000 devices
- Only collects 100 MB per user per week
- Only 0.1% impact on network
- Less than 1% CPU overhead, only at the point of capture

ADD **USER CONTEXT** TO YOUR ECOSYSTEM



observe **it**

THANK YOU