splunk> .conf2017

Splunk UBA:

Setting Active Directory's Security Straight

Stanislav Miskovic, PhD | Splunk UBA

September 27th, 2017 | Washington, DC

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

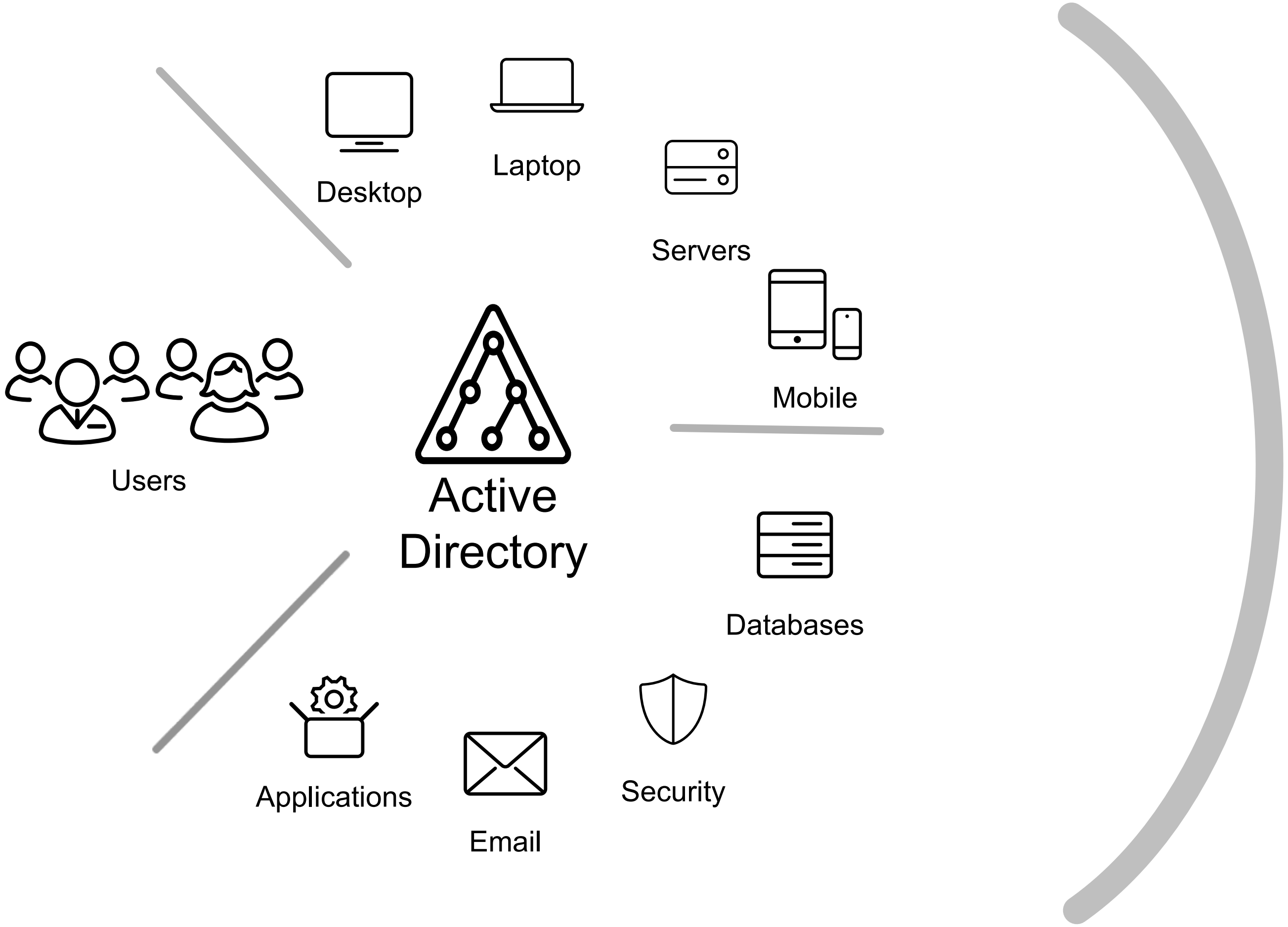
The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

Stanislav Miskovic

Principal Data Scientist, Splunk UBA
smiskovic@splunk.com

Works on data science applications in security, privacy and traffic analysis.
Ph.D. from Rice University, Houston, TX, M.Sc. degree from the University of Belgrade, Serbia.

Assets Under Active Directory



Desktop

Laptop

Servers

Mobile

Users

Active Directory

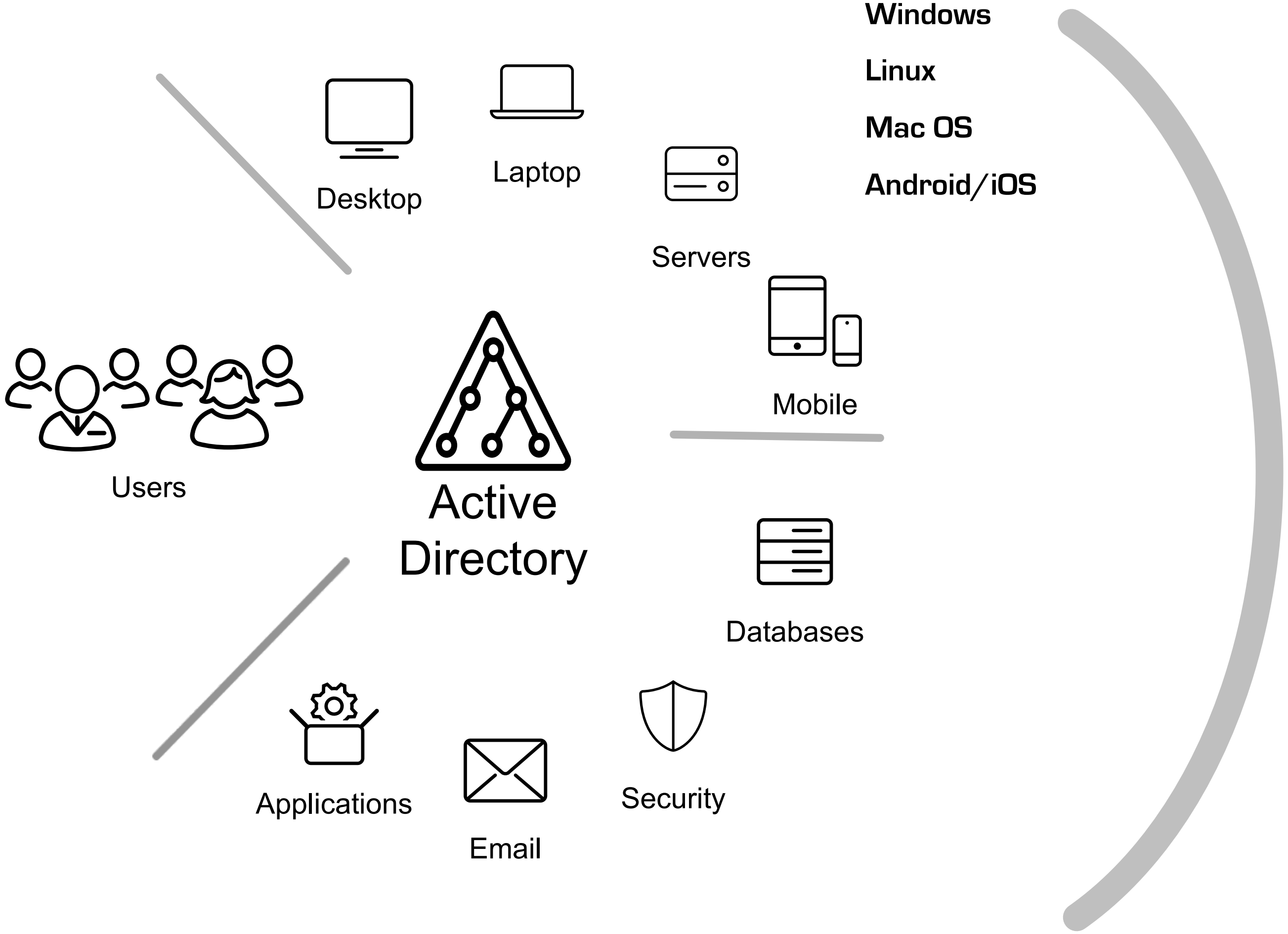
Databases

Applications

Email

Security

Assets Under Active Directory



Active Directory

Users

Desktop

Laptop

Servers

Mobile

Databases

Applications

Email

Security

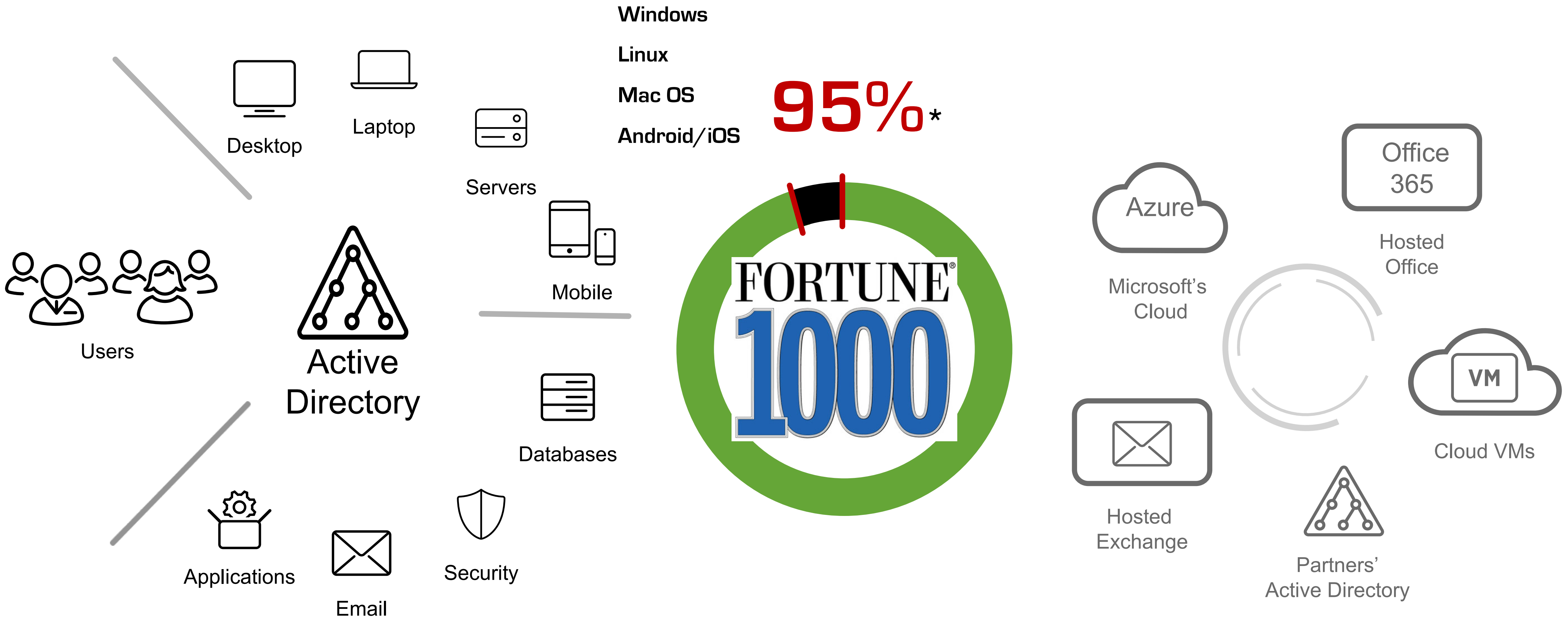
Windows

Linux

Mac OS

Android/iOS

Assets Under Active Directory



Windows

Linux

Mac OS

Android/iOS

95%*

All this is at risk !

Big enigma to security products

* Info Security: http://bit.ly/2hgUY0O

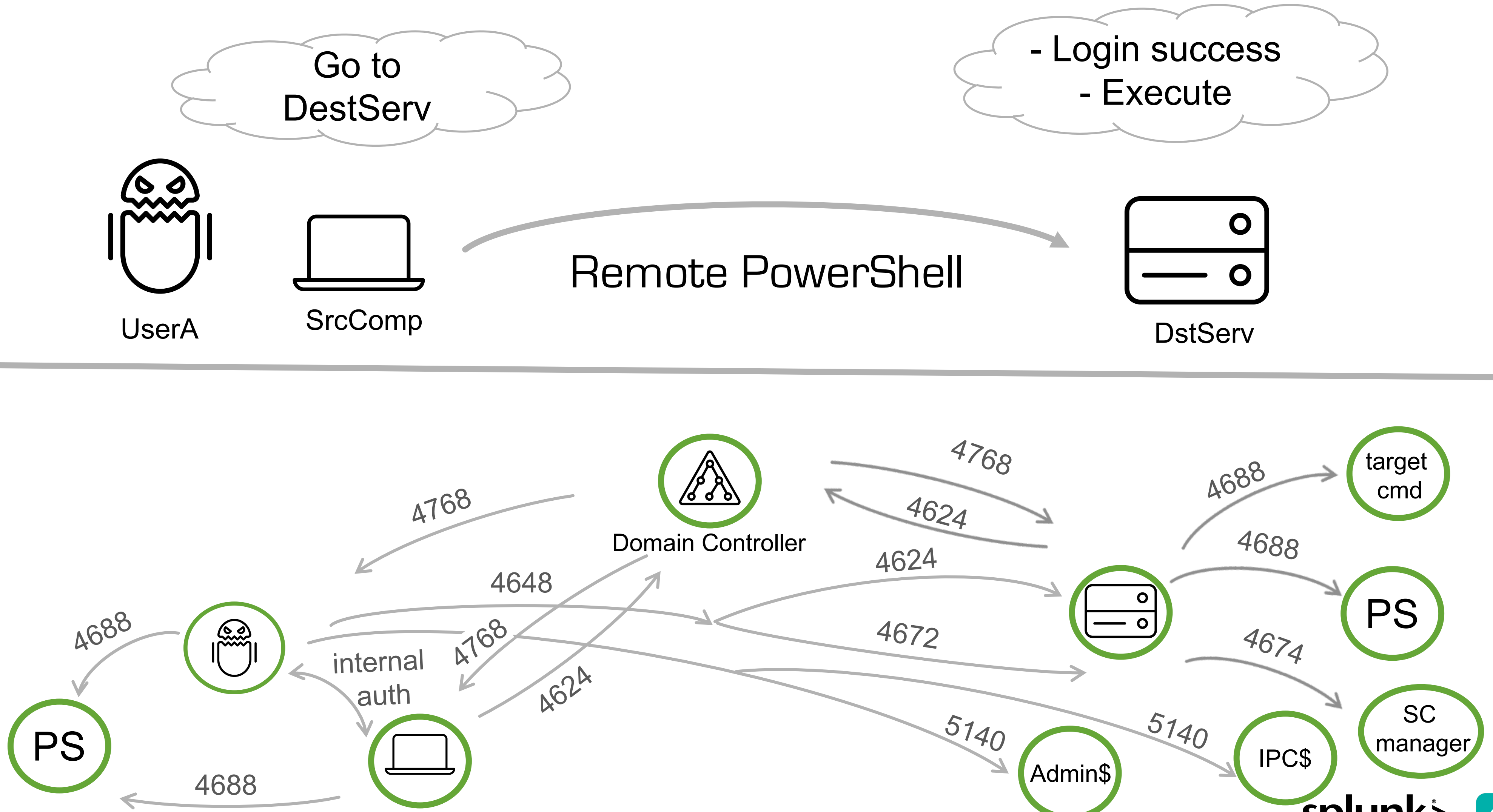
The Talk

- **Unpublished Challenges in AD Security**
  - Spurious attack attributions
  - Over represented incidents
  - Blind spots
- **Splunk UBA: Active Directory Intelligence**
- **State of Your Security**

Root of All Evil

Actual Activities

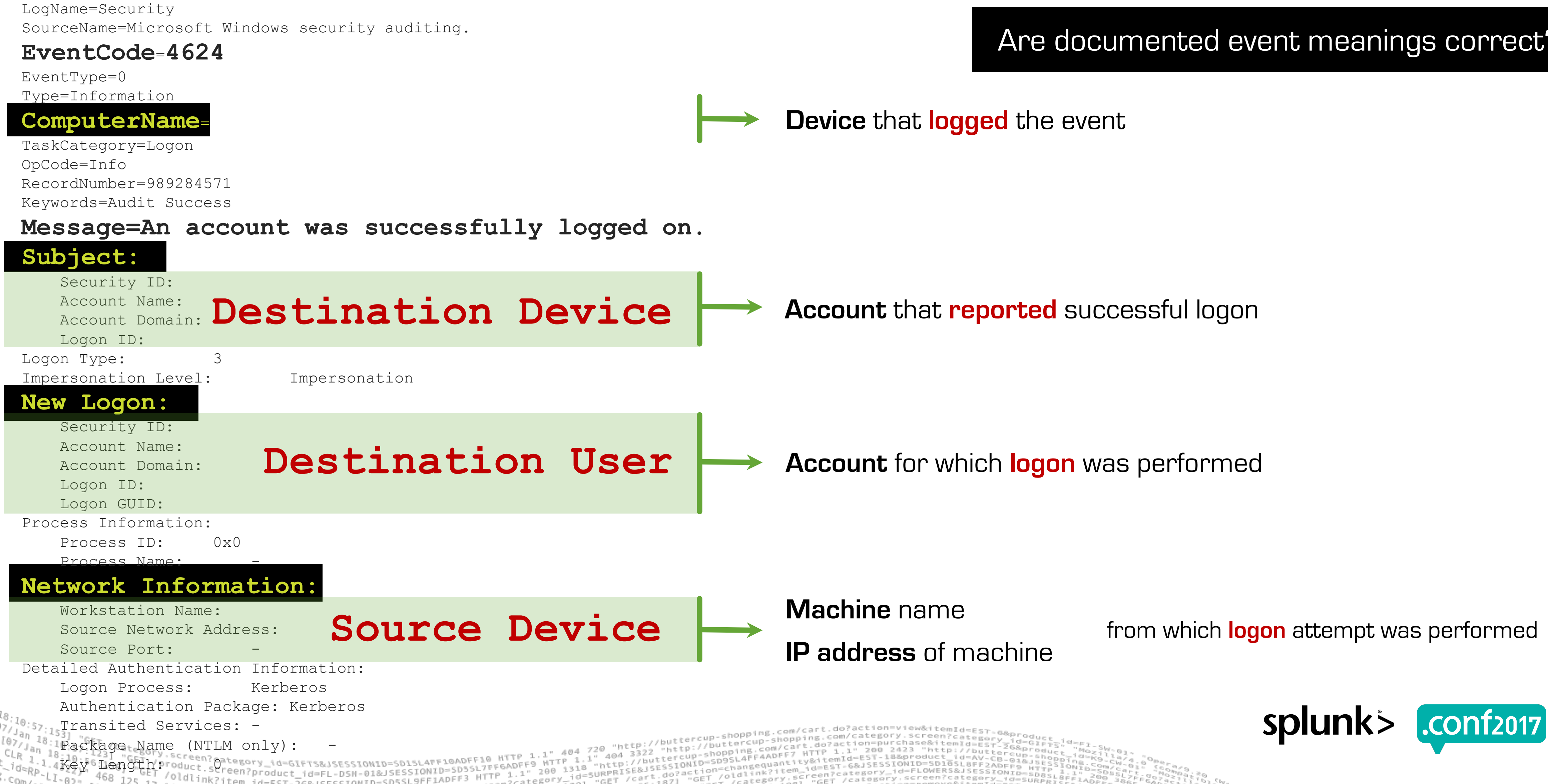
Active Directory Events



Chaotic world of internal micro interactions

Spurious Attack Attribution

Are documented event meanings correct?



```
LogName=Security
SourceName=Microsoft Windows security auditing.
EventCode=4624
EventType=0
Type=Information
ComputerName=
TaskCategory=Logon
OpCode=Info
RecordNumber=989284571
Keywords=Audit Success
Message=An account was successfully logged on.
Subject:
    Security ID:
    Account Name:
    Account Domain:
    Logon ID:
Logon Type:          3
Impersonation Level:        Impersonation
New Logon:
    Security ID:
    Account Name:
    Account Domain:
    Logon ID:
    Logon GUID:
Process Information:
    Process ID:      0x0
    Process Name:        -
Network Information:
    Workstation Name:
    Source Network Address:
    Source Port:         -
Detailed Authentication Information:
    Logon Process:       Kerberos
    Authentication Package: Kerberos
    Transited Services: -
    Package Name (NTLM only):    -
    Key Length:        0
```

Device that **logged** the event

Account that **reported** successful logon

Account for which **logon** was performed

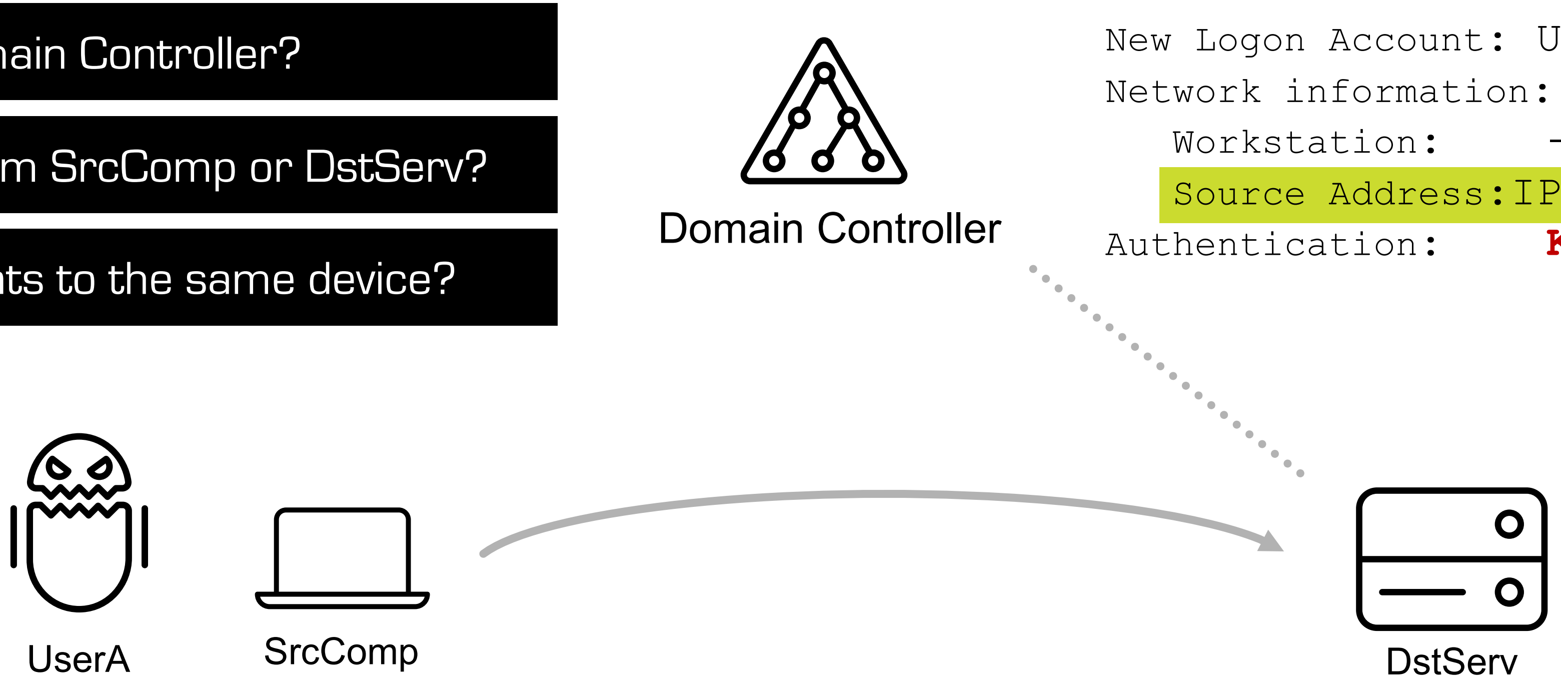
Machine name

IP address of machine

from which **logon** attempt was performed

Spurious Attack Attribution

- UserA at the Domain Controller?
- UserA coming from SrcComp or DstServ?
- Network Info points to the same device?



```
Event:                 4624
New Logon Account:  UserA
Network information:
    Workstation:       -
    Source Address:IP(DstServ)
Authentication:      Kerberos
```

```
Event:                   4624
New Logon Account:   UserA
Network information:
    Workstation:         SrcComp
    Source Address:  IP(SrcComp)
Authentication:          NtLmSsp
```

```
Event:                   4624
New Logon Account:   UserA
Network information:
    Workstation:         DstServ
    Source Address:  IP(SrcComp)
Authentication:          Advapi
```

```
Event ID:               4624
New Logon Account:  UserA
Network information:
    Workstation:         -
    Source Address:  IP(SrcComp)
Authentication:         Kerberos
```

Over Representation Of Incidents

How many logins were there?

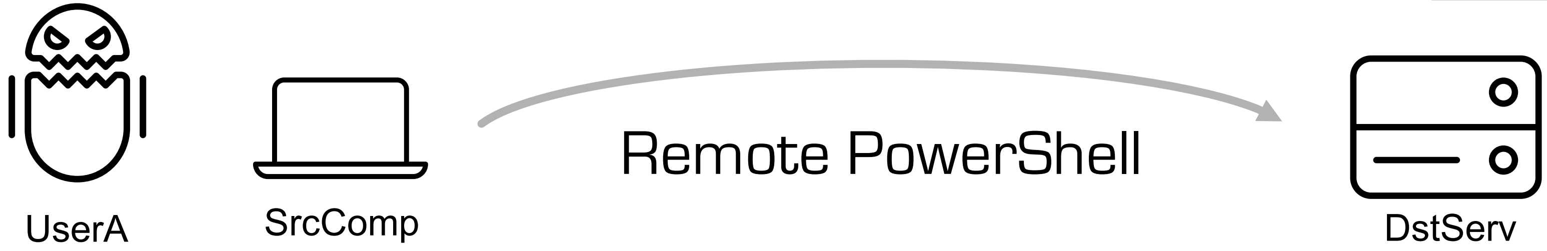
How many processes were run by the user?

Domain Controller

Event	Count
4624 (domain)	5+

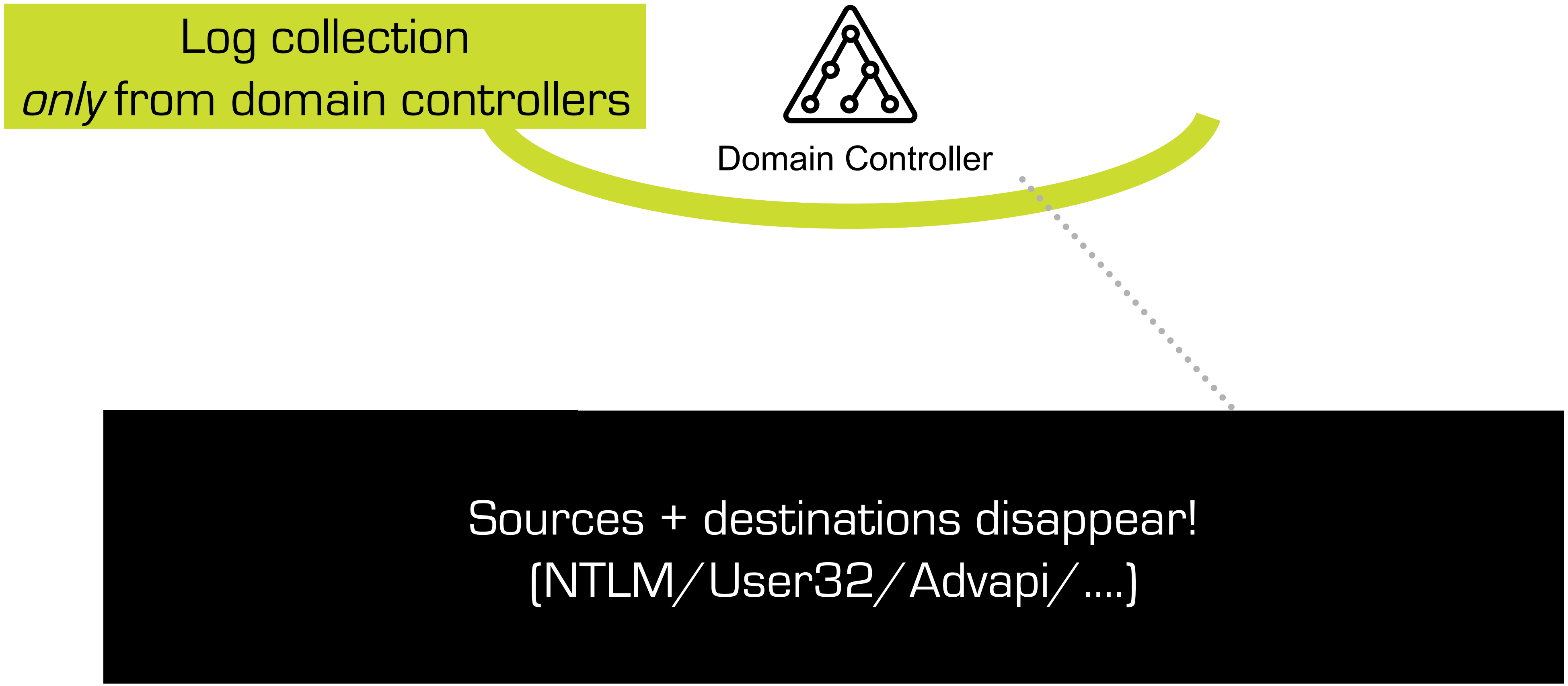
Event	Count
4688	1

Event	Count
4624 (domain)	2
4624 (Advapi)	1
4688	3



Event 4624: An account was successfully logged on
Event 4688: A new process has been created

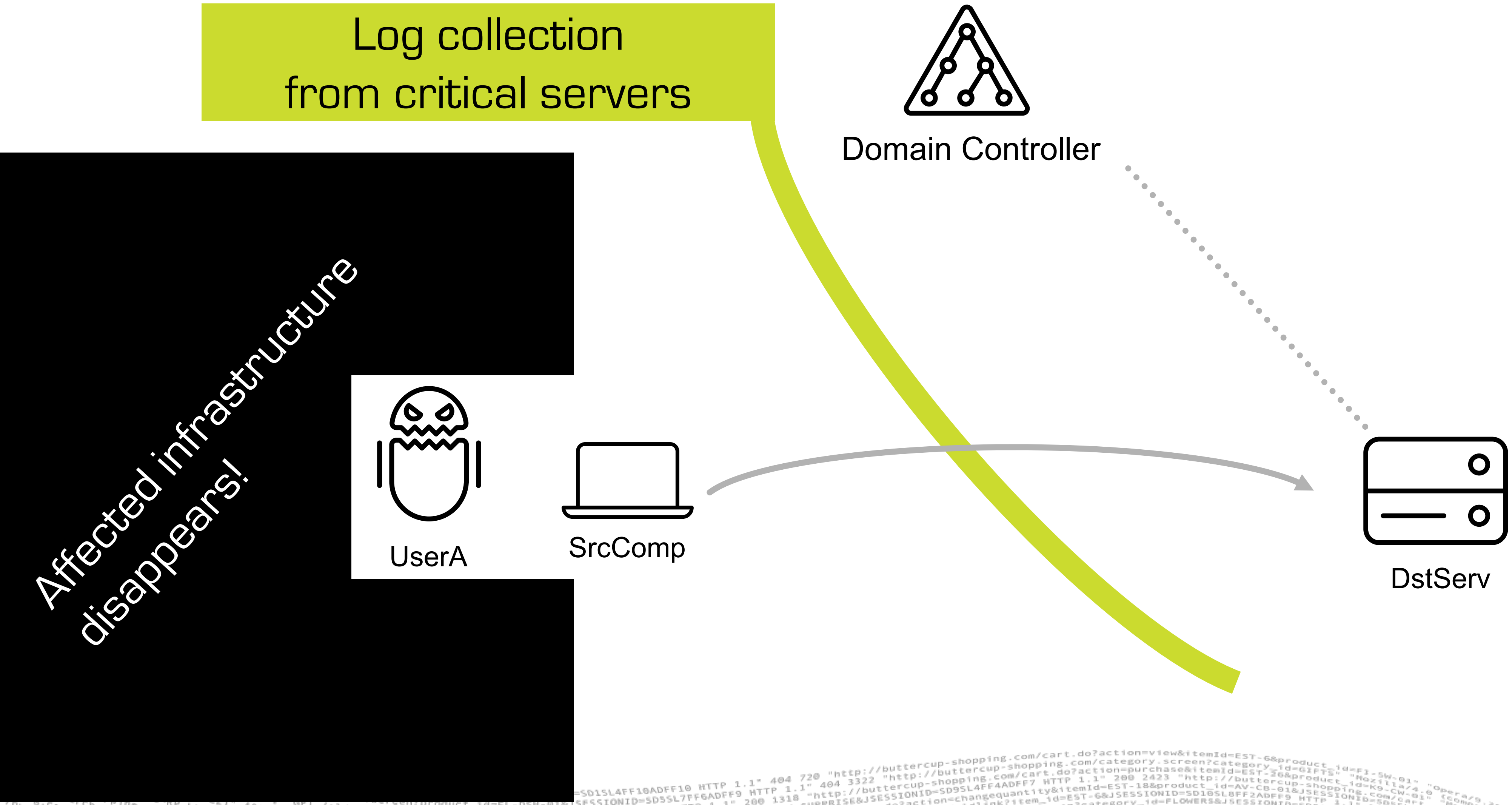
Blind Spots



Log collection
only from domain controllers

Sources + destinations disappear!
(NTLM/User32/Advapi/....)

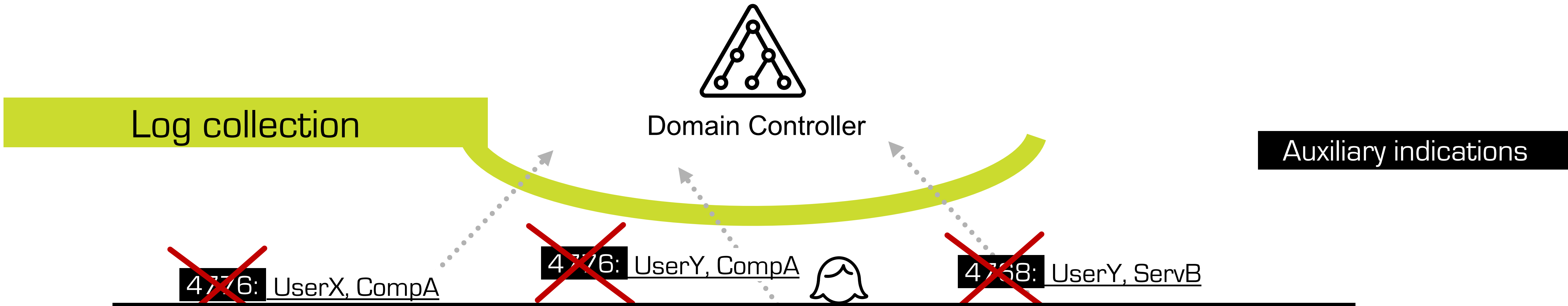
Blind Spots



Log collection
from critical servers

Affected infrastructure
disappears!

Blind Spots

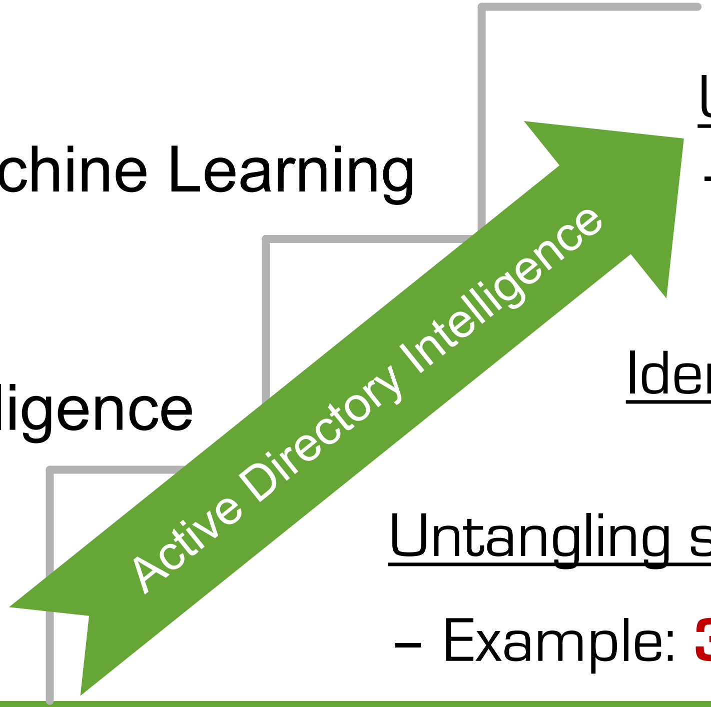


Many things disappear:

- Remote PowerShell
- Access to Shares
- Interactions with Exchange
- Authentications via legacy domain trusts

Splunk UBA:
Active Directory Intelligence

Span of Active Directory Intelligence



Machine Learning

<u>Untangling overrepresentation & blind spots</u>

– Behavioral & peer grouping anomalies

Security Intelligence

<u>Identifying IoC & raising alarms</u>

Data Ingestion / ETL

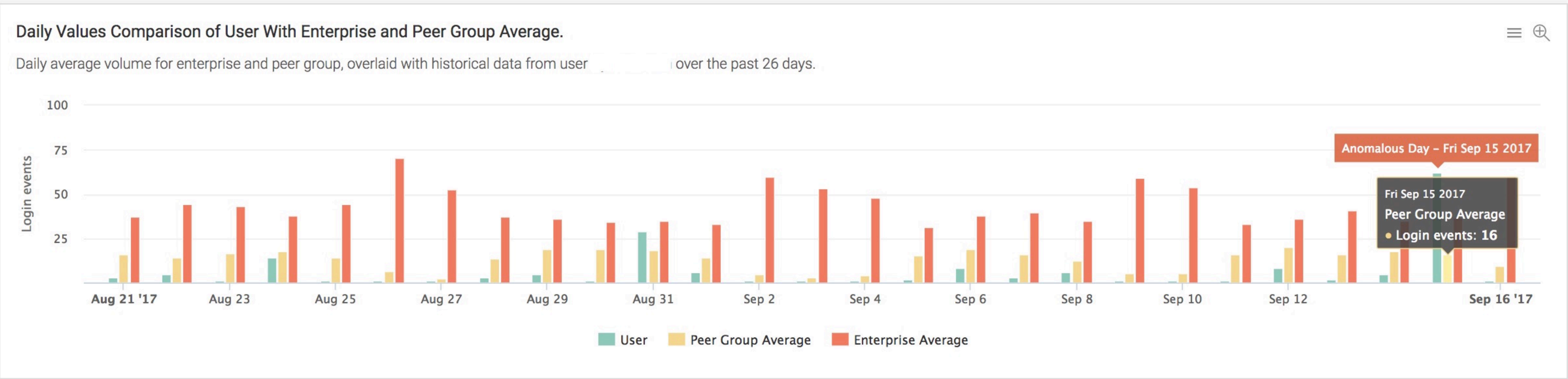
<u>Untangling spurious attributions</u>

– Example: **30+ interpretations of login events**

UBA Lab – Ground truth Infrastructure

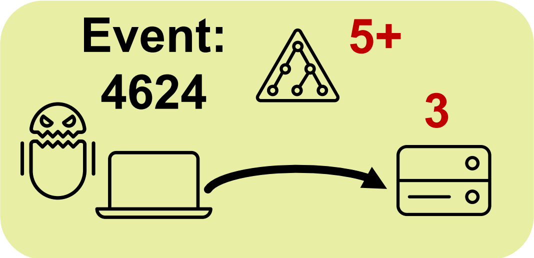
Lack of public knowledge + documentation

Active Directory Intelligence – Machine Learning



Daily Values Comparison of User With Enterprise and Peer Group Average.

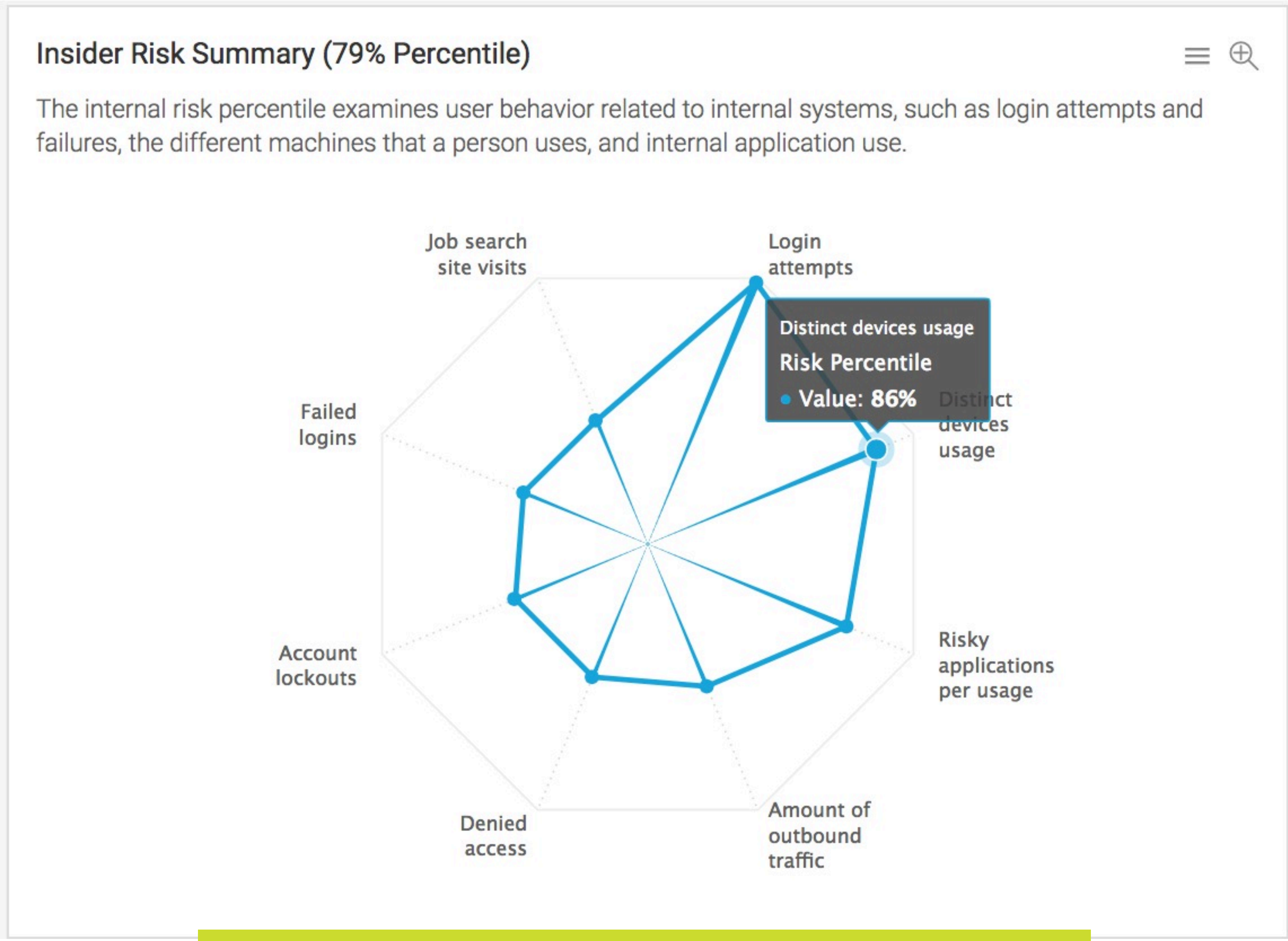
Daily average volume for enterprise and peer group, overlaid with historical data from user [redacted] over the past 26 days.



Event: 4624

Countering inherent over-representation

Active Directory Intelligence – Machine Learning



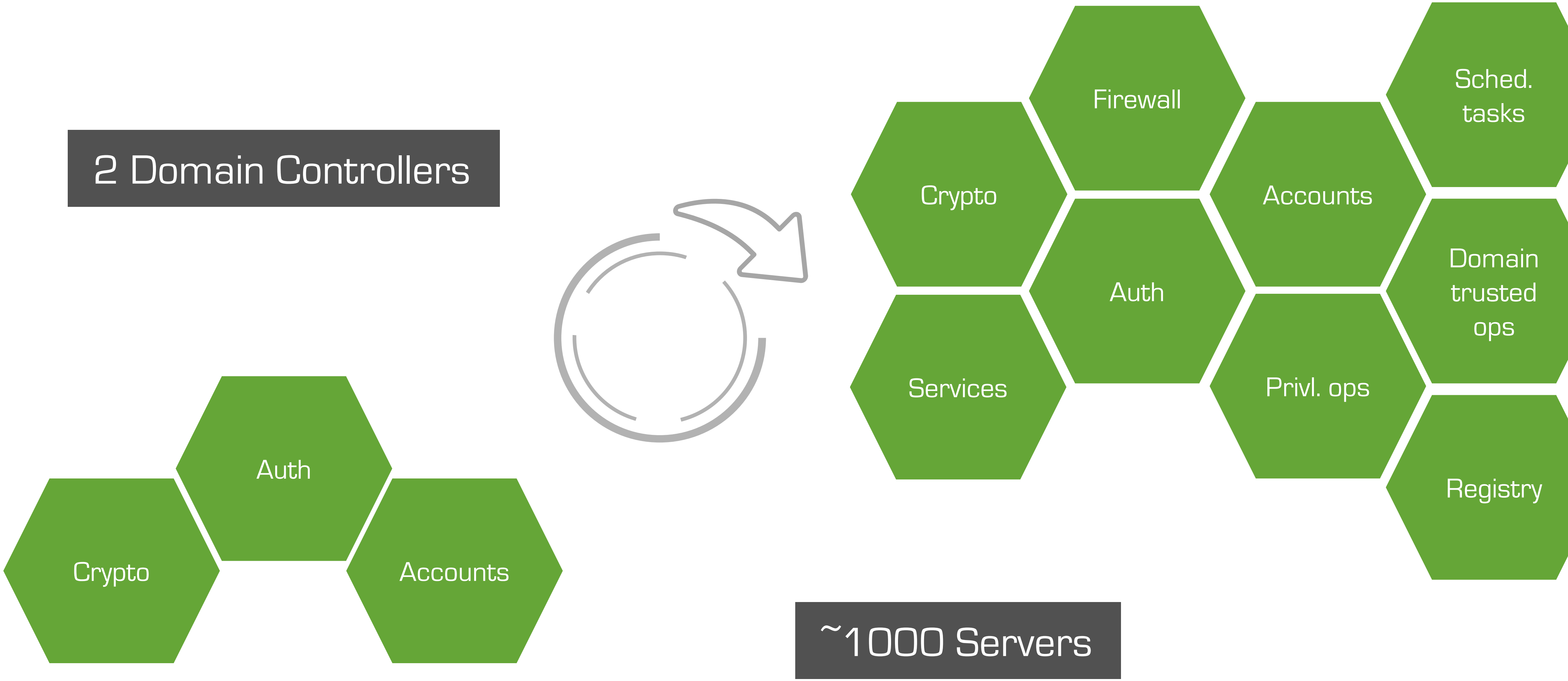
Insider Risk Summary (79% Percentile)

The internal risk percentile examines user behavior related to internal systems, such as login attempts and failures, the different machines that a person uses, and internal application use.

Boosting confidence before threats are raised

State of Your Security

Blind Spots – What/Where Are You Logging?



2 Domain Controllers

Auth

Crypto

Accounts

~1000 Servers

Firewall

Sched. tasks

Crypto

Accounts

Auth

Domain trusted ops

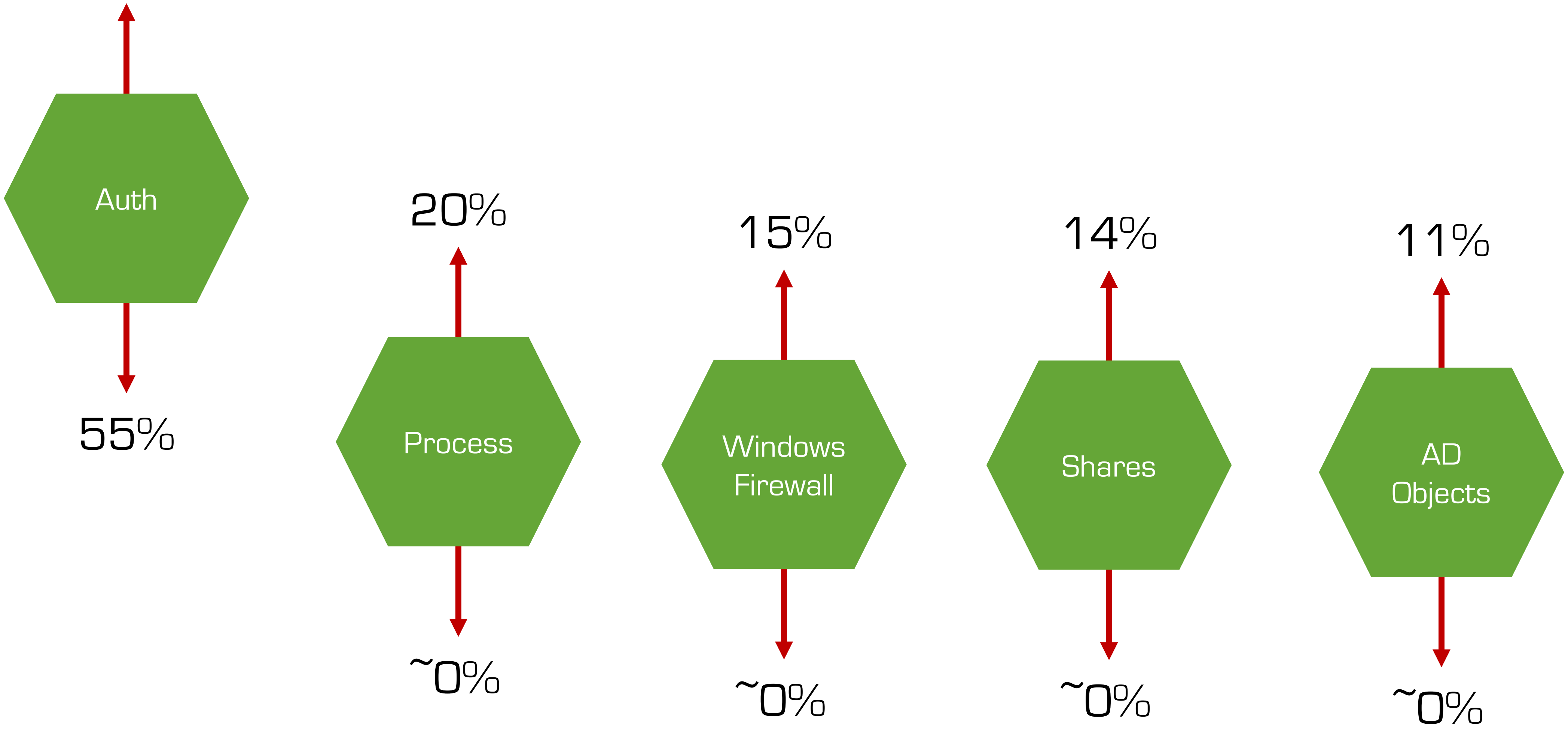
Services

Privl. ops

Registry

Blind Spots – “Cost” Of Logging More

99.5% statistics across various deployments



Auth: 99.5% / 55%

Process: 20% / ~0%

Windows Firewall: 15% / ~0%

Shares: 14% / ~0%

AD Objects: 11% / ~0%

Volume of events

Use Of Safe Authentication Mechanisms

statistics across various deployments

	Min [%]	Avg [%]	Max [%]
Kerberos	62.6	79.8	98.1
NTLM	1.7	16.3	34.1
Advapi	0.1	2.9	8.2
Authz	0	0.8	2.6
User32	0	0	0.0003

- Non Domain Computers
- Windows Shares
- Legacy Domain Trusts
- Exchange Server
- Access via IP addr …

Pass-the-hash exploit is extremely easy!!!

Windows console logins are not enough!

Use of End-of-Life Windows

Domain Controllers

Citrix

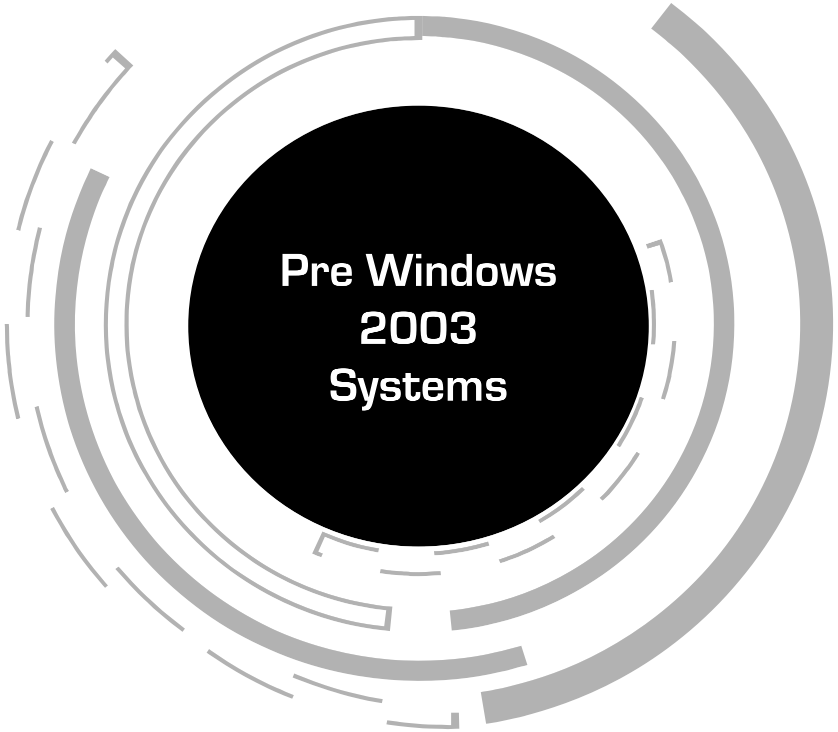
SQL

Web

CRM

Custom Applications

Exchange



Defenses are much weaker!
Events are much poorer!

Key Takeaways

- We know all AD’s tricks!
- Reach out – email or Pavilion booth:
  “Insider Threat Detection & Anomalous Behavior”
- Splunk UBA saves your SOC’s time:
  - Device Access Anomalies
  - Critical Events
  - Lateral Movement
  - Privilege Escalation …

Contact

Stanislav Miskovic, PhD
smiskovic@splunk.com

Thank You

Don't forget to rate this session in the .conf2017 mobile app

splunk> .conf2017