Splunk UBA:
Setting Active Directory’s Security Straight
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.

Splunk, Splunk>, Listen to Your Data, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2017 Splunk Inc. All rights reserved.
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
- Databases
- Applications
- Email
- Security
- Users

Active Directory
Assets Under Active Directory
Assets Under Active Directory

Windows
Linux
Mac OS
Android/iOS

All this is at risk!
Big enigma to security products

95%*

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- Unpublished Challenges in AD Security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

Go to DestServ

Remote PowerShell

- Login success
- Execute

Actual Activities

UserA
SrcComp

Active Directory Events

Domain Controller

Chaotic world of internal micro interactions

目标 cmd
Spurious Attack Attribution

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:

Device that logged the event
Account that reported successful logon
Account for which logon was performed
Machine name
IP address of machine

Are documented event meanings correct?
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: -
  Source Address: IP(SrcComp)
Authentication: Advapi
Over Representation Of Incidents

How many logins were there?
How many processes were run by the user?

<table>
<thead>
<tr>
<th>Event</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>4688</td>
<td>1</td>
</tr>
<tr>
<td>4624 (domain)</td>
<td>5+</td>
</tr>
<tr>
<td>4624 (Advapi)</td>
<td>1</td>
</tr>
<tr>
<td>4688</td>
<td>3</td>
</tr>
</tbody>
</table>

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

Remote PowerShell
Blind Spots

Log collection *only* from domain controllers

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

Log collection from critical servers

Affected infrastructure disappears!

Domain Controller

UserA  SrcComp  DstServ
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

- Untangling overrepresentation & blind spots
  - Behavioral & peer grouping anomalies
- Untangling spurious attributions
  - Example: 30+ interpretations of login events

Lack of public knowledge + documentation

UBA Lab – Ground truth Infrastructure
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 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.

- Distinct devices usage
- Risk Percentile: 86%

Boosting confidence before threats are raised
State of Your Security
Blind Spots – What/Where Are You Logging?

- 2 Domain Controllers
- ~1000 Servers

Diagram:
- Firewall
- Accounts
- Domain trusted ops
- Privl. ops
- Registry
- Sched. tasks
- Services
- Auth
- Crypto
- Auth
- Accounts
- Crypto
- ~1000 Servers
Blind Spots – “Cost” Of Logging More

99.5% statistics across various deployments

- **Auth**: 55%
- **Process**: ~0%
- **Windows Firewall**: ~0%
- **Shares**: ~0%
- **AD Objects**: ~0%

Volume of events
### Use Of Safe Authentication Mechanisms

Statistics across various deployments

<table>
<thead>
<tr>
<th></th>
<th>Min [%]</th>
<th>Avg [%]</th>
<th>Max [%]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kerberos</td>
<td>62.6</td>
<td>79.8</td>
<td>98.1</td>
</tr>
<tr>
<td>NTLM</td>
<td>1.7</td>
<td>16.3</td>
<td>34.1</td>
</tr>
<tr>
<td>Advapi</td>
<td>0.1</td>
<td>2.9</td>
<td>8.2</td>
</tr>
<tr>
<td>Authz</td>
<td>0</td>
<td>0.8</td>
<td>2.6</td>
</tr>
<tr>
<td>User32</td>
<td>0</td>
<td>0</td>
<td>0.0003</td>
</tr>
</tbody>
</table>

- 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

Pre Windows 2003 Systems

Citrix

Web

Custom Applications

SQL

CRM

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