Know Your Insider

Unmasking Lateral Movement with Splunk UBA

Satheesh Joseph | Principal Data Scientist, Splunk

Sep 26 | 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.

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.
About the Authors

Satheesh Joseph
sjoseph@splunk.com
Principal Data Scientist, Splunk

His work spans data science applications in security, big data, analytics and scalable data engineering.

Satheesh holds a Bachelors degree in computer science from University of Madras, India.

Stanislav Miskovic
smiskovic@splunk.com
Principal Data Scientist, Splunk

His work spans data science applications in privacy, security and network communications.

Stanislav holds a Ph.D. in electrical and computer engineering from Rice University, Houston, TX, and M.Sc. degree from the University of Belgrade, Serbia.

George Apostolopoulos
gapostolopoulos@splunk.com
Director of Engineering, Splunk

For the last few years he has been working on the intersection of security, big data and analytics, focusing on log analysis.

George holds a Ph.D. and M.Sc in computer science from the Univ. of Maryland in College Park and a B.Sc. in computer engineering from University of Patras, Greece.
Agenda

- Stats & Industry Challenges
- Insider Threat Stages
- Technical Challenges
- Lateral Movement in the Real World
- UBA Detects Lateral Movement
- Demo
Stats, History & Industry Challenges
Biggest Cybersecurity Threats Are Inside Your Company

Average Detection Time
- Outsider: 107 days
- Insider: 37 days

Time spent on each stage of the Attack
- Initial Breach
- Lateral Movement
- Final Goal

Logic Bomb: 1996
- Tim Lloyd
- 2009

WikiLeaks: 2013
- Chelsea Manning

Edward Snowden: 2013

Anthony Levandowski: 2017

Source: M-Trends 2017
SMOKESCREEN
Industry Challenge: A Call To Action

Chronic Ailment – Not Enough Resources
- Research / Subject Matter Expertise
  - Techniques
  - Logs & specifically Active Directory
- Lack of orchestration
- Cost prohibitive for SMBs
- Creates 3rd and 4th party risk. Nobody is immune
- Security workforce shortage
- 0% unemployment, Huge unfilled requisitions
A Better Model For Today

Research / SME

SOC

Advanced Orchestration, Operational Awareness and Preventative Capabilities
Insider Threat
Kill Chain
Insider Threat Stages

Tipping Point
- Emotional
- Flight Risk

Lateral Movement
- Recon
- Enumeration
- Exploitation
- Offensive packages

Final Goal
- Exfiltration
- Destruction
- Modification

Human Driving Factors

Too late to prevent

Data
Technical challenges faced by the SOC Analyst
Techniques, Tactics & Procedures (TTPs)

- PsExec
- PowerShell
- WMI
- Expanding Access
  - Admin Shares
  - PsExec
  - Diamond PAC
- Privilege Escalation
  - Dest.
  - Port
  - Time
- Port Scan
- Cleanup
- SPN Scan
- Kerberoast
- Mimikatz
- DCSync
- Enumeration
  - Privileged Account
  - Credentials
  - SPN Scan

© 2017 SPLUNK INC.
A Login Activity from the Perspective of Active Directory Logs

- **Lsass.exe**
  - 2 login events (4648)
  - 1 Process Creation event (4688)

- **Kerberos**
  - 6+ login events (4624)
  - 2 Object Access events (4661)
  - 4+ privilege escalation 4672
  - Multiple Service Ticket requests

- **Winlogon.exe**
  - 2 login events (4624)
  - One 4648 event
  - 1 Special Privilege event
  - 2 process creation event
  - Multiple Object Access event

4624 => An account was successfully logged on
4648 => A logon was attempted using explicit credentials
4672 => Special privileges assigned to new logon
4661 => A handle to an object was requested
4769 => A Kerberos service ticket was requested
Active Directory Vantage Points

RDP login to a domain account, source and destination are domain members

- 10.141.38.100 (workstation1)
  - Bob logging in as Admin from 100 to 101

- Domain Controller
  - Admin asking service ticket for 100 and 101
  - Admin logging in to 101

- 10.141.38.101 (workstation2)
  - Admin logging in from 100 to 101
UBA Intelligence
Lateral Movement in the Real World

- Kerberos Pre Auth Failed
- Kerberos Auth Ticket Requested
- Privilege Escalation
- Process Creation
- Kerberos Pre Auth Failed
- Kerberos Auth Ticket Requested
- Privilege Escalation
- Process Creation

Anomalies
- Unusual Zone Access
- Unusual Machine Access
- Unusual Windows Sequence

Temporal Correlation
Connecting Rare Paths

Subtle IOC
- Increase in Auth Tickets
- Increase in process creation
- Unusual Registry Access

User Transition
- Suspicious Privilege Escalation
- Rare User Transition

IOC

Admin

Bob

Anomalies

IOC

IOC

Admin
UBA Detects Lateral Movement

Users

Users with Anomalies
UBA Detects Lateral Movement
Mining Anomalies

Anomalies
- Rare
- Unusual Sequence
- Out Of Profile

Meta Data
- Profiling
- Context

Contextual Anomalies

Unusual Windows Sequence of Events
- Involves high deviation from baseline
- Involves new activities
- Involves out of peer group activities

Rare Process or Events
- Enterprise or Peer Group

UBA
UBA Detects Lateral Movement
Higher Level - Indicators of Compromise

- Enumeration
- Return Code
- Group Edits
- Lockouts

- Rare Process
- Rare Events
- Suspicious Process

- Anomalies reflect Insider movements, derive context and continuity

- Kerberos Service Tickets
- Kerberos Authentication
UBA Detects Lateral Movement

Lateral Movement Kill Chain in time sequence

Service Account

Bob

Charlie

UBA
Lateral Movement Demo
Lateral Movement

Categories: Internal, Specialized Threat Model

Threat model observed the following stages of Lateral Movement Kill Chain phase while analyzing user’s behavior before and after in time.

- **Suspicious or rare process:** This stage involves a process that is tagged as suspicious and used for Lateral Movement and a process that is only observed across few users and days and a process that is not seen in enterprise or user’s peer group.

- **Activities that deviated from the baseline:** This stage involves out of profile activities by the user.

- **Probing activities:** This stage involves repeatedly creating multiple new processes, an indicator that is predominantly seen in lateral movement and suspicious probe action, caused by failure return codes for ticket request across multiple devices and suspicious probe action, caused by credential validation for multiple machines.

Timeline:

- **Start Date:** 22 Aug, 2017
- **Last Update:** 2 Sep, 2017
- **Duration:** 11d

Anomalies (4):

- Unusual AD Event (4)

Users (1):

- Ken Westin

Devices (2):

- Internal
  - cnu2509kyq-a
  - cnu2509kyq-a.buttercup.com

Threat Relations
Advanced Correlation and Analytics Layer
Deeper Insights With UBA to Detect Anomalies

What we Know
- Truly Adaptive and Holistic Security

What we Don’t
- ES
- UBA

Truly Adaptive and Holistic Security
Improved quality of alerts means we can deprecate less effective/efficient correlations, reducing volume of alerts and time on dead ends.

Investigation is accelerated due to the intuitive way a threat is visually portrayed in UBA.

Allows us to invest more resources in engineering orchestration, developing operational awareness and threat prevention activities.
1. TTPs vary, vast, in-memory and gets less noisy
2. Consider Authentication & Service tickets along with Login events
3. Insider Threat is a continuous process
4. SME Knowledge + ML + Active Research or Buy Splunk UBA 4.0
Thank You

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