AVESHKA

Are you Ready?

# CONDUCTING USER ACTIVITY WITH YOUR EXISTING INFRASTRUCTURE

October 2018

# Max Alexander, DPA, CISSP, CISM, CISA

## CHIEF TECHNOLOGY OFFICER, DIGITAL TRANSFORMATION

## AVESHKA INC

- US Army (Retired), Intelligence Operations Officer
- Counterintelligence (CI), Human Intelligence (HUMINT), and Signals Intelligence Collection (SIGINT)
- Certified DoD Cyber Crime Investigator
- Professor of Digital Forensics at The George Washington University and the University of Maryland University
- Master of Science and Technology Intelligence from the National Intelligence University
- Master of Engineering (Cybersecurity) from The George Washington University
- Doctorate in Public Administration (Science and Technology Policy) from Valdosta State University
- Corporate experience in implementing insider threat and cybersecurity governance in government, corporate, and non-profit organizations.

# Terminal Learning Objectives

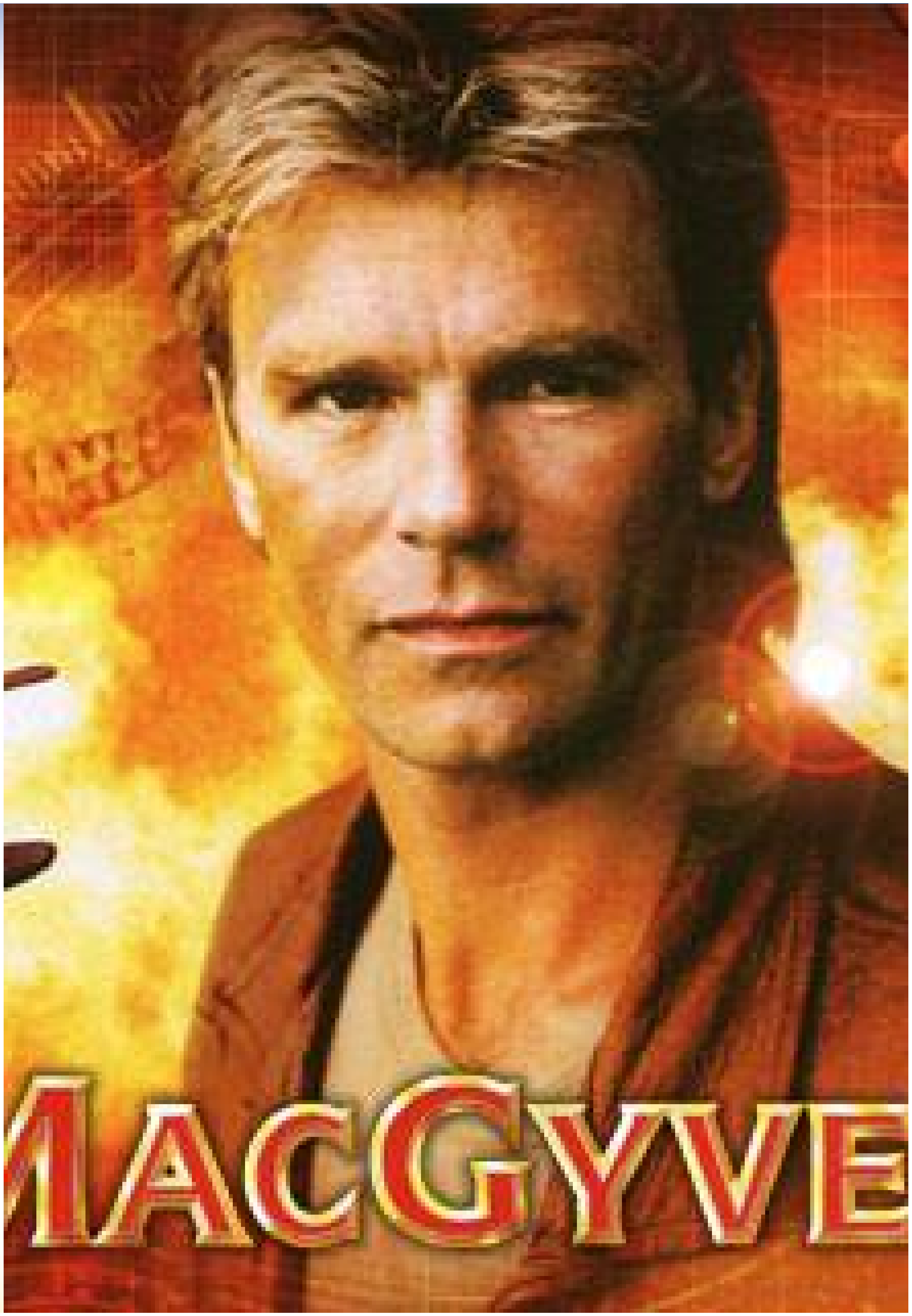
- nderstanding what you want to monitor
  - Crown Jewels Assessment
  - Planning your UAM program
- esource assessment
  - Data Assessment
  - Tool Assessment
  - Resource Efficiency
- mplementing the solution
  - Tuning your existing cyber tools
  - Monitoring

# It’s MacGyver Time

How can I best protect my organization with the assets I have?

How can I reduce the insider threat attack surface of my organization with limited resources?

How can I use cybersecurity tools to manage insider threat risk?



# You can do it

## BUT NOT SO FAST

- **“Given the time, it is possible to tune your existing cybersecurity tools to detect insider threats”**

- You will experience failures in your quest to implement a UAM program because of the follow issues:
  - Failure to plan
  - Failure to understand your data
  - It is a secondary task
  - You do not have enough resources
  - You try to do too much, too fast

# Where do we want to go and how do we get there?

[redacted]

*"If you don't know where you are going, you might wind up someplace else."*

[redacted]

- *Yogi Berra*

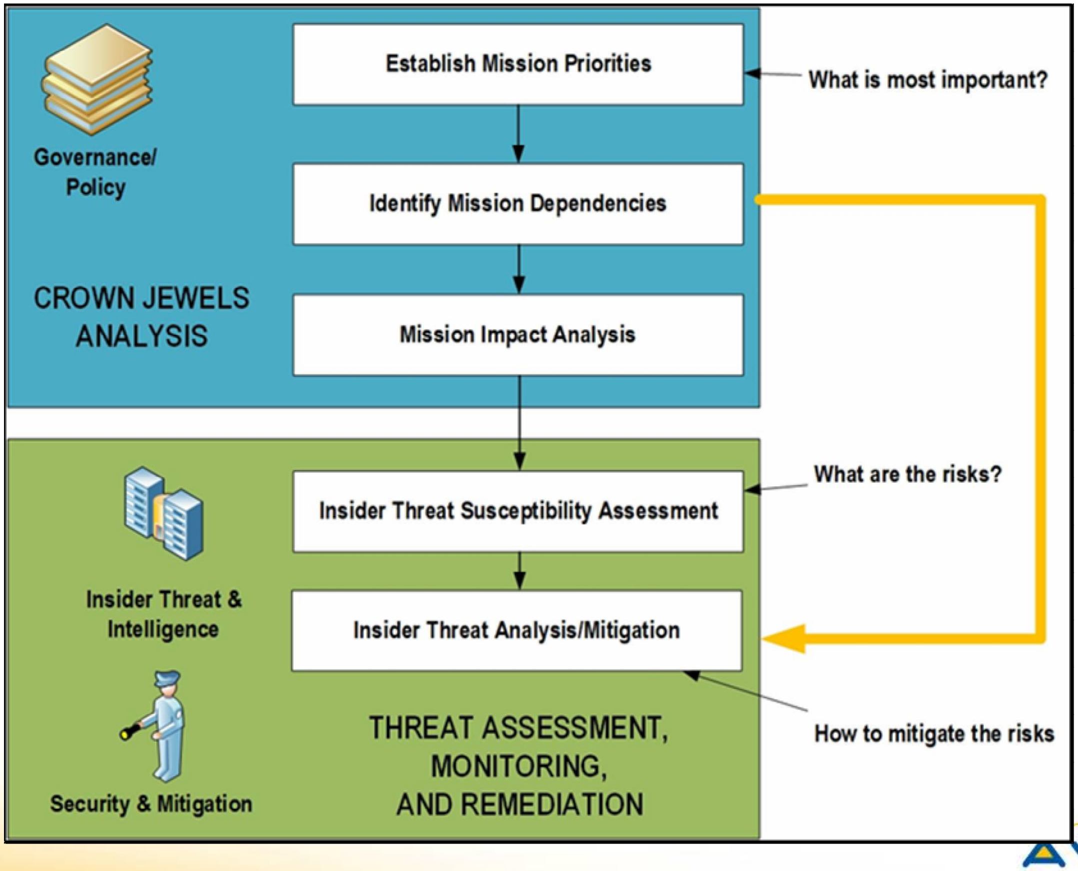
[redacted]

# Picking Your Destination

- hat do I want to detect?
- hat data do I need to detect it?
- ow am I going to detect it?
- ow am I going to analyze the data?
- hat do I do once I find something?
- hat am I required to do?
- hat other resources do I need?
- s UAM going to be a secondary task or will I hire a dedicated team?

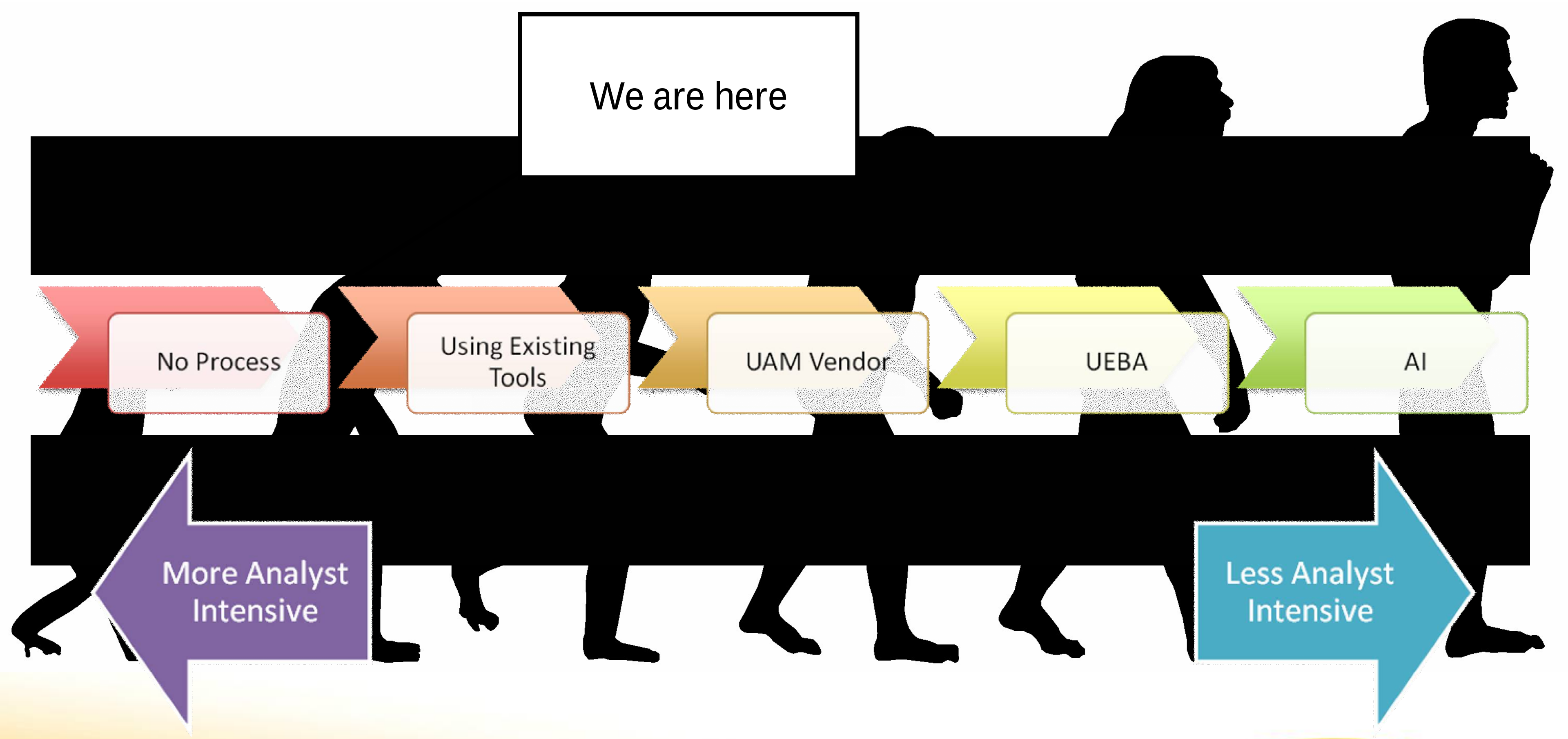
# Crown Jewels Assessment

## PROTECTING WHAT MATTERS WITH EFFICIENCY


Governance/ Policy
CROWN JEWELS ANALYSIS
Establish Mission Priorities
What is most important?
Identify Mission Dependencies
Mission Impact Analysis
Insider Threat & Intelligence
Insider Threat Susceptibility Assessment
What are the risks?
Insider Threat Analysis/Mitigation
Security & Mitigation
THREAT ASSESSMENT, MONITORING, AND REMEDIATION
How to mitigate the risks

# UAM Tools Perspective

## UAM TOOL EVOLUTION



AVESHKA

# Countermeasures

## USER ACTIVITY MONITORING TRIAD

People

•Trained analyst able to recognize InT behavior

•A fool with a tool, is still a fool

Process

•Is what I am doing legal/what data can I look at?

•What do I do when I catch someone?

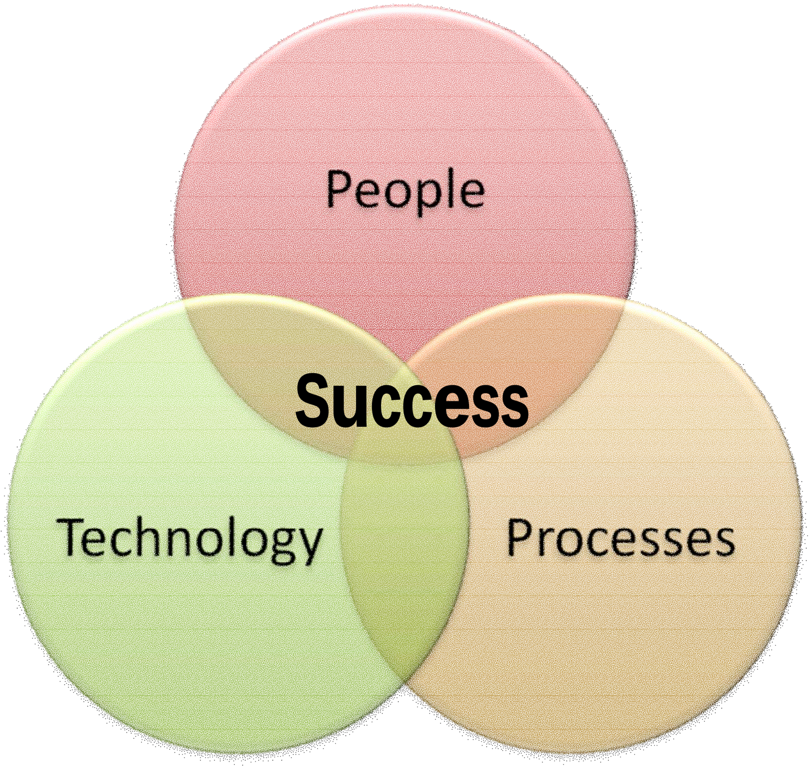
•If you do not already have good cybersecurity and governance polices, a new process will not help you.

Technology

•Data

•Establish triggers or thresholds

•Alerting



# Measurements

## FINDING THE METRICS THAT MATTER

- Without data, you are just another person with an opinion.
- If you cannot measure it, you cannot manage it.
- Measure what you need to know,
- Report on what you want to change
- Be consistent, especially important for analysis over time.
- Use Dashboards

- Data: A signal, stimulus, or fact
- Information: A collection of data in a series, or otherwise organized
- Knowledge: Information placed into relevant context
- Wisdom: The ability to put knowledge into practical use

# Data Sources

## THE MOST BANG FOR YOUR BUCK

Where I am likely to experience a  risk?
How do I monitor for that risk?

Important Data sources:
•Printmon (Quantity, Type)
•Antivirus (Numerous events)
•DLP (Frequent burning, type of data)
•Proxies (unauthorized activity, competitor)
•Netflow (Internal network probing)
•Evtx (Log on/Log Off, Security, Log Clear)
•Email server (Data, Competitor)

# Understanding Human Behavior

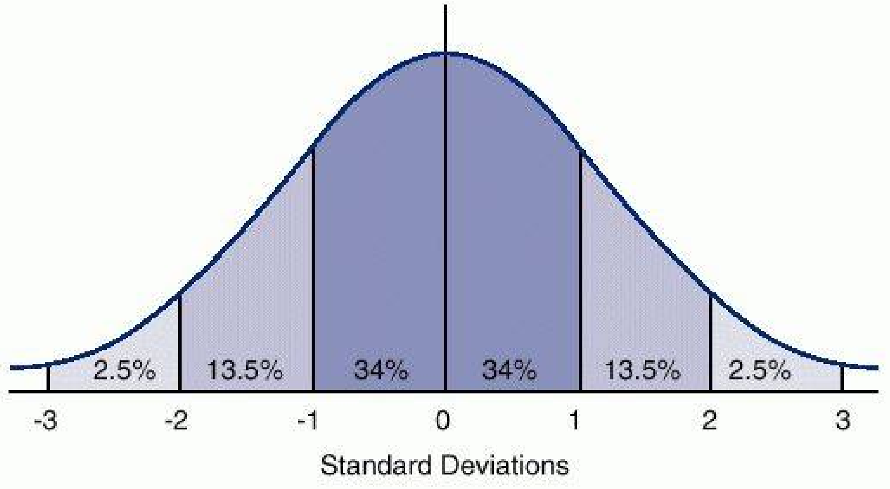
## USING YOUR SIEM TO FIND ANOMALIES

- What else can we look for?
- A user doing something he has never done before
  - Printing from a new printer
  - Visiting new websites
  - Working different hours
  - Job searching
- A user doing something outside the norm for his peer group
  - Larger than normal printing
  - Burning disks
  - Contact outside the organization
- A user violating the laws of space-time.
  - A user should not be on vacation and logging in at work at the same time
- Even if a user trips one of these triggers he is not “guilty” of being an insider threat
- More monitoring may be warranted

# Finding Evil Using Hypotheses

## DETERMINING WHAT TO LOOK FOR

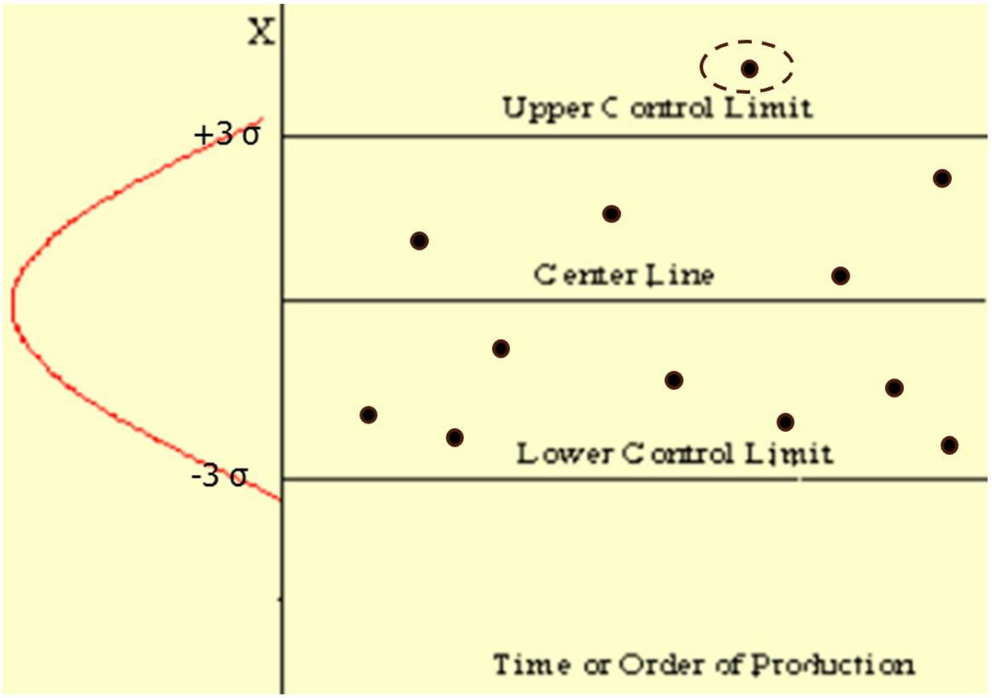
- Insider Threats will exhibit behavior that can be defined as “abnormal.”
- To find evil you must know what is normal
- E.g. “It is suspicious when a user is three standard deviations away from normal when analyzing print volume.”
- Therefore you must have a tool that allows you to analyze behavior across a population.
- Visualization is key
- May be harder to detect low and slow attacks, but those users will eventually fall outside the norm



AVESHKA

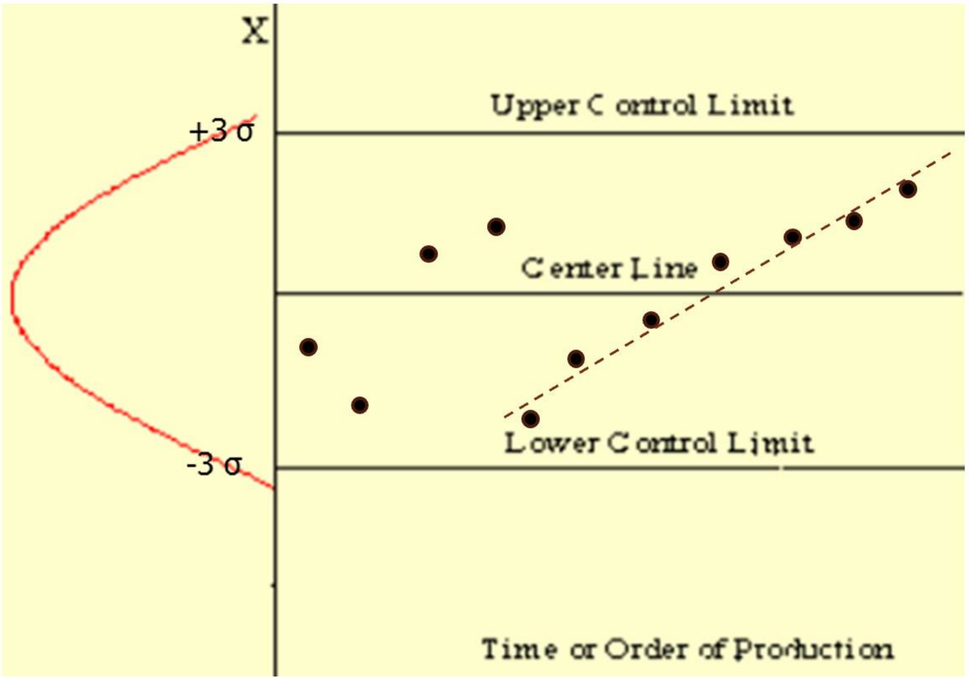
# Process Control Chart

PROCESS IS OUT OF CONTROL



# Process Control Chart

- ULE OF 7
- ROCESS IS TRENDING OUT OF CONTROL

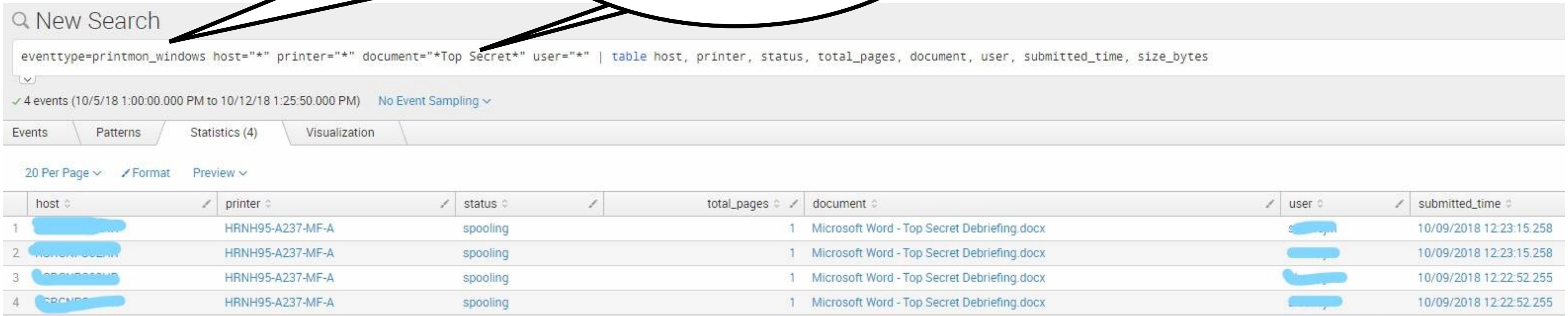


# Suspicious Document Printing

## TOP SECRET DOCUMENT

Printmon Index

*Top Secret*



New Search

```
eventtype=printmon_windows host="*" printer="*" document="*Top Secret*" user="*" | table host, printer, status, total_pages, document, user, submitted_time, size_bytes
```

✓ 4 events (10/5/18 1:00:00.000 PM to 10/12/18 1:25:50.000 PM) No Event Sampling

| | host | printer | status | total_pages | document | user | submitted_time |
|---|---|---|---|---|---|---|---|
| 1 | [redacted] | HRNH95-A237-MF-A | spooling | 1 | Microsoft Word - Top Secret Debriefing.docx | [redacted] | 10/09/2018 12:23:15.258 |
| 2 | [redacted] | HRNH95-A237-MF-A | spooling | 1 | Microsoft Word - Top Secret Debriefing.docx | [redacted] | 10/09/2018 12:23:15.258 |
| 3 | [redacted] | HRNH95-A237-MF-A | spooling | 1 | Microsoft Word - Top Secret Debriefing.docx | [redacted] | 10/09/2018 12:22:52.255 |
| 4 | [redacted] | HRNH95-A237-MF-A | spooling | 1 | Microsoft Word - Top Secret Debriefing.docx | [redacted] | 10/09/2018 12:22:52.255 |

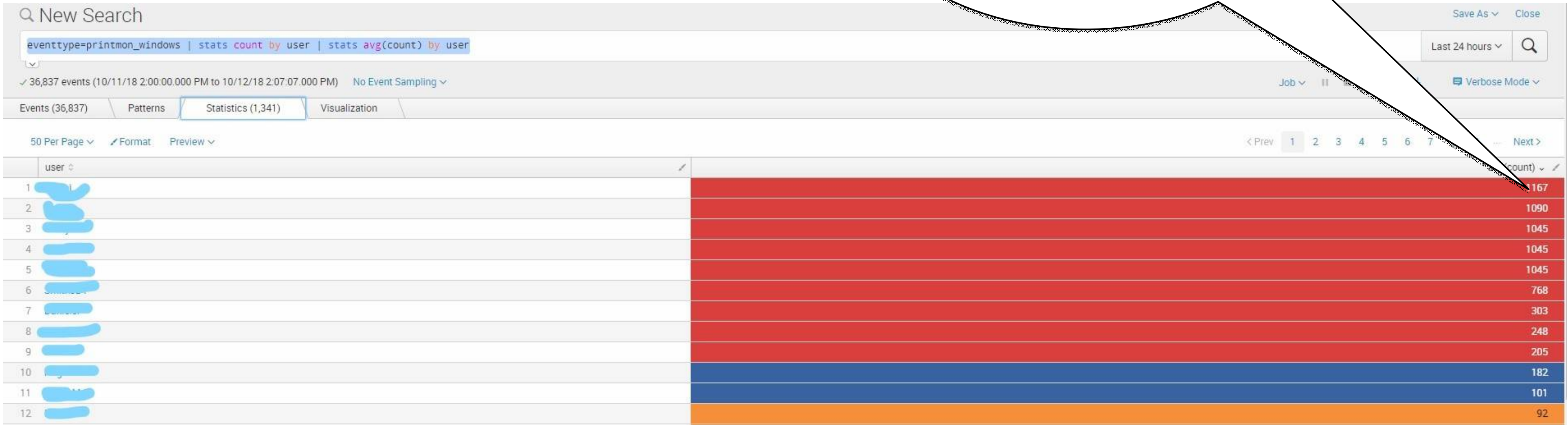
Top Secret Debriefing.docx

User Name and DTG

# Print Volume

## AVERAGE PAGES PER USER

Identifying High Volume Users



```
eventtype=printmon_windows | stats count by user | stats avg(count) by user
```

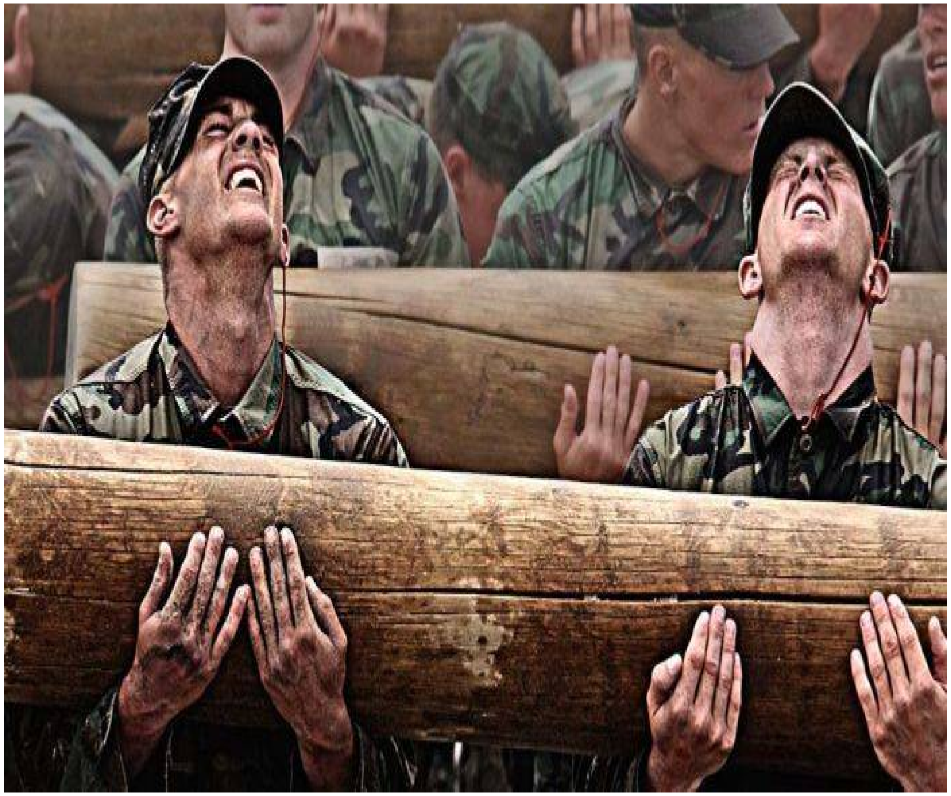
✓ 36,837 events (10/11/18 2:00:00.000 PM to 10/12/18 2:07:07.000 PM)

|  | user | (count) |
|---|---|---|
| 1 | [redacted] | 1167 |
| 2 | [redacted] | 1090 |
| 3 | [redacted] | 1045 |
| 4 | [redacted] | 1045 |
| 5 | [redacted] | 1045 |
| 6 | [redacted] | 768 |
| 7 | [redacted] | 303 |
| 8 | [redacted] | 248 |
| 9 | [redacted] | 205 |
| 10 | [redacted] | 182 |
| 11 | [redacted] | 101 |
| 12 | [redacted] | 92 |

# Make Your Bed Everyday

## DOING THE SIMPLE “STUFF” WELL

- Using cybersecurity policies to your advantage
  - Do you have a user agreement?
  - Do you have a Privileged Access Agreement?
  - Do you provide cybersecurity awareness training?
  - Do your enforce a vacation policy?
  - Do you have segregation of duties?
  - Do you continually assess who has access to data



# Use of Other Cybersecurity Tools

- ncase Enterprise/Forensic
    - Review system files
    - Deleted files
- anium
    - Application monitoring
    - Installed new applications
    - Disabled antivirus or other security software
- ofense (Phishme)
    - Do user click phishing emails
- ameware
    - Visually monitor employees

# If everything is important, nothing is

## YOU CANNOT WATCH EVERYONE ALL THE TIME

- Set priorities
- Use polices to strengthen your program
- Who has access to your data
- What do they do with it
- Why do they need access
- Who authorized their use of the data
- What are the data flows?
- Do they still need access?
- Focus on privileged Users
- Use Human Intelligence (HR, Legal, Tips)