Something is Better than Everything

*a distributed approach to audit log anomaly detection*

Presented by: Isis Rose, Nicholas Felts
Additional authors: Alexander George, Emily Miller, Max Planck

IEEE SecDev 2017
Hi!

Isis Rose
Mathematician
Research Scientist
obligate extravert

Nicholas Felts
Computer Scientist
Software Engineer
hat-wearer
This is a philosophy

- not a tool
- not a product
- not a service
- not selling a thing
Scope – what it is

• What are we talking about?
  • Measuring activities that span across:
    • Multiple users
    • Multiple machines
    • Multiple actions
  • Identifying and encoding scenarios of interest
  • Understanding that all data is not equally valuable
  • Making life easier for system administrators
Scope – what it isn’t

• What aren’t we talking about?
  • Seeing how many people mistyped a password today
  • Looking for anomalous behavior via machine learning
  • Looking for the unknown
  • A tool that solves all your problems all the time
  • Not a SIEM
there are a lot of logs

first thought: aggregate them!
the problem:
most of them don’t matter
write once (read never)

computation resources

personnel limitations

scaling analysis with increasing data

bandwidth limitations

massive quantities of information

there are many challenges

computation resources

there are many challenges

write once (read never)

computation resources

personnel limitations

scaling analysis with increasing data

bandwidth limitations

massive quantities of information

sysadmins expected to do security
endless data == perpetual analysis

looking at everything doesn’t scale
stop trying to do everything

at least not all at once
The process

A. Prioritize protection of critical assets
B. Identify scenarios of interest
C. Track actions of interest, not everything
D. Aggregate and correlate results
Benefits of this approach

• Detect defined events rapidly
• Conserve resources at scale
• Make junior analysts:
  • more effective
  • more quickly
  • more better
• Automation is your friend
Some caveats

• Only looking for known-knowns
  • never going to discover novel pathways

• Partial solution now is better than a perfect solution ‘someday’*

*something is better than everything
Know what to look for

one-time dissemination of targeting information

SME knowledge

actions of interest

...
I'm over big data. Where's some adorably smol data?
Move smol amounts of data

ongoing distributed collection & centralized alerting
We made a prototype
Actor B recruits Actor C

- Actor C has access
- Opens targeted files
- Lowers permissions
- Moves directory to shared drive
- Bundles with tar, renames
- Exfiltrates data with scp

Actor B

Actor C

locate

access

possess

exfil
Experiment design

• 3 insider exfiltration scenarios

• Implemented on operational network on honeytokens

• Detection team given no context
Detection

detection team
• Found 3 insiders
• Data exfiltrated
• Identified target data accurately

ground truth
• 3 insiders
• Data exfiltration
• Honeytoken data

one-click analysis
full context
The process

A. Prioritize protection of critical assets
B. Identify scenarios of interest
C. Track actions of interest, not everything
D. Aggregate and correlate results
sometimes something
really is better
than everything
Image Credits

• slide 3: ”The Thinker” by August Rodin. From https://www.famsf.org/blog/framework-thinker-rodin

• slide 4: “Tron” by Disney.

• slide 5: Swiss Army Knife by Wenger. From https://www.amazon.com/Wenger-16999-Swiss-Knife-Giant/dp/B001DZTJRQ

• slide 9: From https://elainesphilosophythoughts.wordpress.com/2016/02/16/the-hamster-wheel/


• slide 12: “Airplane!” by Paramount Pictures.