NOT IN MY HOUSE!

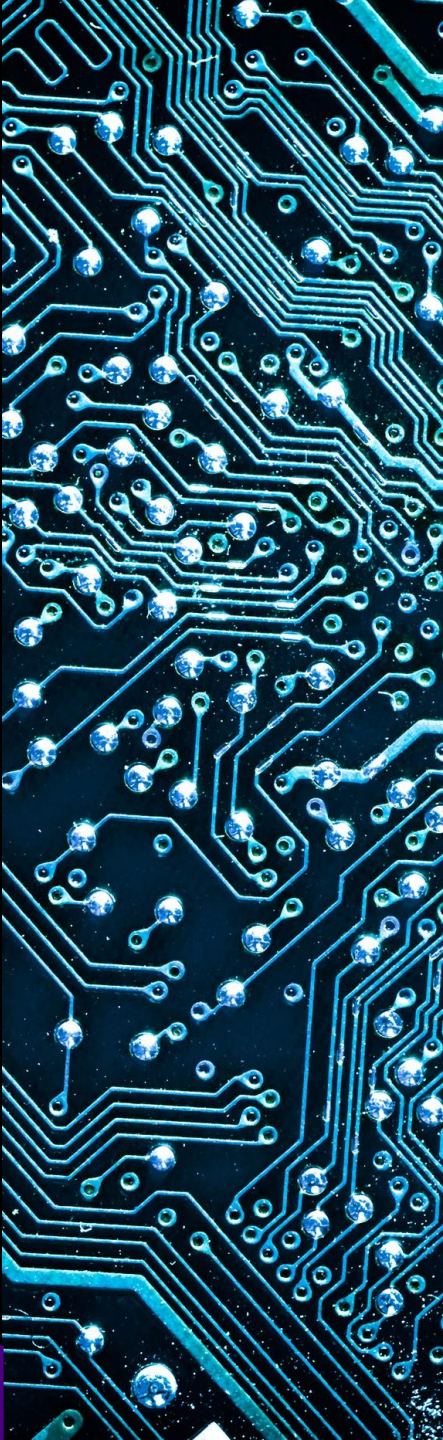
Layered alerting to drive detection time to zero

About Me

- Managing Partner of InfoSec Innovations
- Certified Instructor
  - SANS SEC 504
  - SANS SEC 555
- @BetterSafetyNet

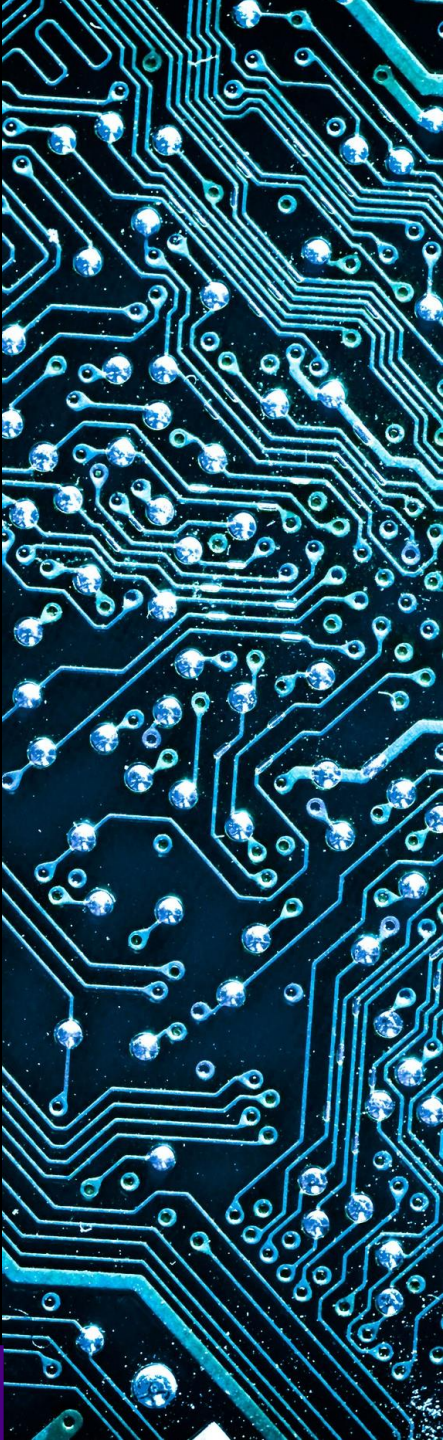
The InfoSec Innovations Motto

Better Information Security through; Science, Creativity, and Caring.



The InfoSec Innovations Motto

Better Information Security through; Science, Creativity, and Caring.



These slides are available at:

https://infosecinnovations.com/talks

Free download,
NO SIGN UP!

Too much to write?!
GET THE DECK!

Over abundance of clues

EVERYTHING generates clues

Three places to look

1) Network

Three places to look

1) Network
2) Memory

Three places to look

1) Network
2) Memory
3) Disk

It’s way more than that...

ATT&CK and Defend Matrix

Where you can *really* detect

Network Detections

- Firewall
- IDS/IPS
- Flow data
- Patch management
- Config management
- Log monitoring
- NAC

Host Detections

- NG-protections
- HIPS
- Anti-virus
- DLP
- Patch management
- Config management
- Log monitoring
- File integrity monitoring
- App whitelisting

Best return on effort?

Network Detections

- Firewall
- IDS/IPS
- Flow data
- Patch management
- Config management
- Log monitoring
- NAC

Host Detections

- NG-protections
- HIPS
- Anti-virus
- DLP
- Patch management
- Config management
- Log monitoring
- File integrity monitoring
- App whitelisting

Where do I start?

Start easy

What are you good at?

Are you OK at any of these? Start there!!

Network Detections

- Firewall
- IDS/IPS
- Flow data
- Patch management
- Config management
- Log monitoring
- NAC

Host Detections

- NG-protections
- HIPS
- Anti-virus
- DLP
- Patch management
- Config management
- Log monitoring
- File integrity monitoring
- App whitelisting

What do I do with this though?

DEMO!!

Our goal as defenders…

COMPLIANCE

REAL Security

These slides are available at:

https://infosecinnovations.com/talks

Free download,
NO SIGN UP!

Too much to write?!
GET THE DECK!