THIRD PARTY
THREAT HUNTING

COMPLIANCE IS FOUL

Get away from the checkbox stupor!

About the Speaker

Gregory Rasner, CISSP, CIPM, CCNA

Author "Cybersecurity & Third-Party Risk: Third-Party Threat Hunting" (Wiley, 2021)

"Zero Trust and Third-Party Risk: Reduce the Blast Radius"; (Wiley 2023). Technical Editor – Jerry Chapman; Forward by George FInney

Content Creator for "Third Party Cyber Risk Assessor" (TPCRA) training and certification from Third Party Risk Association

Host of Podcast "Third Party Threat Hunters"

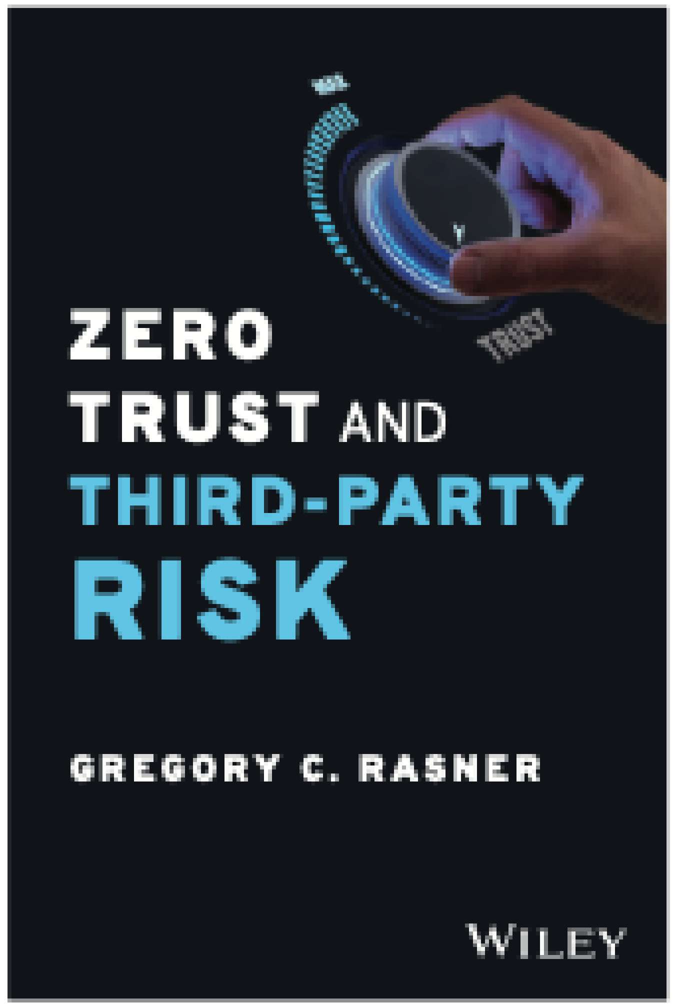
CEO at Third Party Threat Hunting LLC
greg@thirdpartythreathunting.com

GREGORY C. RASNER (ISC)²

CYBERSECURITY & THIRD-PARTY RISK

Third Party Threat Hunting

WILEY



ZERO TRUST AND THIRD-PARTY RISK

GREGORY C. RASNER

WILEY

THIRD PARTY THREAT HUNTING

THIRD PARTY CYBER RISK ASSESSOR CERTIFICATION TPRA

COMPLIANCE
IS NEEDED

- We need to track progress
- Regulators and LoDs use compliance
- Compliance artifacts are used in a variety of ways

COMPLIANCE
IS NOT RISK MANAGEMENT
AND NOT 'THE GOAL' IN CYBER

STRATEGY

WHAT IS IT?

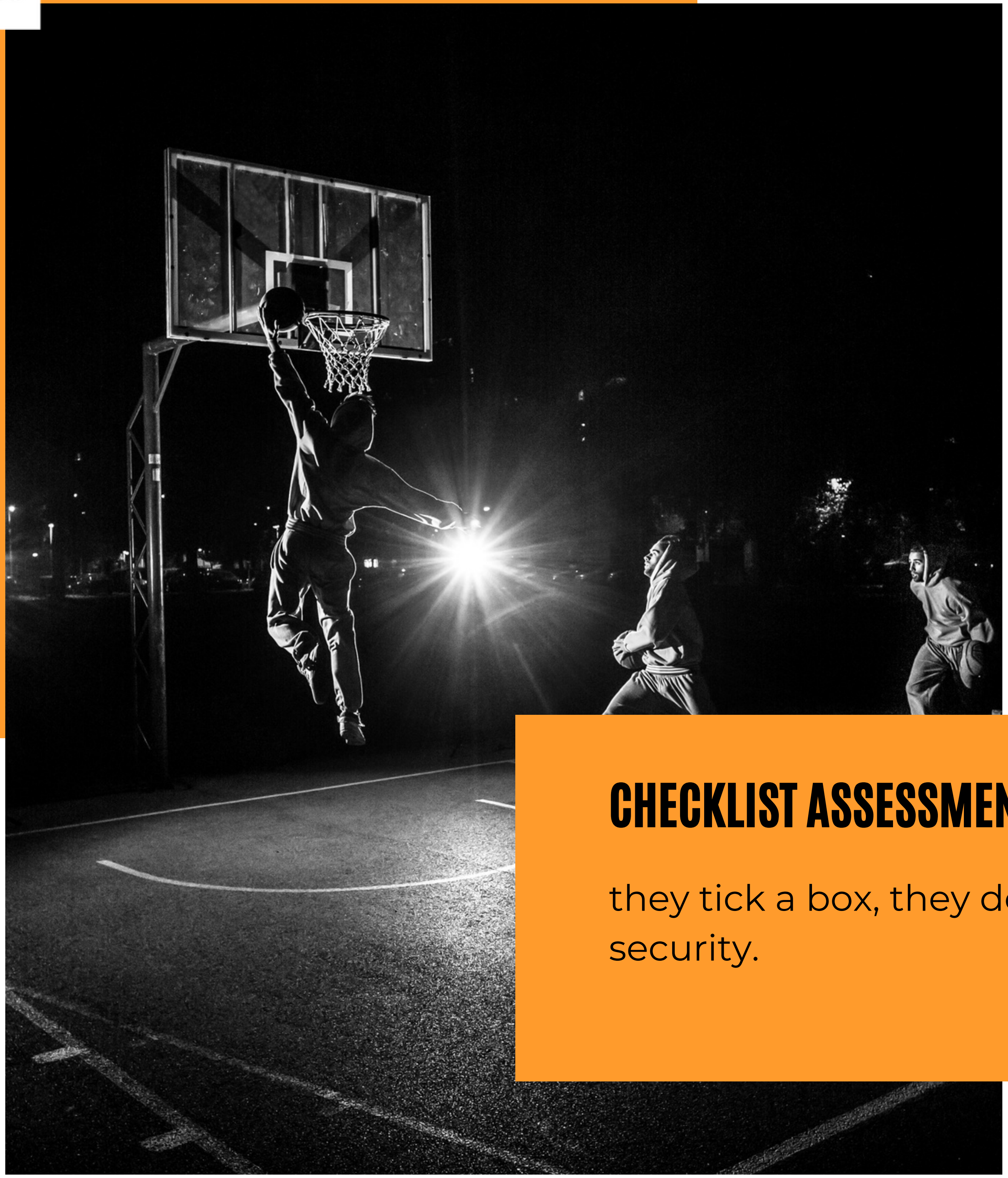
WHY IS IT IMPORTANT?

BUILD IT AND IT WILL COME
GREAT RISK MANAGEMENT

- Build a great cybersecurity program
- Support it and mature it with great risk management program and process
- Compliance will be a result of these, not the goal in and of itself

COMPLIANCE WILL BE AUTOMATED IN NEAR FUTURE

THIRD PARTY
THREAT HUNTING



HOW COULD I BE BREACHED?
I AM "COMPLIANT"...

Nearly every company ever breached had some 'clean' SOC2, ISO, or some other compliance approved. Don't confuse compliance with security.

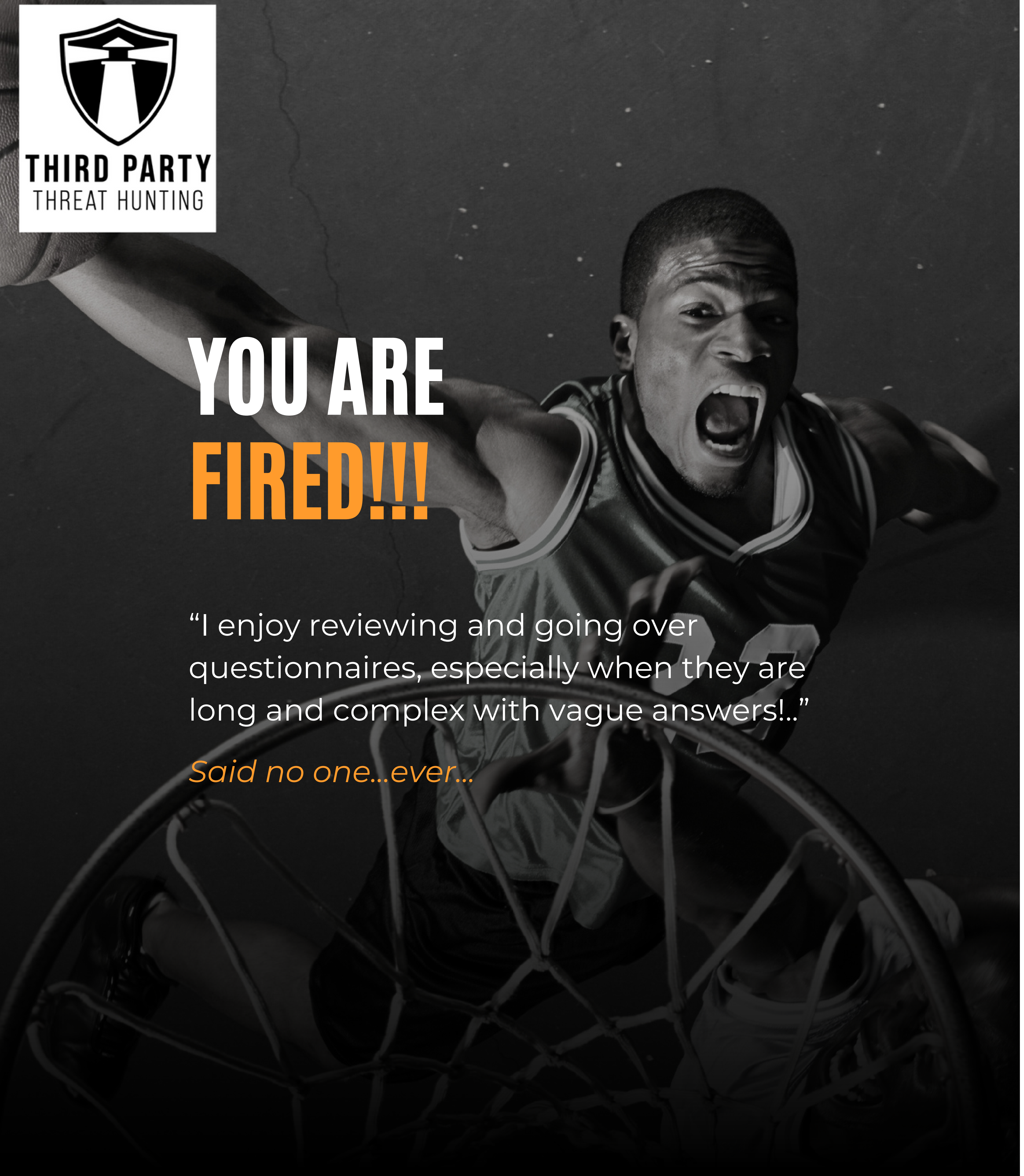
CHECKLIST ASSESSMENTS

they tick a box, they do not evaluate a vendor's security.

PHYSICAL VALIDATIONS

for your critical vendors, provide a level of assurance and a relationship with this vendor risk type that is invaluable.

THIRD PARTY
THREAT HUNTING



YOU ARE FIRED!!!

"I enjoy reviewing and going over questionnaires, especially when they are long and complex with vague answers!.."

Said no one...ever...

OLD SCHOOL

point-in-time assessments capture what happened or was done. Past tense, not what they are doing (or not) doing now

BENEFITS FROM AI/LLM AND ML

There is no better place where Artificial Intelligence, Large Language Models, and Machine Learning can be leveraged than in questionnairres

CONTINUOUS MONITORING UNLEASHED!

free your practitioner brains and firepower to focus on risk identification and reduction in real-time. Why focus on the past?

CORRELATION IS KEY

look to add other data sources, such as

- Threat Intel tools
- Security Info and Event Managemet (SIEM)
- Next-Gen Firewalls
- Data Loss Prevention (DLP)
- Keep going...charge for the net!

THIRD PARTY
THREAT HUNTING

CONTINUOUS MONITORING TEAM

26

INTERNAL SYSTEMS

Defender

18

PRACTITIONERS

Team Captain

09

VENDOR RISK TOOLS

Playmaker

THIRD PARTY
THREAT HUNTING

TEAMWORK - DATA LAKE

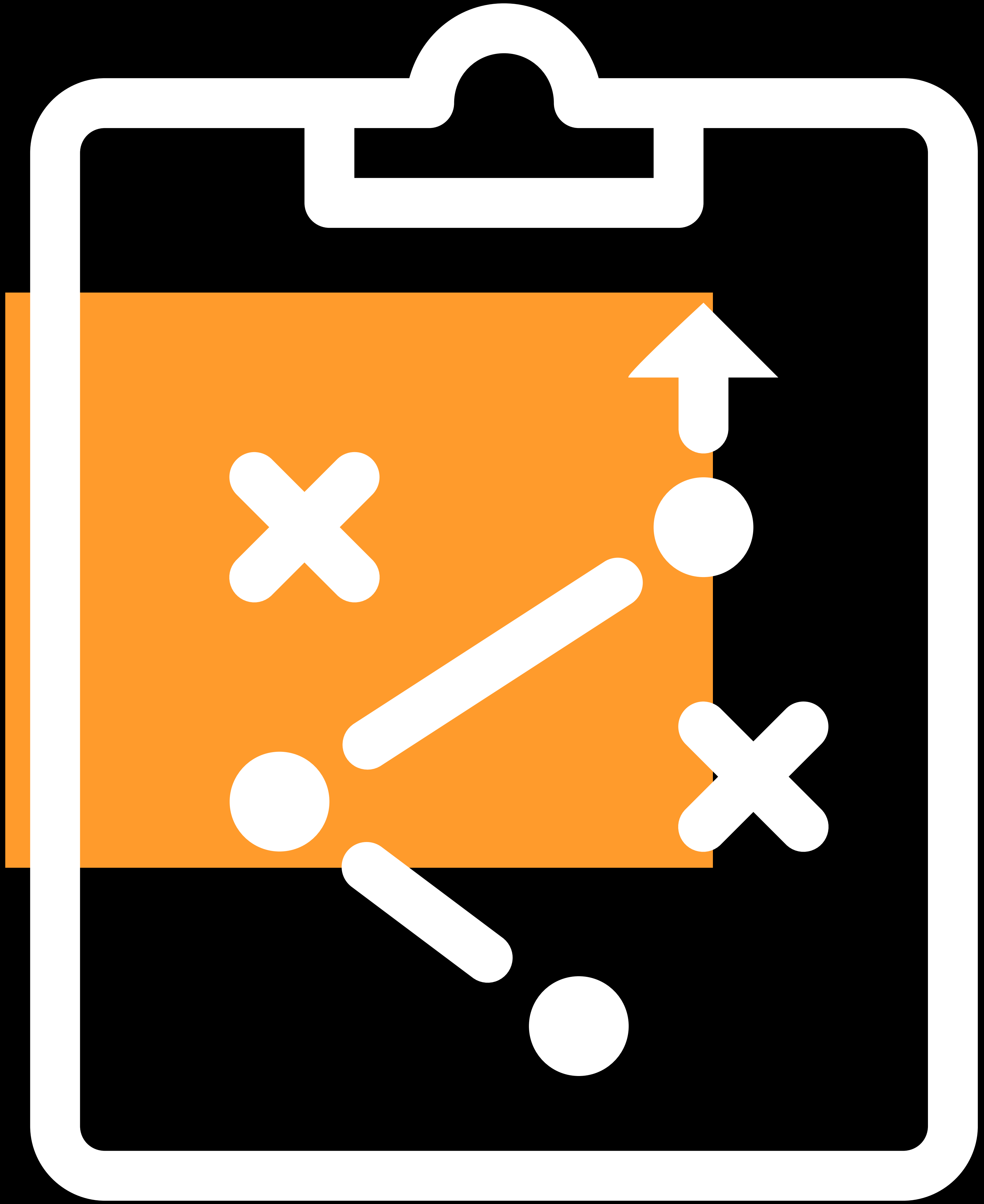
Bring all these teammates together in a data lake (or data pond, if that is all you can get) and start looking for correlations and patterns.

CONTINUOUS MONITORING
SLAM DUNK

Easier reporting and escalations make this a 3-pointer strategy every time.

CONTINUOUS MONITORING STRATEGY

- Data Feeds
- Data Sources
- Weights and Algorithm
- Evaluate Risk (Risk-Based)
- Inform Vendor of specific threat/vulnerability
- Follow-up based upon risk and date-driven
- Update System of Record



THIRD PARTY
THREAT HUNTING

THANK YOU.