PROTECTWISE™

BUILDING A THREAT HUNTING PRACTICE IN THE CLOUD

March 22, 2017

TODAY'S SPEAKERS

James Condon
Director of Threat Research and Analysis
ProtectWise

Tom Hegel
Senior Threat Researcher
ProtectWise

TODAY'S AGENDA

- Threat Hunting 101
- Requirements for Effective Threat Hunting
- How the Cloud Can Help
- Threat Hunting Best Practices
- Questions
- Next Steps

THREAT HUNTING 101

Following anomalous behavior when or where it occurs to confirm whether it was an actual, active attack.

Detection

Catch and respond to known threats.

vs.

Hunting

Identify detection gaps and unknown threats. Prevent future incidents.

WHY HUNT FOR THREATS?

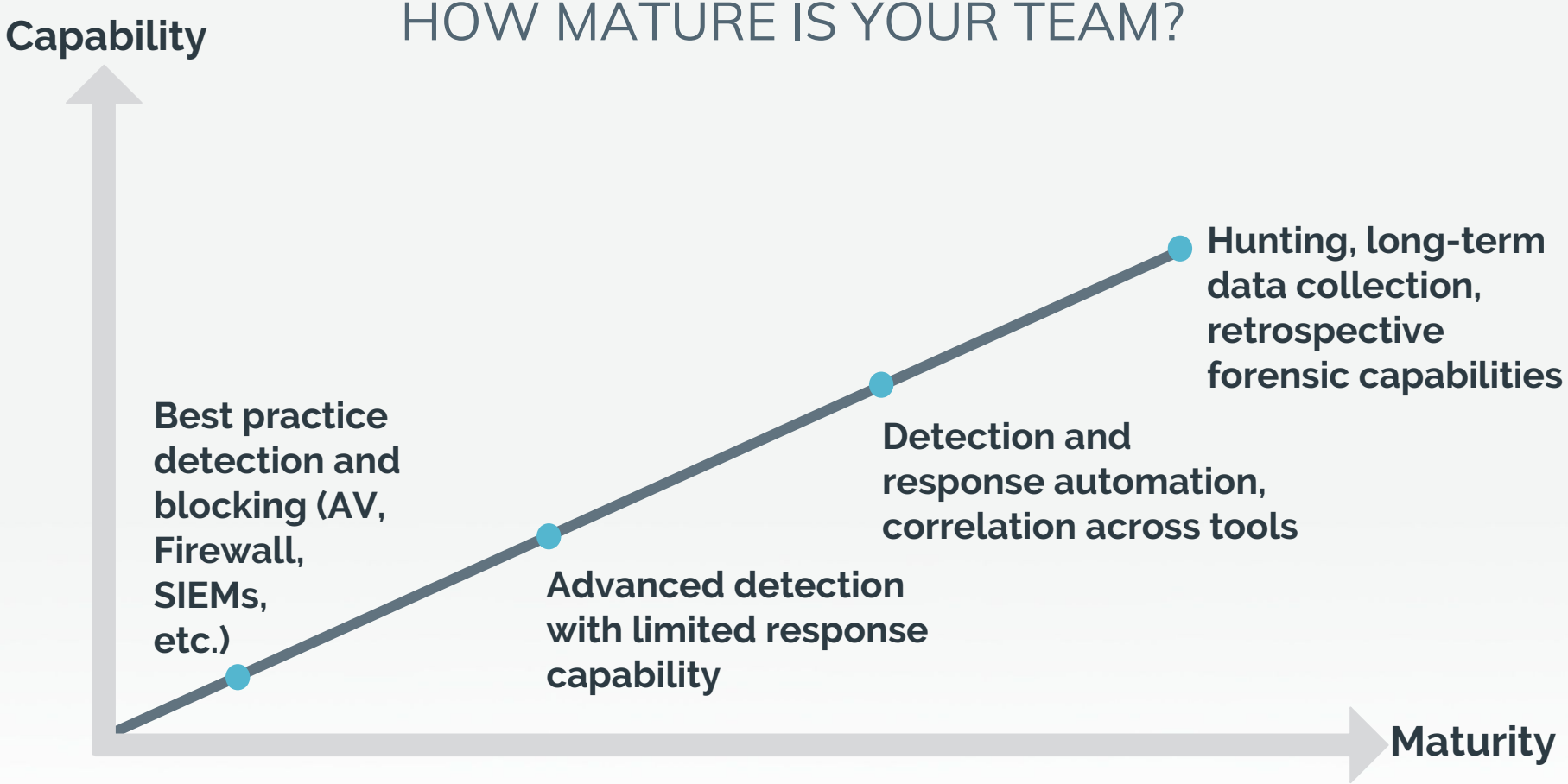
Be More Proactive

Catch What is Unknown and New

Increased Team Skill, More Fun

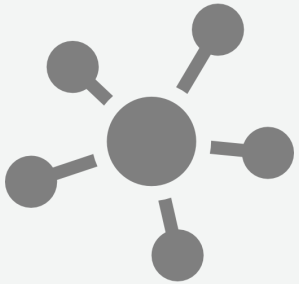
POLL QUESTION

HOW MATURE IS YOUR TEAM?

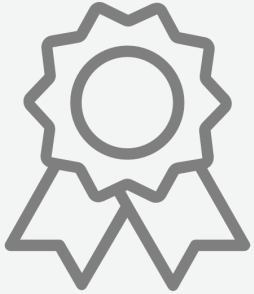


BEFORE YOU BEGIN

Master Detection and Response



Correlate Activity Between Tools



Detect on Quality Over Quantity

Automate As Much As Possible

REQUIREMENTS FOR EFFECTIVE THREAT HUNTING

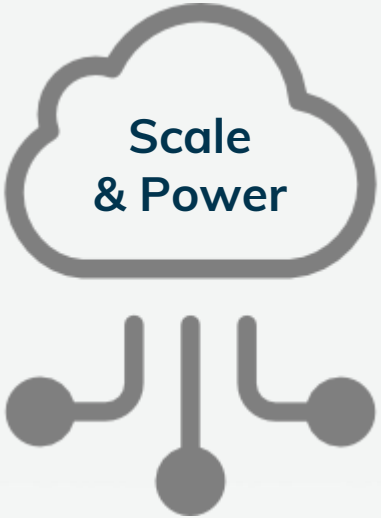
Collect the Right Data

Understand the Landscape

1. **Capture**
2. **Store**
3. **Extract**
4. **Index**
5. **Search**

POLL QUESTION

HOW THE CLOUD CAN HELP



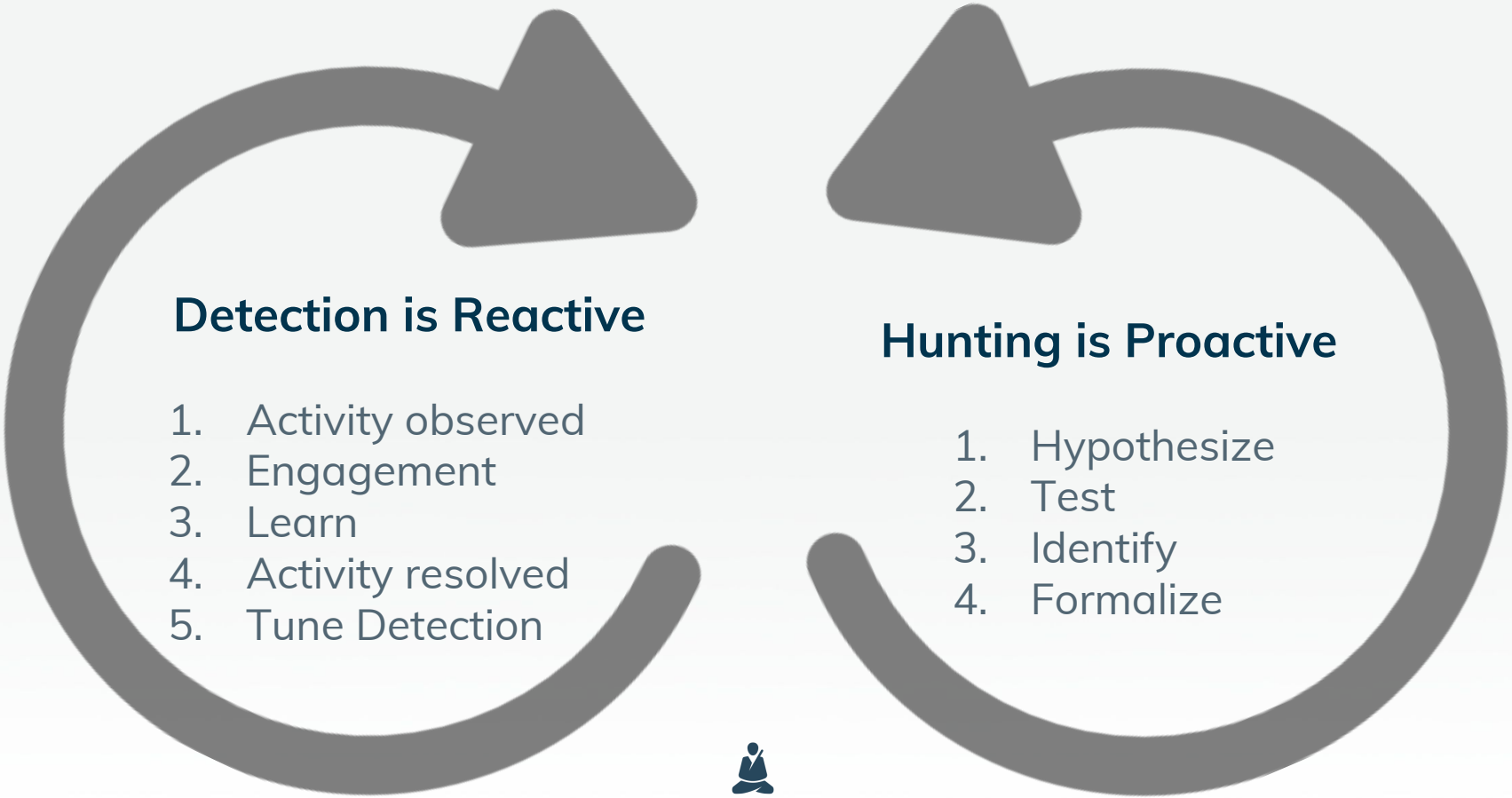
What does it give you?

- Unlimited storage
- Advanced analytics capabilities
- Unified haystack

What do you get?

- Comprehensive context
- Continuous analysis
- Pervasive visibility

DETECTION VS. HUNTING LOOPS



THREAT HUNTING BEST PRACTICES

- Foster an investigative mindset
- Develop and pursue leads
- Gather evidence
- Keep asking questions
- Avoid confirmation bias
- Avoid tunnel vision

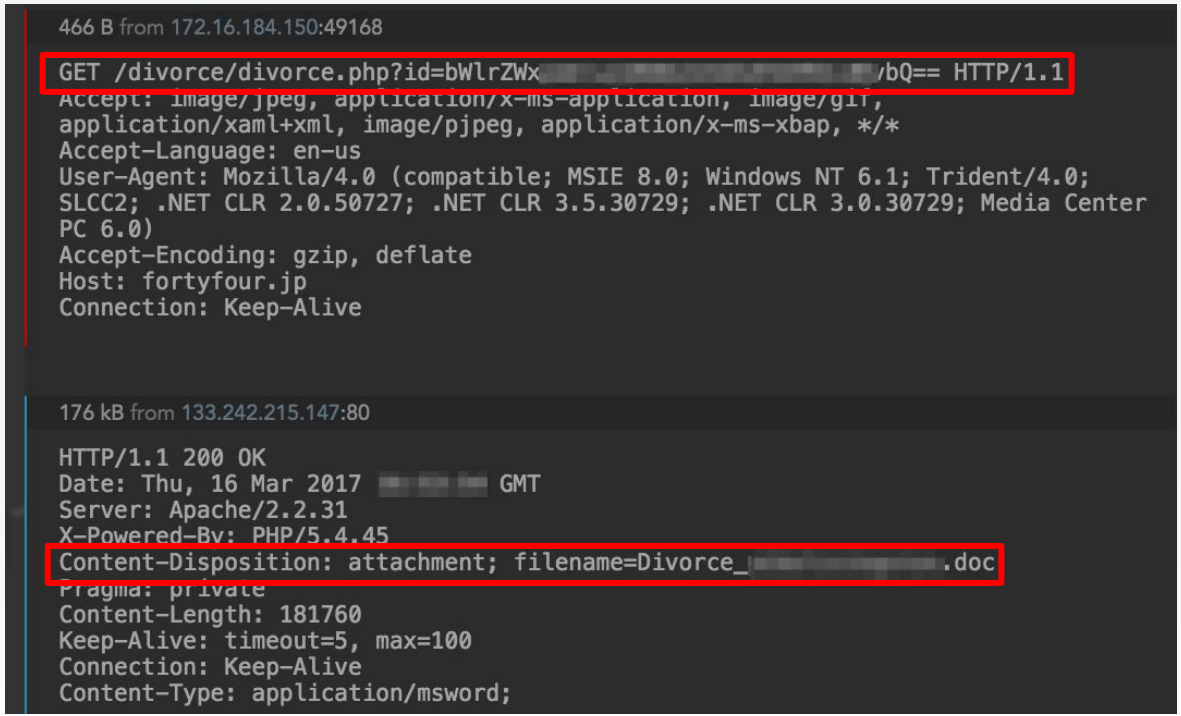
THE REALITY OF HUNTING AT SCALE

- Not always about an APT
- Embrace the analyst mindset
- Expand your knowledge
- Share and grow together
- Look beyond InfoSec rockstars

MALICIOUS HTTP REQUEST EXAMPLES

Differences between malicious & legitimate HTTP requests

- Small number of headers
- Headers out of order
- Unusual or small User-Agents



QUICK RECAP

A great threat hunting practice...

- ... acts **proactively** (hunting), not reactively (detection).
- ... collects the **right data**, and know your **landscape**
- ... relies on the **cloud** for **scalability and power** you need.
- ... follows **best practices**, they make you more **effective**.
- ... is **realistic** about outcomes and results.

PROTECTWISE™

Q&A

NEXT STEPS

- We'll be sending you a copy of our whitepaper "*A Comprehensive Start-Up Guide for Proactive Threat Hunting Across Time.*"
- Questions? Email sales@protectwise.com

PROTECTWISE™

THANK YOU

www.protectwise.com