RAPID7

A Risk Management Platform

Are You Ready For Compromised?

Michael Lai

CISSP, CISA, MBA, MSc, BEng(hons)

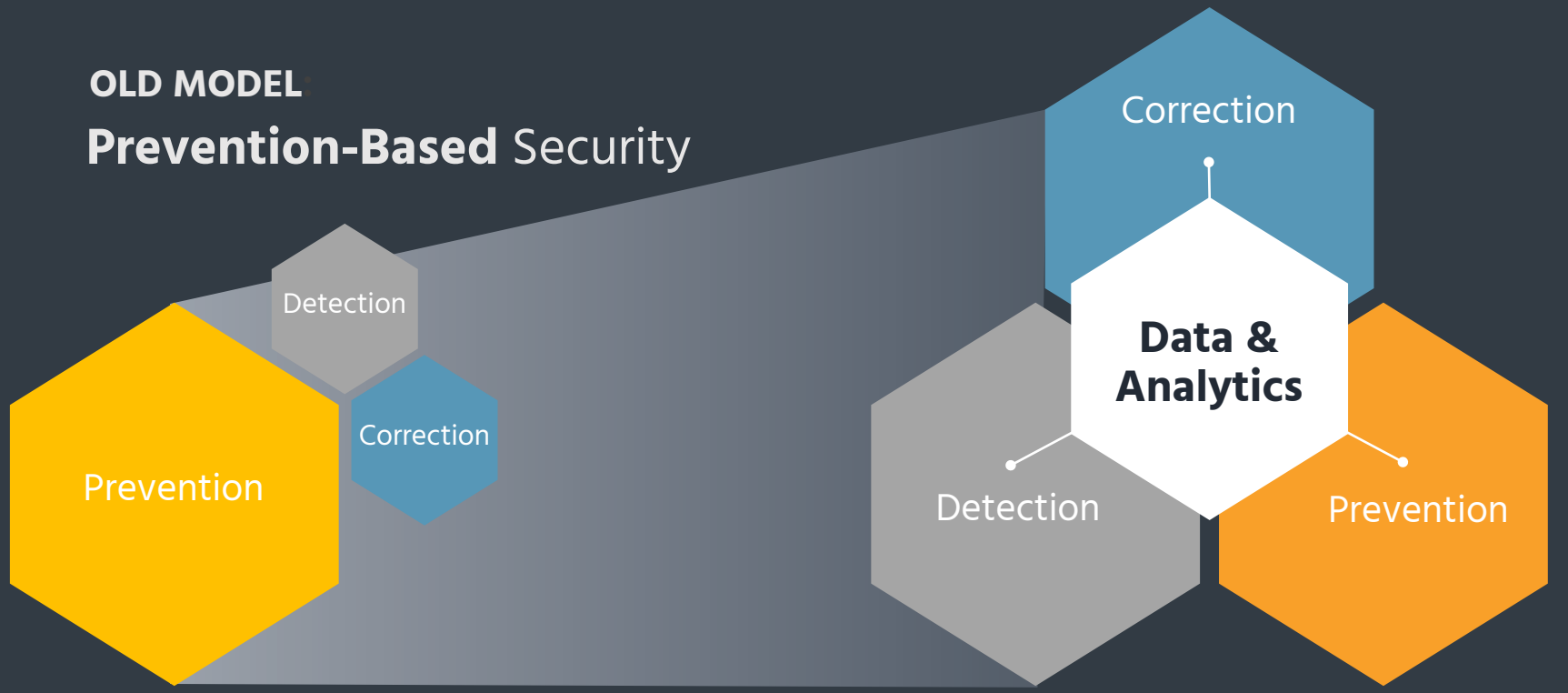
Territory Manager & Senior Security Sales Engineer


RAPID7
Gain the clarity, confidence, and confidence to embrace innovation and drive your business forward. Rapid7 transforms your data and uncertainty into answers.
Rapid7's mission is to lead the emerging SecOps movement with our multi-product analytics and automation cloud and expertise.

Shift to Risk-Based Security

OLD MODEL
Prevention-Based Security

NEW MODEL:
Risk-Based Security



By 2020,

60%

of enterprise information security budgets will be allocated for **rapid detection and response approaches.**

- *Gartner: "Shift Cybersecurity Investment to Detection," dated 7 January 2016*

RAPID7

Solve Critical Security & IT Questions

Am I Vulnerable?	Am I Compromised?	Am I Optimized?
Threat Exposure Management	Incident Detection & Response	Log Management & IT Analytics
VULNERABILITY MANAGEMENT	USER BEHAVIOR ANALYTICS	Orchestration & Automation
APPLICATION SECURITY TESTING	INCIDENT DETECTION & RESPONSE	INFRASTRUCTURE MONITORING & TROUBLESHOOTING
ATTACK SIMULATION	ENDPOINT VISIBILITY & INTERROGATION	LOG MANAGEMENT & COMPLIANCE

Software + Managed Services

Every Day Problem

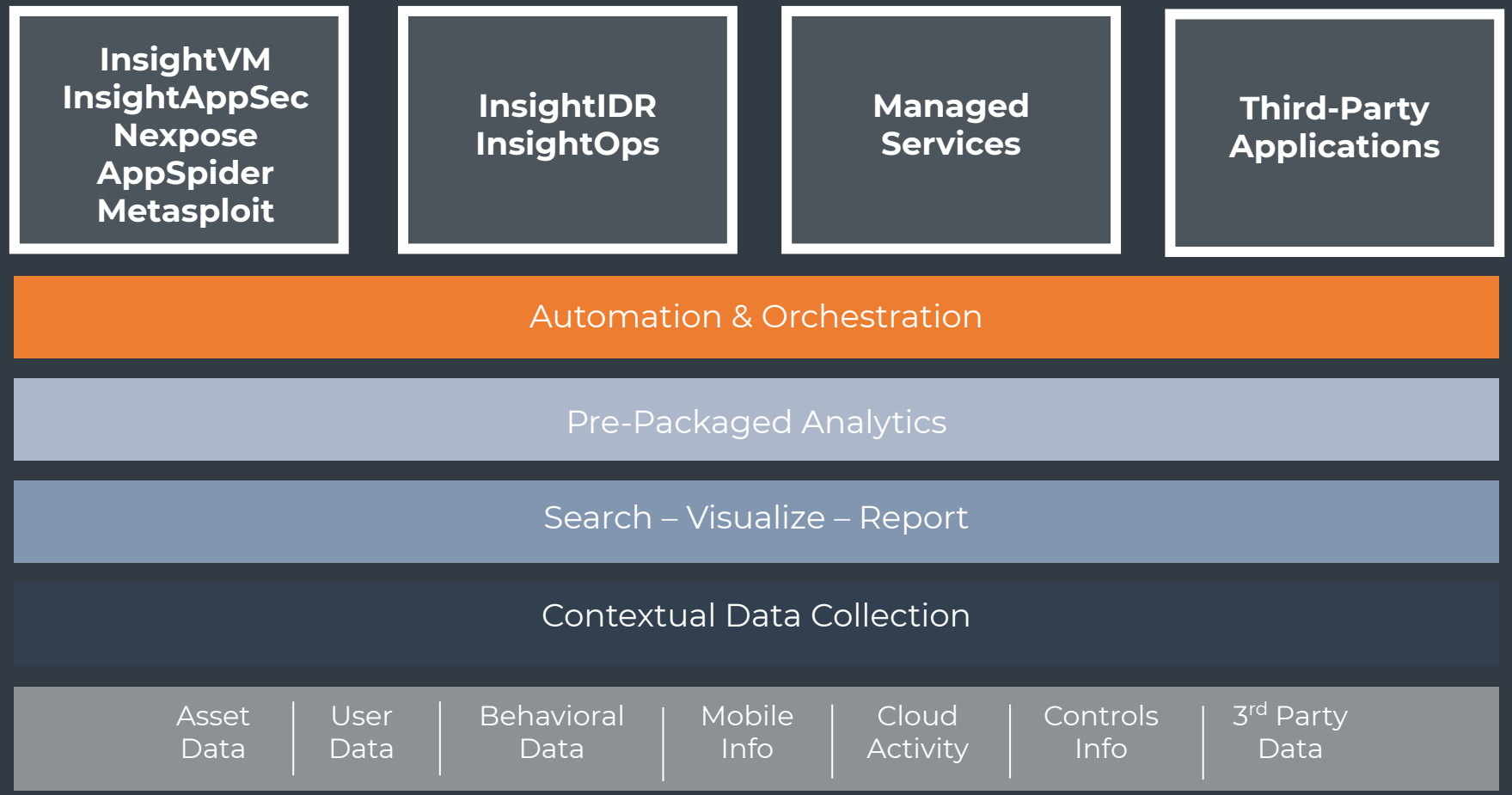
A company in HK have 17 people in security team and 8000 assets. Although SIEM has been deployed, they have difficulty to collect and consolidate data from 40-50 points solution data together.

A HK subsidiary wants to make himself ready before the audit by the the HQ in French. They have difficulty to collect the system information such as patch applied, software installed, etc ...

A bank in East Asia has SEIM deployed and employed big4 for annual PT but still breached. R7 PT team was on-site and collected lot of critical data but none alert from SIEM. Large part of SOC team was fired.

RAPID7

Security Automation & Orchestration Opportunity



Rapid7 Managed:

- Managed Detection and Response
- Managed Vulnerability Management
- Managed Application Security

Rapid7 Consulting:

- Penetration Testing
- Security Maturity Assessment
- Program Development & Benchmarking
- Threat Modeling
- Incident Response
- IoT Strategy and Testing

RAPID7

COLLECT

Consideration

1. What to collect? E.g. Asset data, system log, threat intelligence
2. How to collect? E.g. Scanner, syslog, agent, external party
3. Who to collect? E.g. IT security team, asset owner
4. When to collect? Schedule, manual, event trigger, blackout

What Question Is Answered

RAPID7

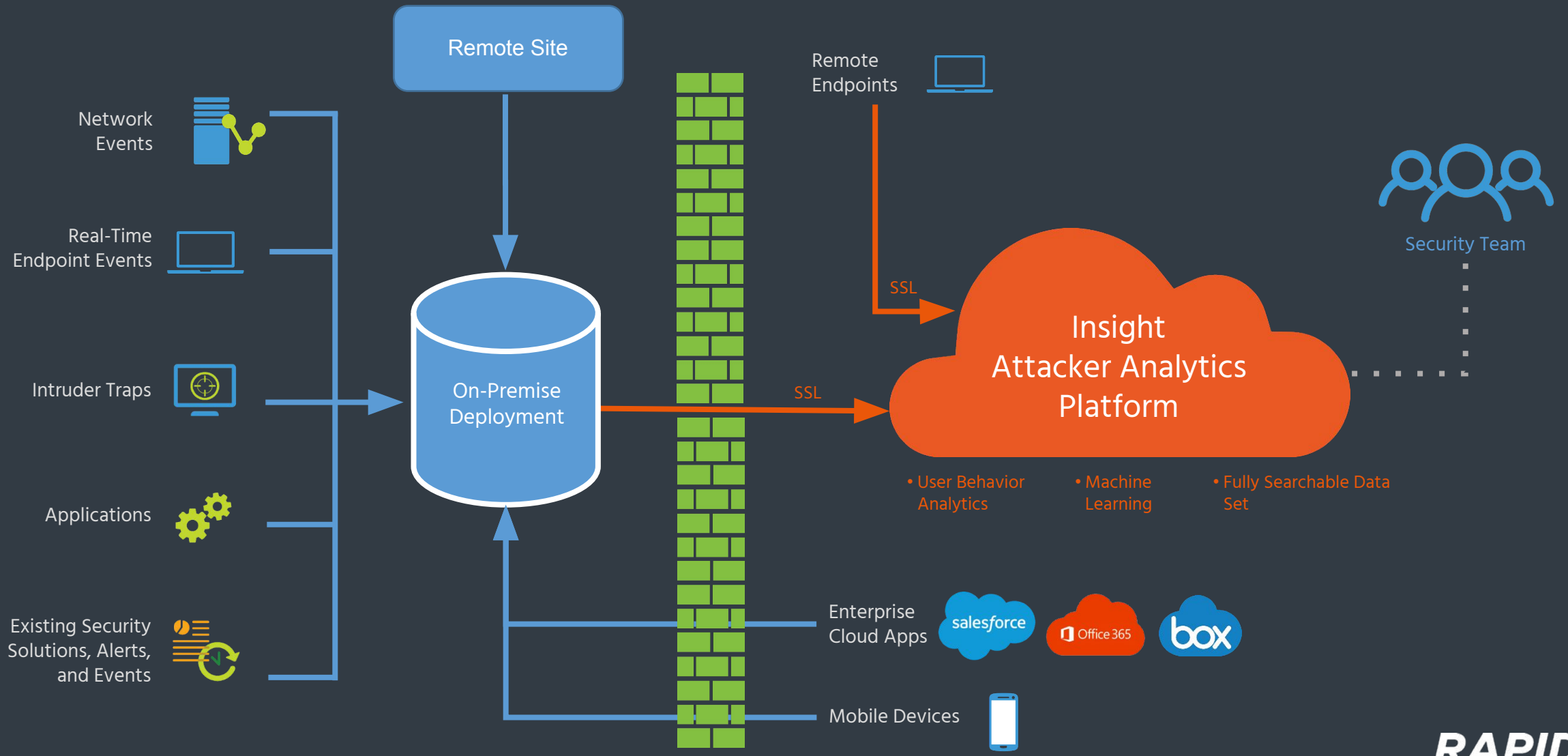
COLLECT

1. Deploy an infrastructure to collect from end point to cloud
2. Feed with external threat intelligence (exploit database)
3. Asset ownership grouping
4. Integration with other system (e.g. for authentication)
5. Testing data (in-house penetration test, 3rd social engineering test)
6. Activity baseline

A customer in HK spent 2 weeks to located hosts out of a few hundred which has WannaCry by checking the applied MS Patch

RAPID7

Solution Architecture



RAPID7

ANALYSIS

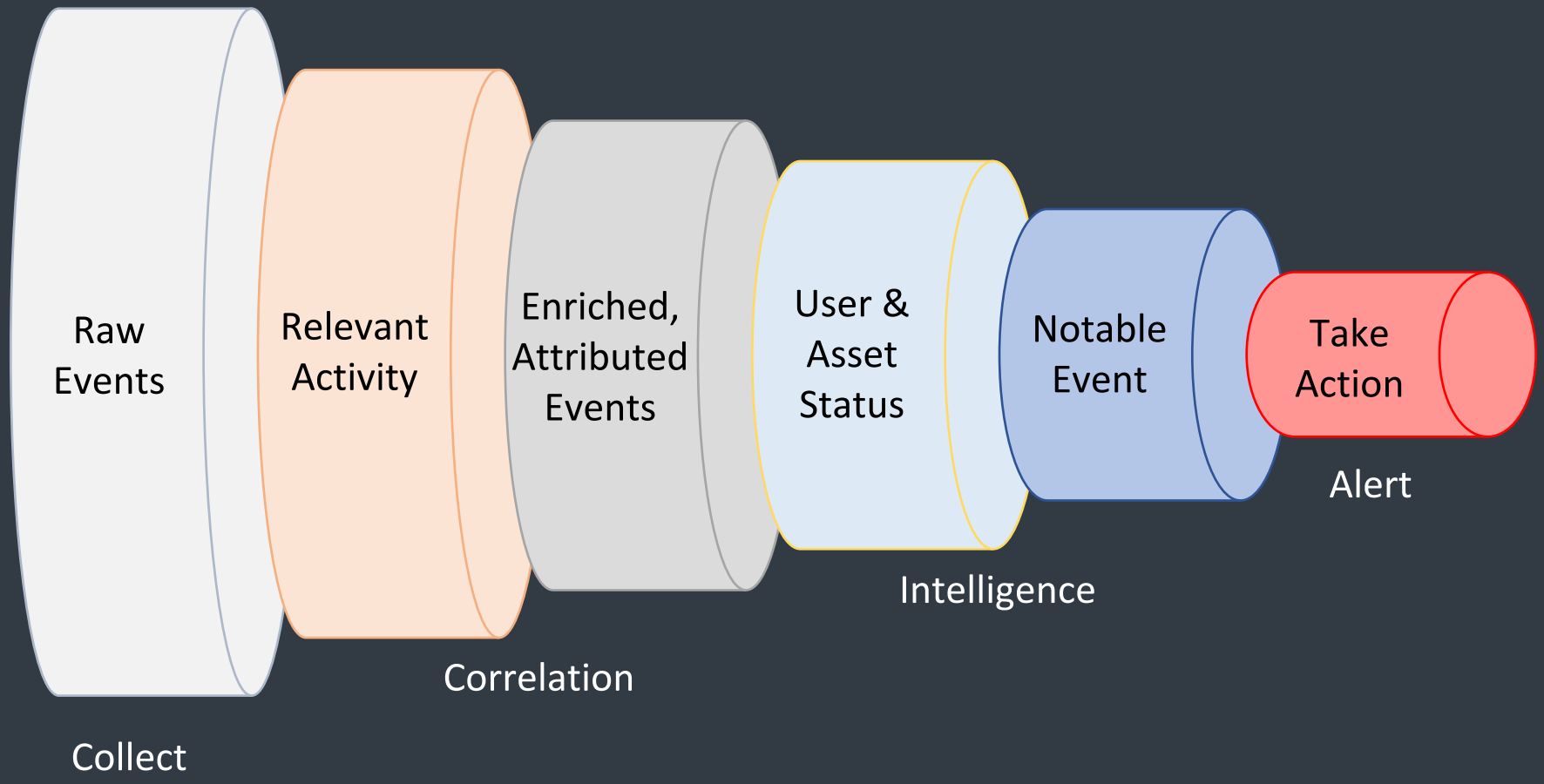
Consideration

1. What is log, event (e.g. a virus detected) and alert (take action)?
2. Who to analyze? In-house team, outsourced,
3. How to analyze? Self learning (e.g. Dr. Watson), manual built IF-THEN rule.

Ready for Any Question

RAPID7

Convert Data To Action



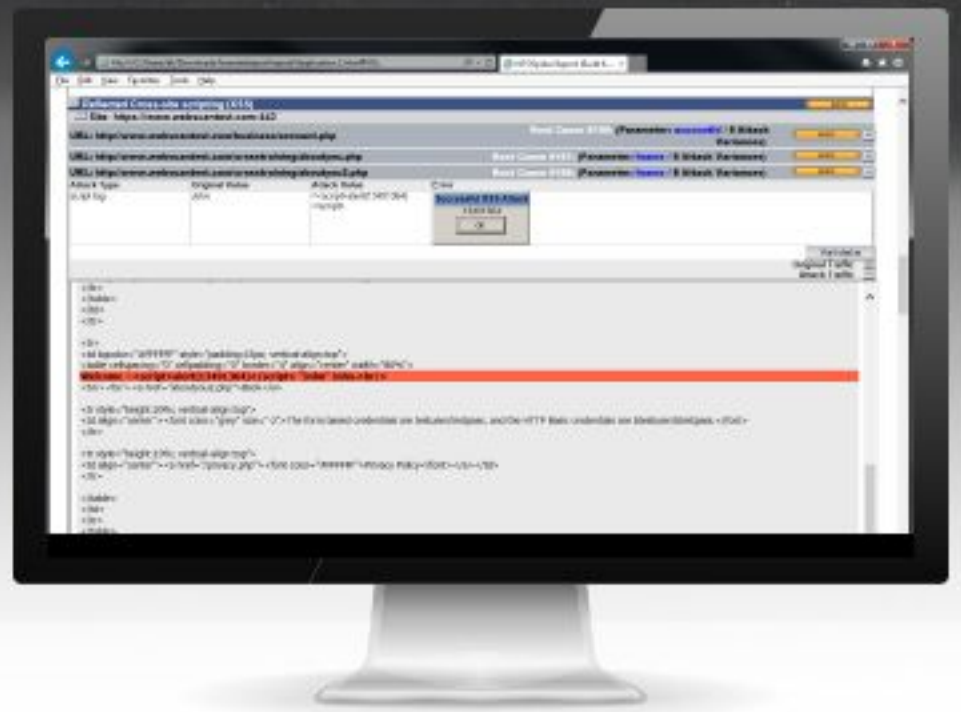
ANALYSIS

1. Build a team or an army (security data science expert)
2. Automation
3. Ability to correlate data and information recursively
4. Continuous improvement (self learning, reduce false +ve/-ve)

Hidden Figures (2016)

A few years ago, a world wide Japanese company was breached and the manager asked the "security team" to analyze the system log files with editor manually.

ANSWER



Consideration

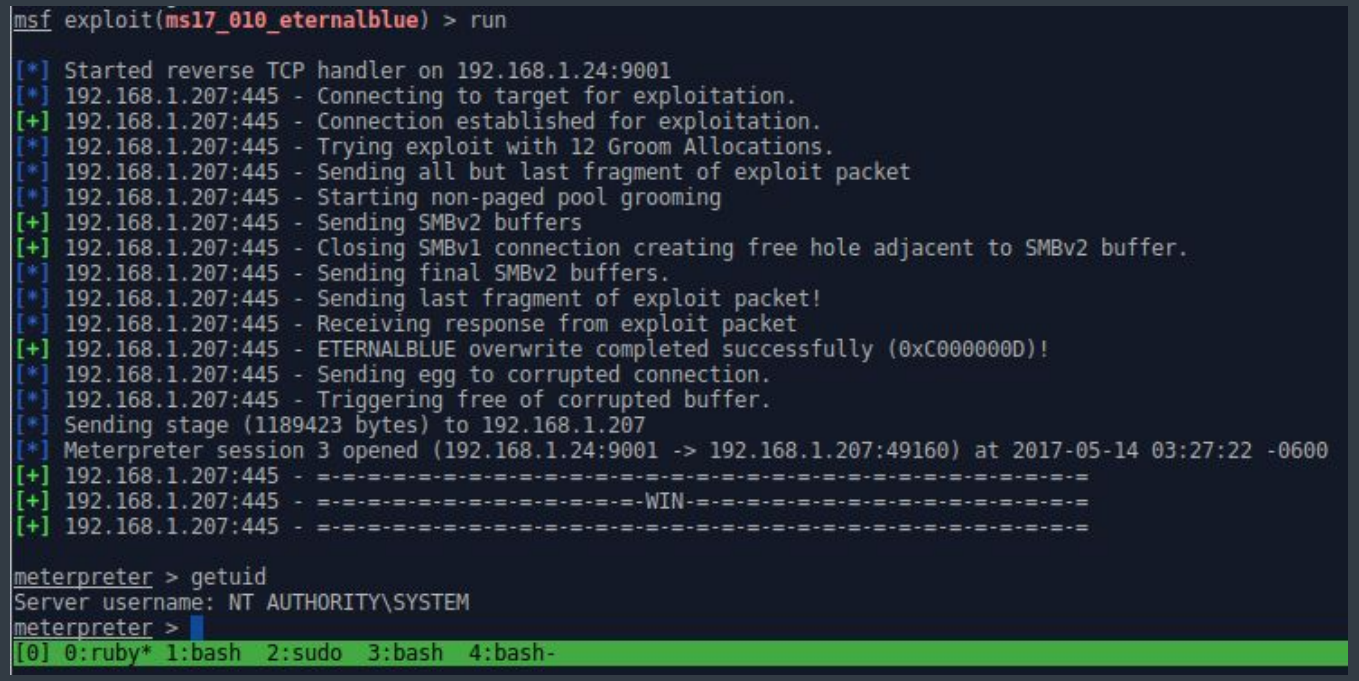
1. When the answer is ready? (Ad hoc, schedule)
2. Who will raise the question? (Asset owner, CSO)
3. What the question will be?
4. How to remediate?

Give the Right Answer

RAPID7

ANSWER

1. Agility to any question from all parties
2. Prioritized event and action
3. Feed to system for tuning (minimize the false +ve/-ve)
4. Minimize effort to get the answer and take remediation
5. Integration with other system (e.g. for automation, sharing with other)



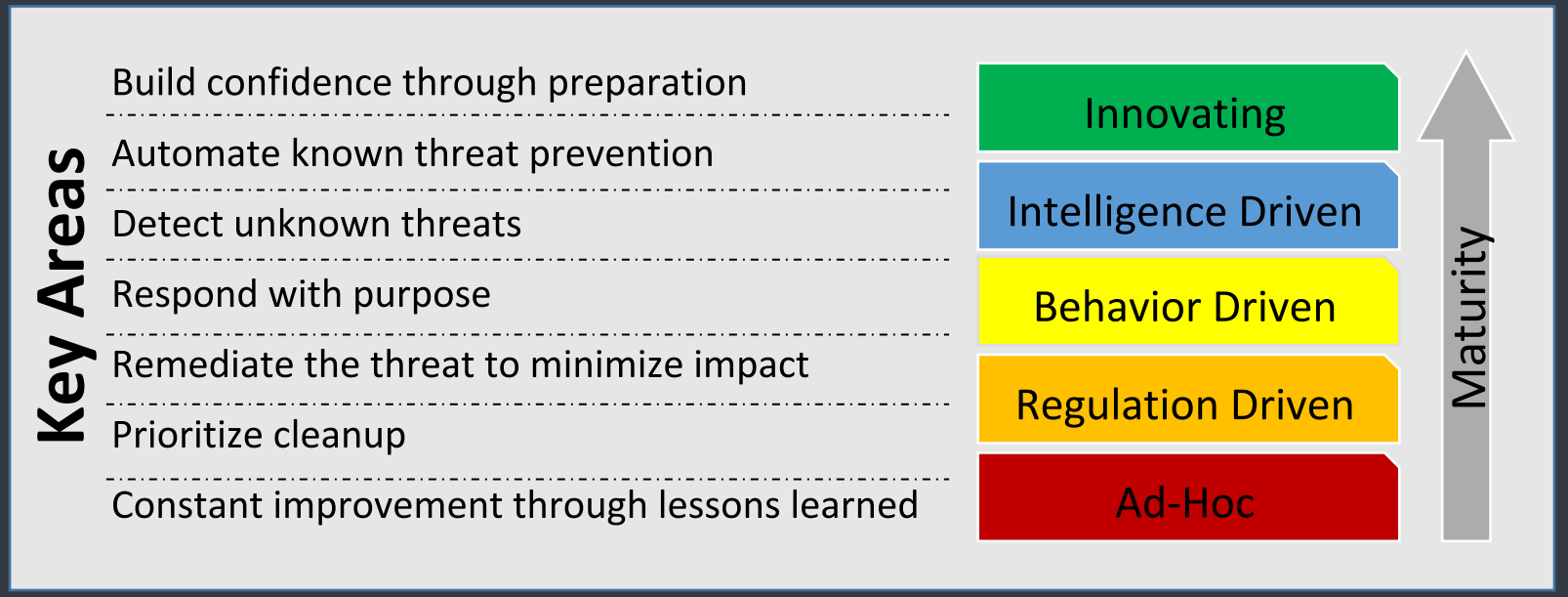
A University in HK centralized the risk management from all faculty. The CSO can get the risk intelligence of any faculty, group or asset handily.

RAPID7

NEXT STEP

How It Goes

1. Can everyone get the required information?
2. What is the workload to have the information?
3. How accurate is the information?
4. How can you response to a risk or breach?
5. Can you predict where the hacker will get in?



Many SIEM/SOC deployed but do not know how good it is.

RAPID7

INCIDENT READINESS ASSESSMENT

Threat detection and incident response evaluation. Increases response efficiency and effectiveness. For example, playbook for following a critical vulnerability announcement (e.g. WannaCry) or APT.

Detection Ability (Identify risk or breach)

Documentation (playbook, reporting)

Follow Up Procedures (remediation, scoping)

TABLETOP EXERCISES

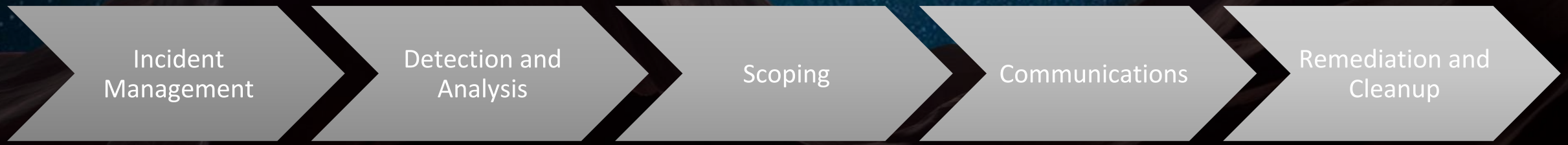
Threat simulation exercise, aimed at evaluating the ability to effectively detect and respond to incidents. To ensure that the READINESS is working.

Initiate	Prepare	Deliver	Recommend
•Project Scoping •Discovery • Threat Scenario • Existing Capabilities	•Full Threat Scenario •Threat Guide •Evaluator Guide •Coordination	• Execute Exercise • Analyze Findings, Feedback, and Evaluator Forms	• Report Delivery • List Recommended Improvements in IDR Program

RAPID7

BREACH RESPONSE

Usually employ 3rd party to raise a PT and audit the risk platform. Will not notify anyone about the maneuver unless required.



THANK YOU