RSAConference2015
Singapore | 22-24 July | Marina Bay Sands

CHANGE
Challenge today's security thinking

SESSION ID: SPO-R01

‘They will get in’
Detect and Respond to Advanced Threats via Security Intelligence

A Reference Model for IT Security Practitioners

Bill Taylor

General Manager APAC
LogRhythm Pte Ltd
@LogRhythm

LogRhythm™
The Security Intelligence Company

#RSAC

The Expanding Cyber Threat Motive

Political

Ideological

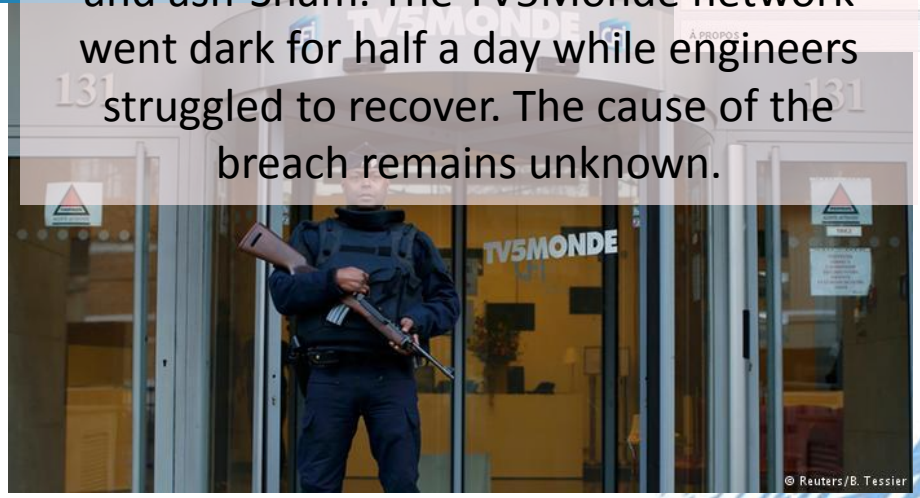
Criminal

LogRhythm™
The Security Intelligence Company

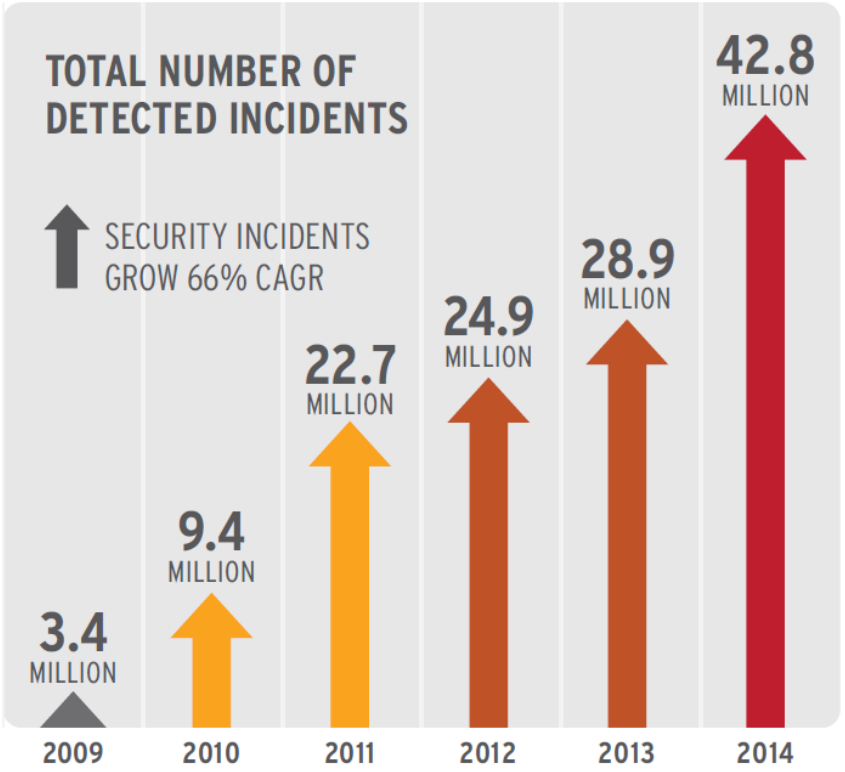
A Dramatic Change in Severity levels

TV5MONDE

The unknown hackers who penetrated TV5Monde used the compromised social networking accounts to post slogans and images in favor of the Islamic State of Iraq and ash-Sham. The TV5Monde network went dark for half a day while engineers struggled to recover. The cause of the breach remains unknown.



Ever Increasing Cyber Risk

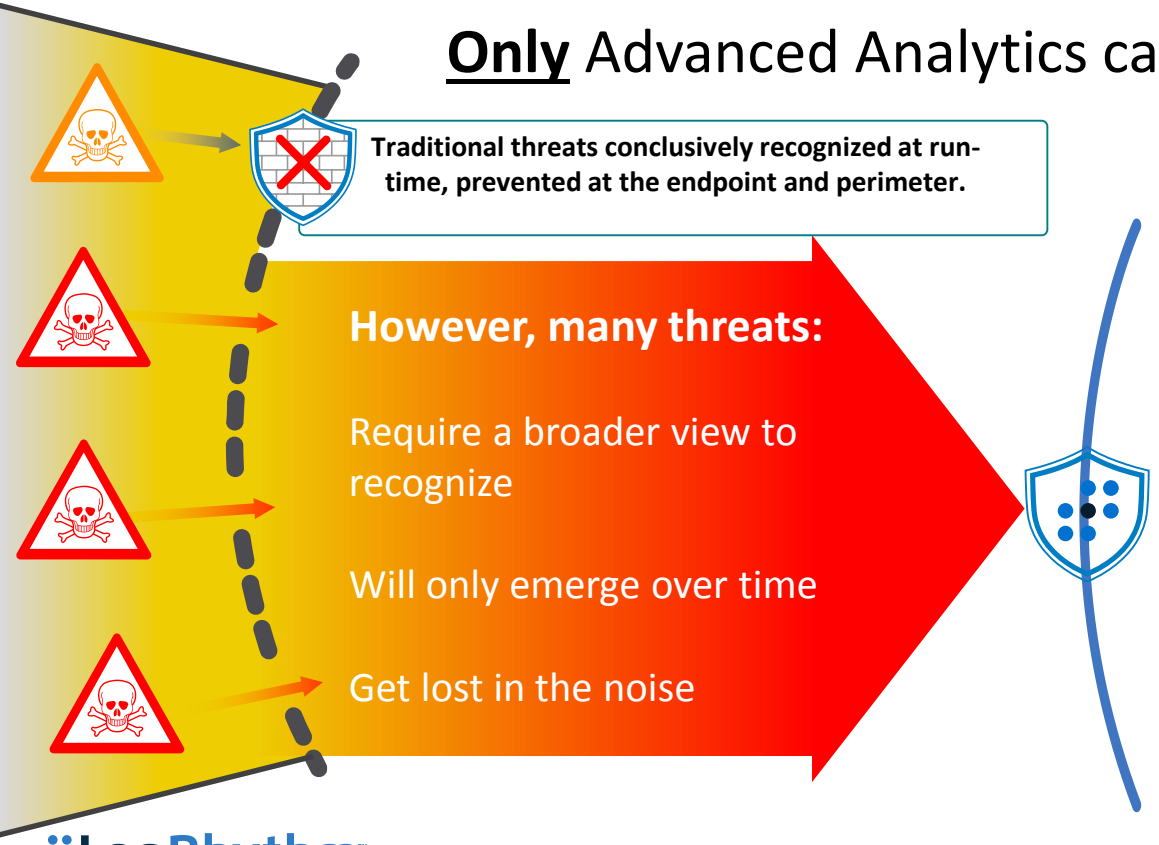


Source: PwC, The Global State of Information Security Survey 2015

ADVANCED THREAT / APT DETECTION
DATA EXFILTRATION
COMPROMISED HOSTS
INAPPROPRIATE NETWORK USE
FRAUD
INSIDER THREATS
COMPROMISED ACCOUNTS
COMPROMISED HOSTS
COMPROMISED CREDENTIALS
NETWORK MISUSE
COMPLIANCE VIOLATIONS
STATE-SPONSORED ATTACKS

Today's Threat Environment is different..

Only Advanced Analytics can detect these threats



Traditional threats conclusively recognized at run-time, prevented at the endpoint and perimeter.

However, many threats:

Require a broader view to recognize

Will only emerge over time

Get lost in the noise

Detecting a class of threats only a Big Data, Machine Analytics based approach can realize

Effectively prioritizing threats, separating the signal from the noise

Providing the intelligence required to deliver optimally orchestrated and enabled incident response

Prevention is Futile

“Advanced targeted attacks make prevention-centric strategies obsolete. Securing enterprises in 2020 will require a shift to information and people-centric security strategies, combined with pervasive internal monitoring and sharing of security intelligence.”

“By 2020, 60% of enterprise information security budgets will be allocated for rapid detection and response approaches up from less than 10% in 2013.”

- *Neil MacDonald*

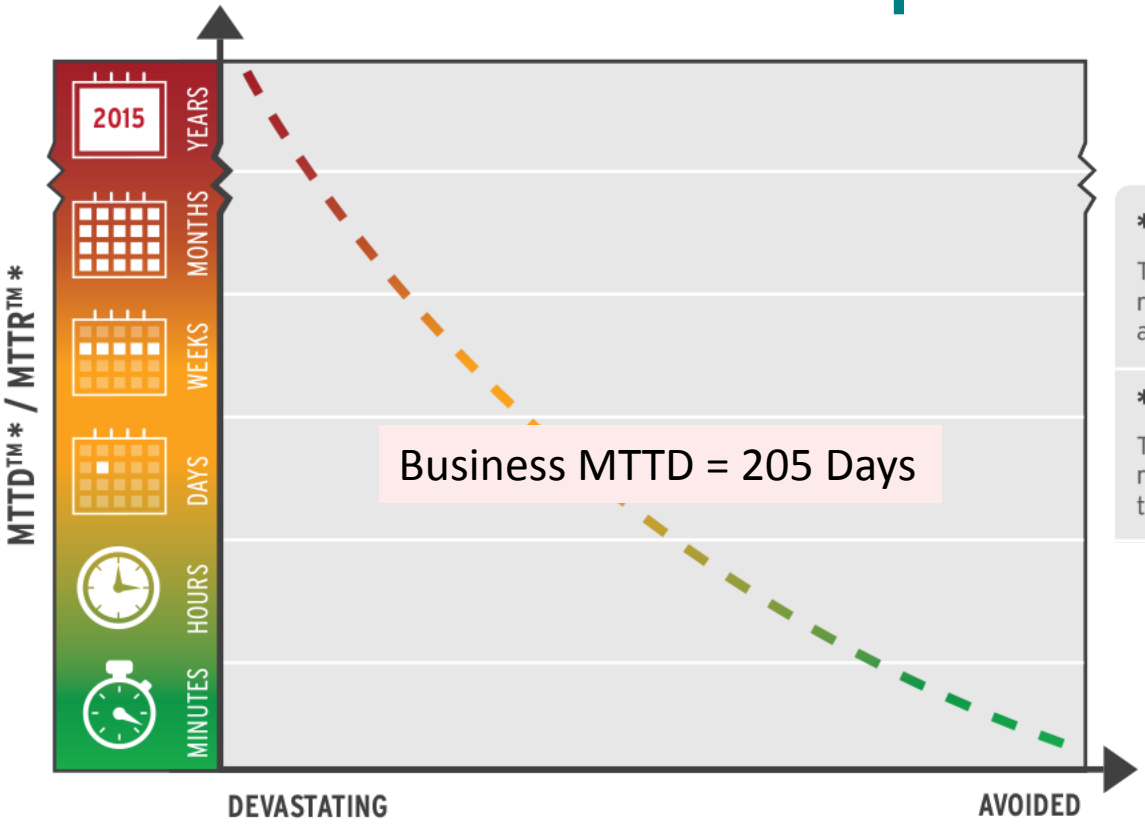
Gartner

A Security Intelligence Driven Approach is Required

The cost of mitigating a threat, and risk to the business, rise exponentially across the lifecycle of a threat from inception to mission attainment.

Organizations that desire to reduce their risk of experiencing a high impact cyber breach or incident must kill the threat early in its lifecycle, across the holistic attack surface.

Faster Detection & Response Reduces Risk



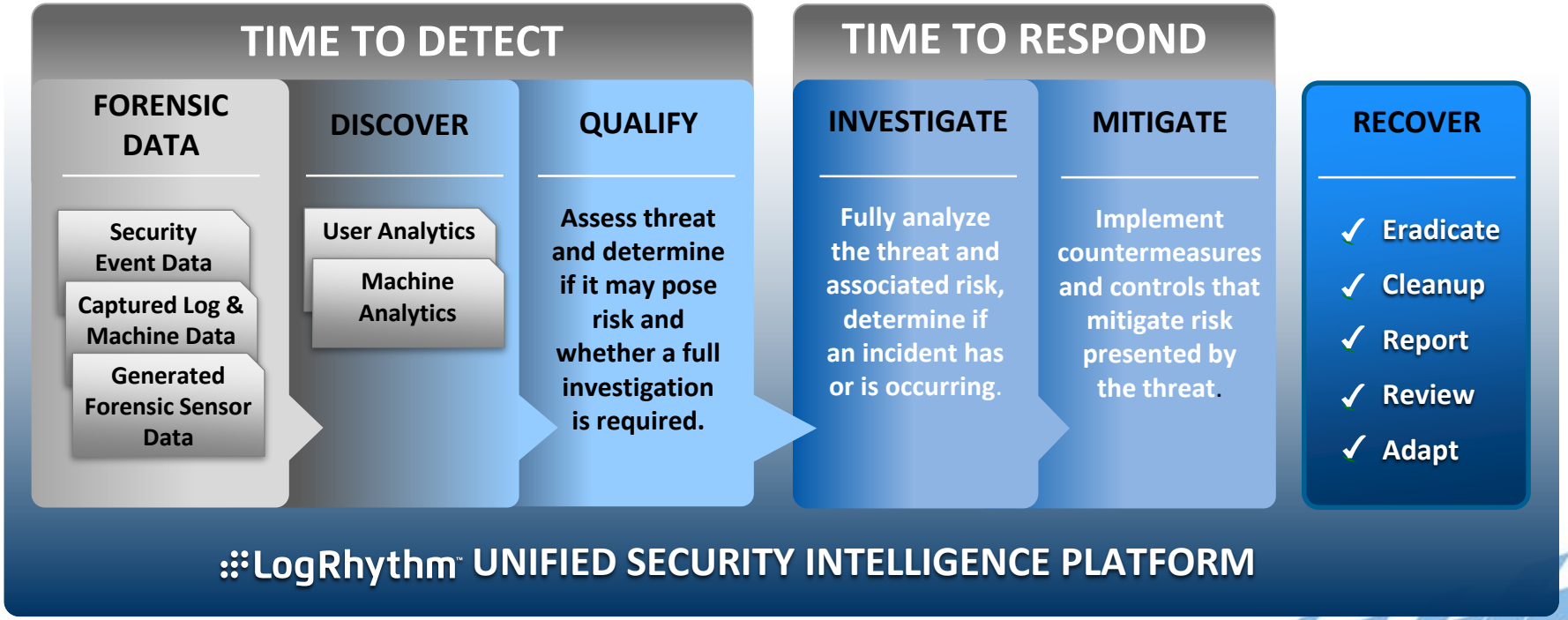
***MEAN-TIME-TO-DETECT (MTTD)**
The average time it takes to recognize a threat requiring further analysis and response efforts

***MEAN-TIME-TO-RESPOND (MTTR)**
The average time it takes to respond and ultimately resolve the incident

As organizations improve their ability to quickly detect and respond to threats, the risk of experiencing a high impact breach is greatly reduced.

Threat Lifecycle Management

End-to-End Detection & Response Workflow



Why a Security Intelligence Maturity Model ?

- There is an increasing rate and growing sophistication of cyber threats, which is leading to an increased awareness of the severity of cyber threats
- A fundamental shift is taking place on how an Enterprise delivers Security Intelligence and Cyber Security protection to the organization
- Security Monitoring and Intelligence are still not well defined and need a framework to enable recognition, review and response
- A clear definition and maturity model provides organizations with a roadmap of how to orchestrate this shift to achieve organizational security goals - What is your Mean time to detect and respond..?

Thank You!

Any questions?

Download the Security Intelligence Maturity Model whitepapers at:
www.logrhythm.com/simm