RSA Conference2016
San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: AIR-R02

Make IR Effective with Risk Evaluation and Reporting

Mischel Kwon
President/CEO
MKA Cyber
@mkacyber

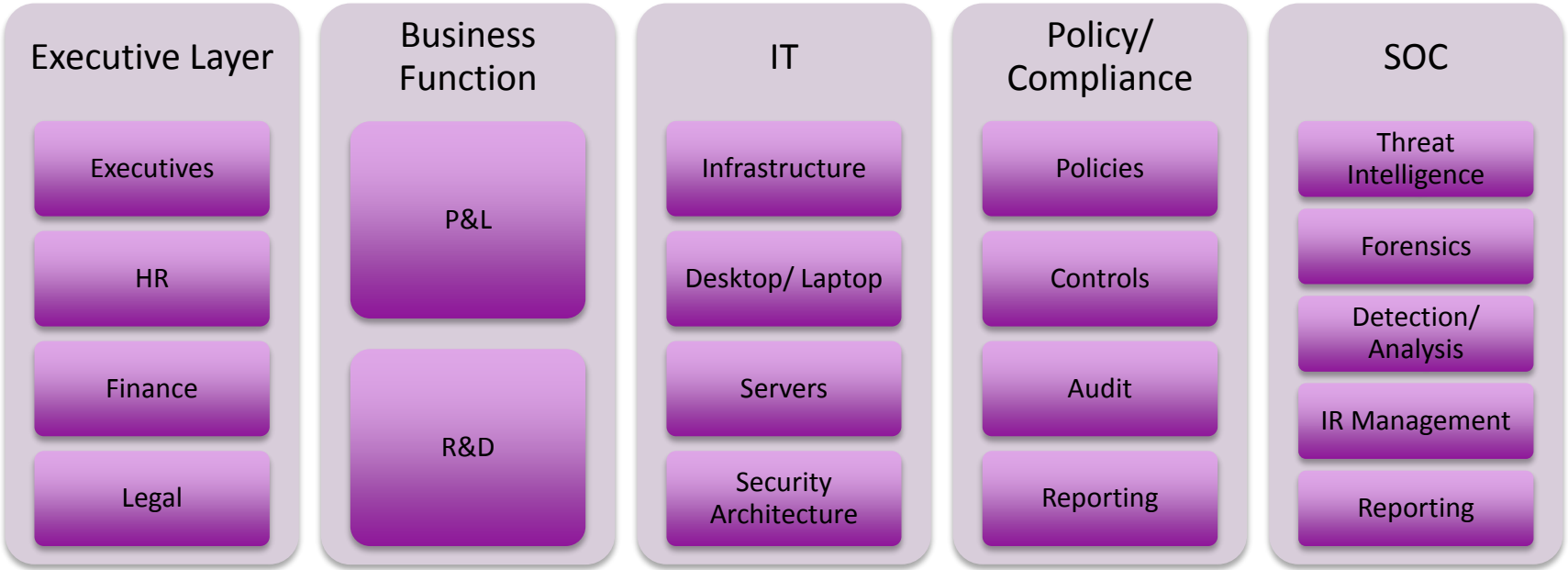
Justin Monti
Sr. VP Security Engineering
MKA Cyber

#RSAC

You've Got an Incident – Now What?

- Monitoring detects new rogue AD accounts
- Preliminary investigation suggests an intrusion
- What next? Who runs the incident?
- Forensic investigation reveals many technical details of the attack but fails to grasp business impact
- Without clear understanding of risk to company and client data, internal escalation is inadequate before client notification
- Company is behind the 8-ball as clients aggressively respond to potential breach

Classic Stove Piped Compliance Driven Security Program



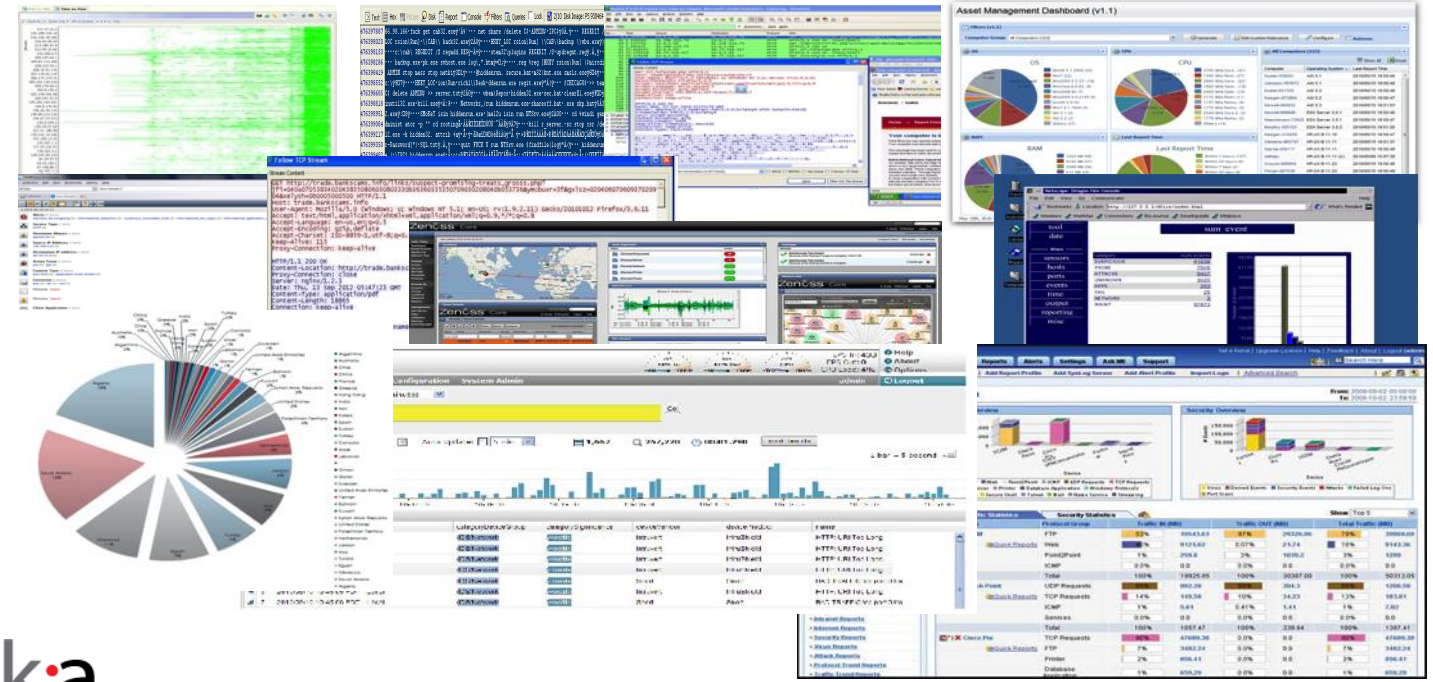
mk·a cyber

Classic SOC Practices

- Indicators based on disk forensics and canned vendor-delivered signatures
- SEIM Alert
- Pick a number – address the first 40 incidents because that's what you can handle
- Malware focus
- Find the dirty box and reimage
- Count up the hits – measure by numbers
- An occasional hunt and campaign discovery

mk·a cyber

This is What it Looks Like:



Incident Response – The Old Way

- OMG it's malware! – Manual Anti-virus
- Risk is all about the "sexiness" of the malware
- No distinction by systems impacted – critical business process or the soda machine
- Business owners not involved – treated as an IT issue only
- No criteria for severity – impact or technical sophistication – leaves open-ended decisions to analysts
- Anti-virus vendor, scan vendor – High, Medium, Low
- Impossible to articulate risk to executives – the sky is always falling
- The SOC ran the IR

Old IR Approach = FAIL

- External attention to an incident requires careful handling – missteps can be impossible to recover from
- Not understanding the true impact to the business mission hinders mitigation efforts
- Incident is not just impacting IT – it impacts the business
- Loss of business capability = loss of revenue
- Reputational damage = loss of customer confidence/trust, brand damage
- Regulatory/Investigation = penalties and other consequences

mk:a cyber

Why this does NOT work…

Data

Infrastructure Damage

Business Loss

Reputation

Remediation

Reconstitution

Reputation

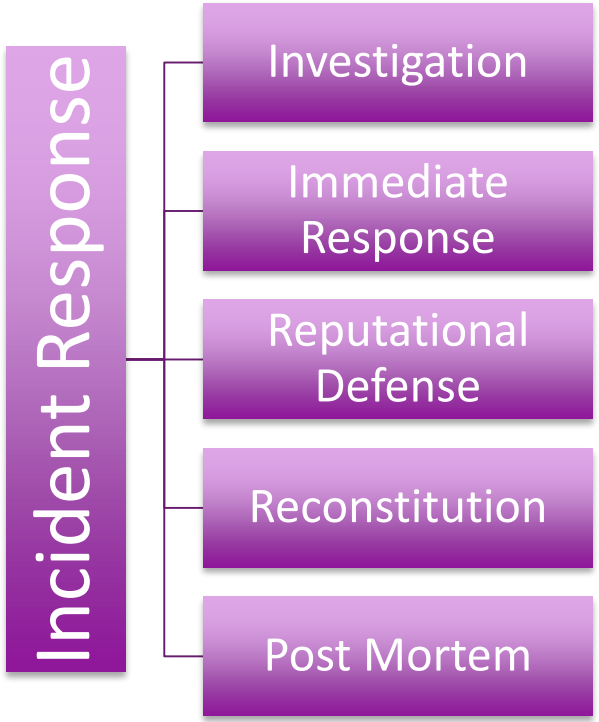
mk·a cyber

Threat and Business Risk Driven Program

- Not just SOC
- Education/Training/Exercise prior to incident
- Often other types of risk processes are used if a cyber incident affects a large amount of the enterprise/business – Crisis Teams

mk:a cyber

Business Driven Incident Response



- Business may take over responding to the incident
- Collaboration and early education on the threat is critical
- Risk is more than losing the box
- Risk is more than losing data
- Risk is:
  - Loss
  - Cost
  - Time
  - Reputation

mk:a cyber

Articulating Incident Risk to the Business

Cyber Risk Condition

Severe	Severe Risk to the Entity's mission or function
High	High Risk to the Entity's mission or function
Elevated	Elevated Risk to the Entity's mission or function
Guarded	Guarded Risk to the Entity's mission or function
Low	Low Risk to the Entity's mission or function

The Algorithm

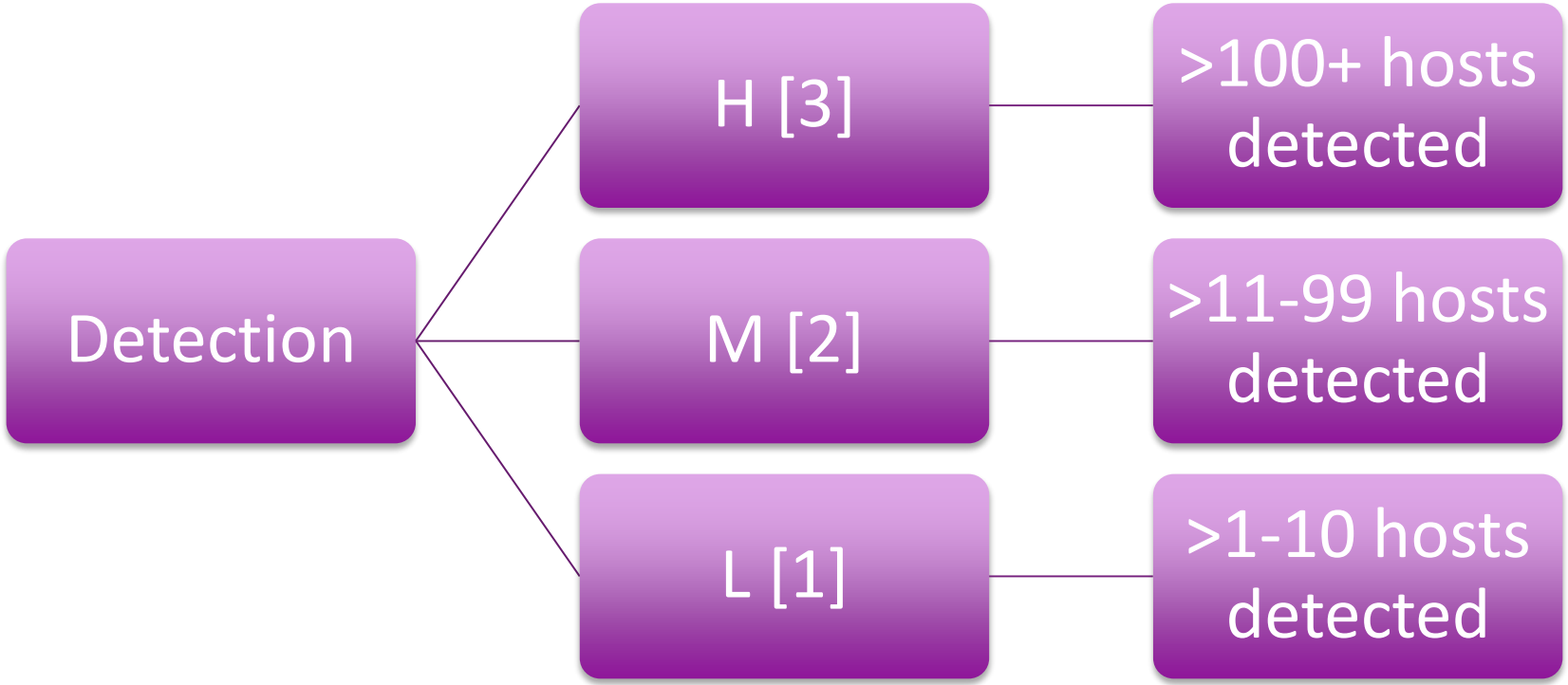
Attack Score * (Detection + Response + Remediation + Recovery + Reputation) = Risk Score

Severe	129 - 200
High	73 - 128
Elevated	33 - 72
Guarded	9 - 32
Low	0 - 8

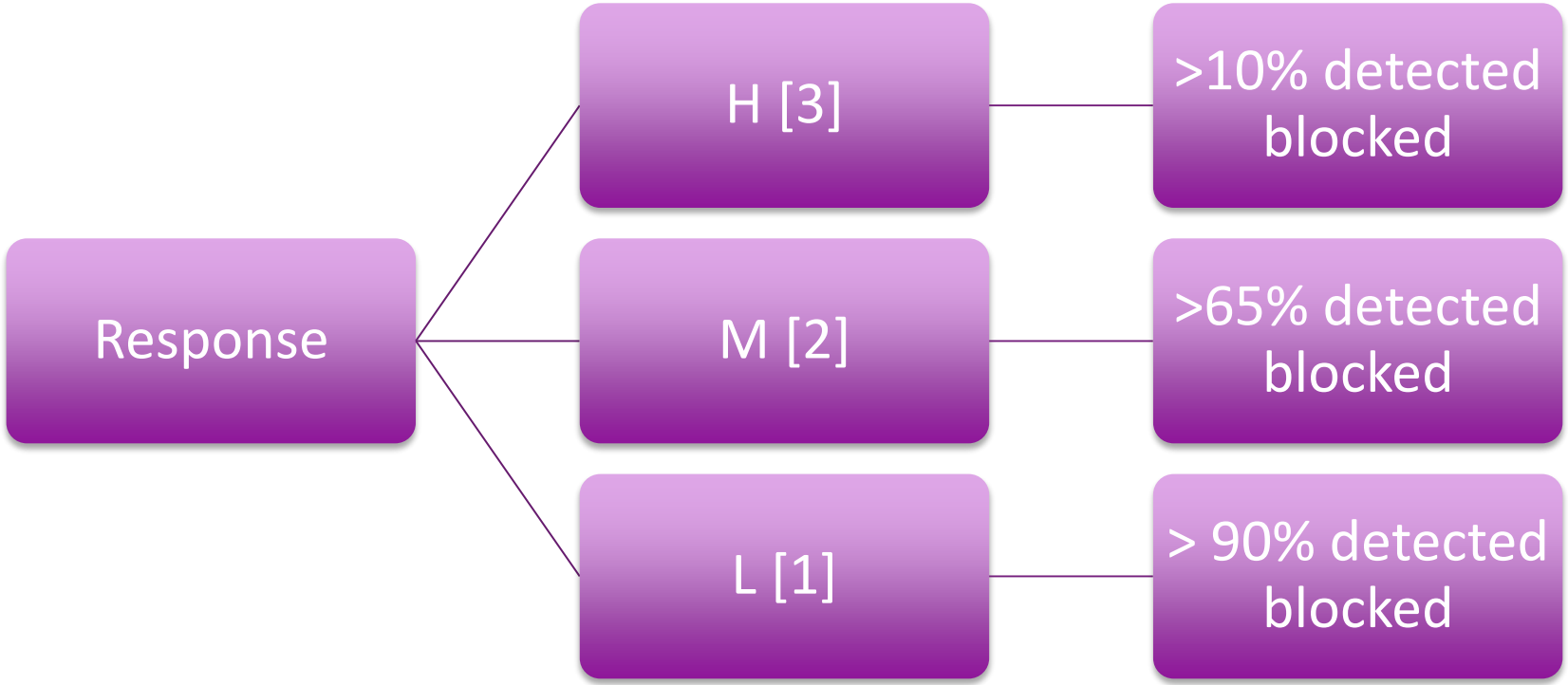
This is an example – you would tailor this to your organization

mk:a cyber

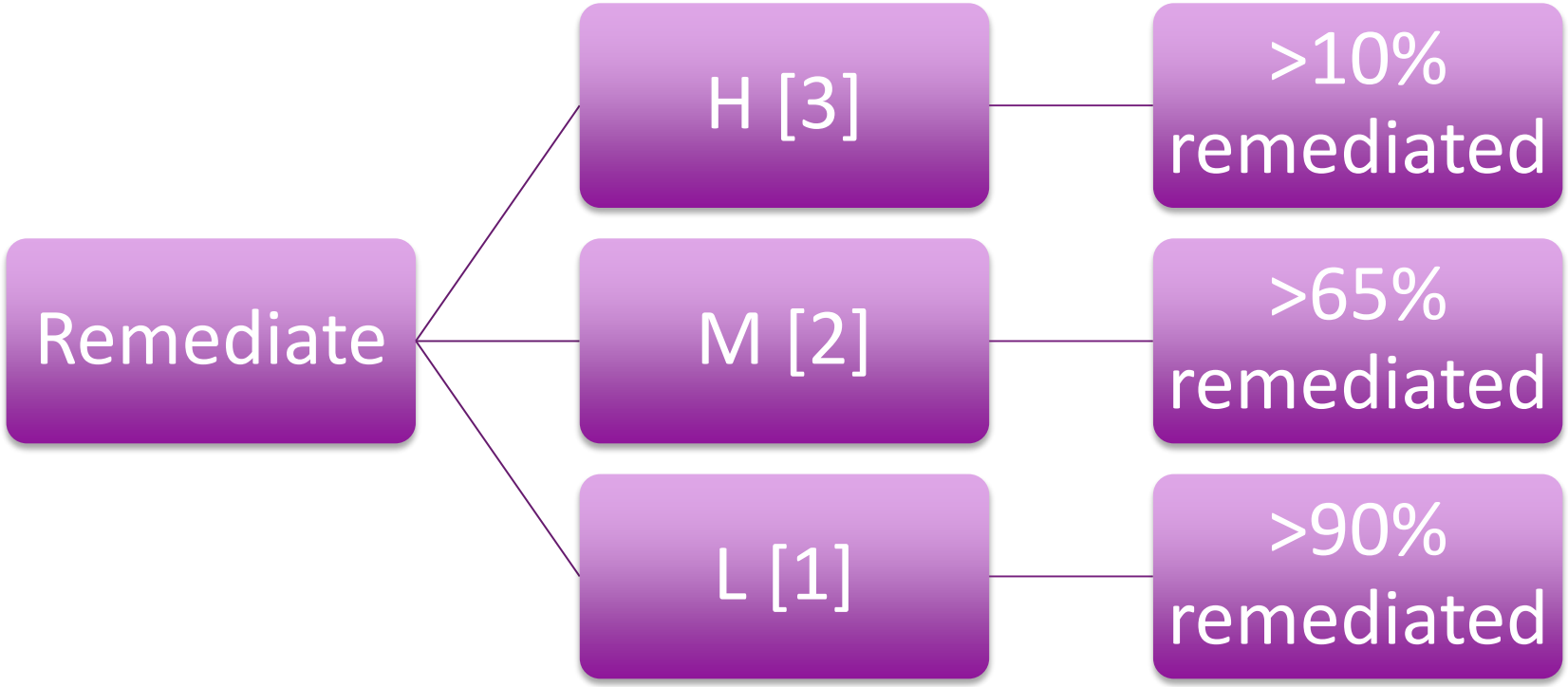
Detection Score



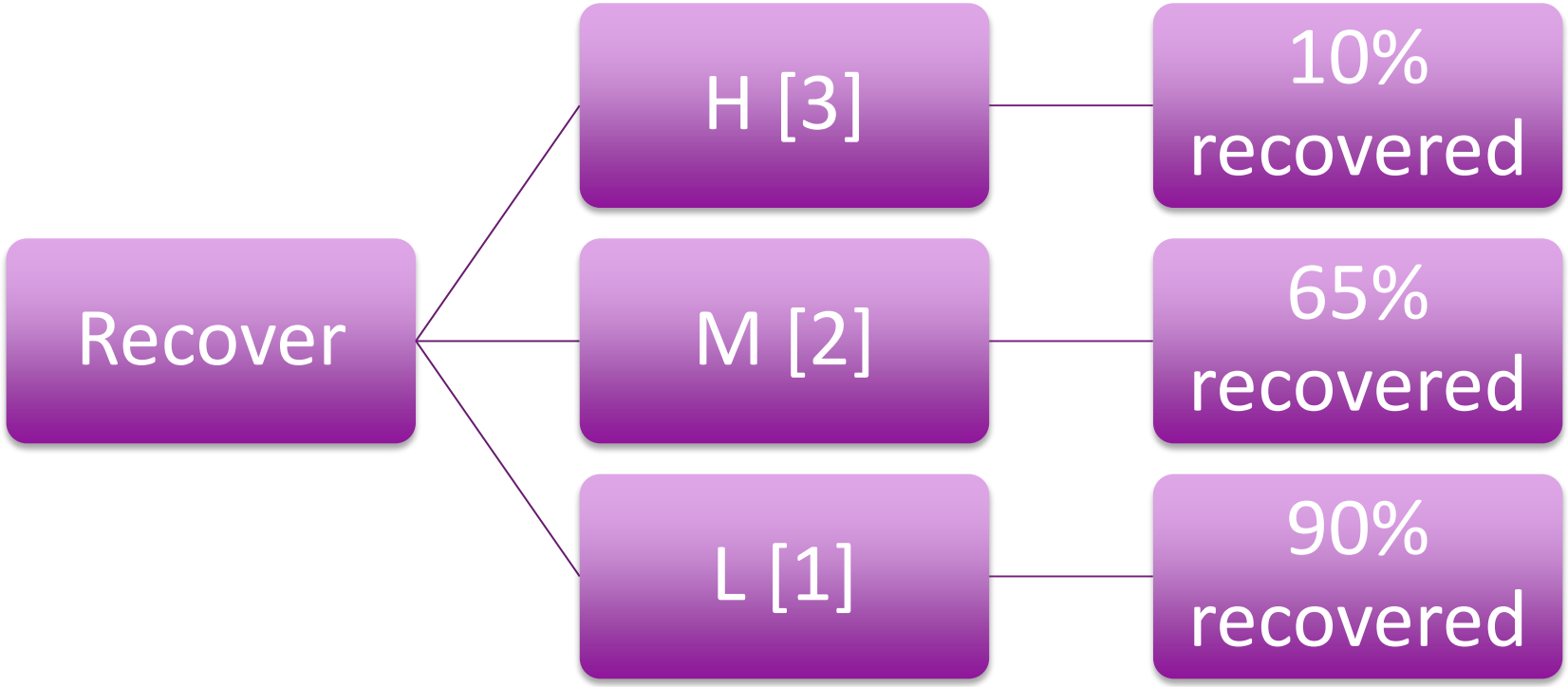
Response Score



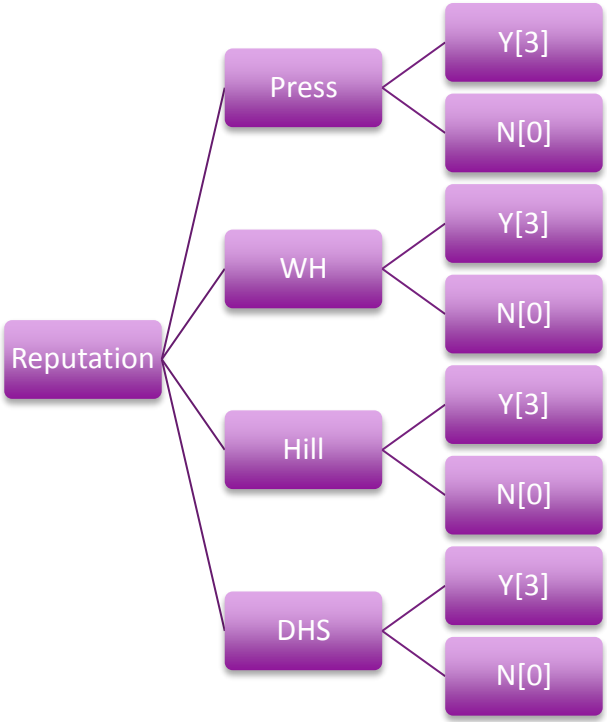
Remediation Score



Recover Score



Reputational Score



Scoring the Malware

$$AttackScore = \frac{Sum(Scores)}{Count(Attributes)}$$

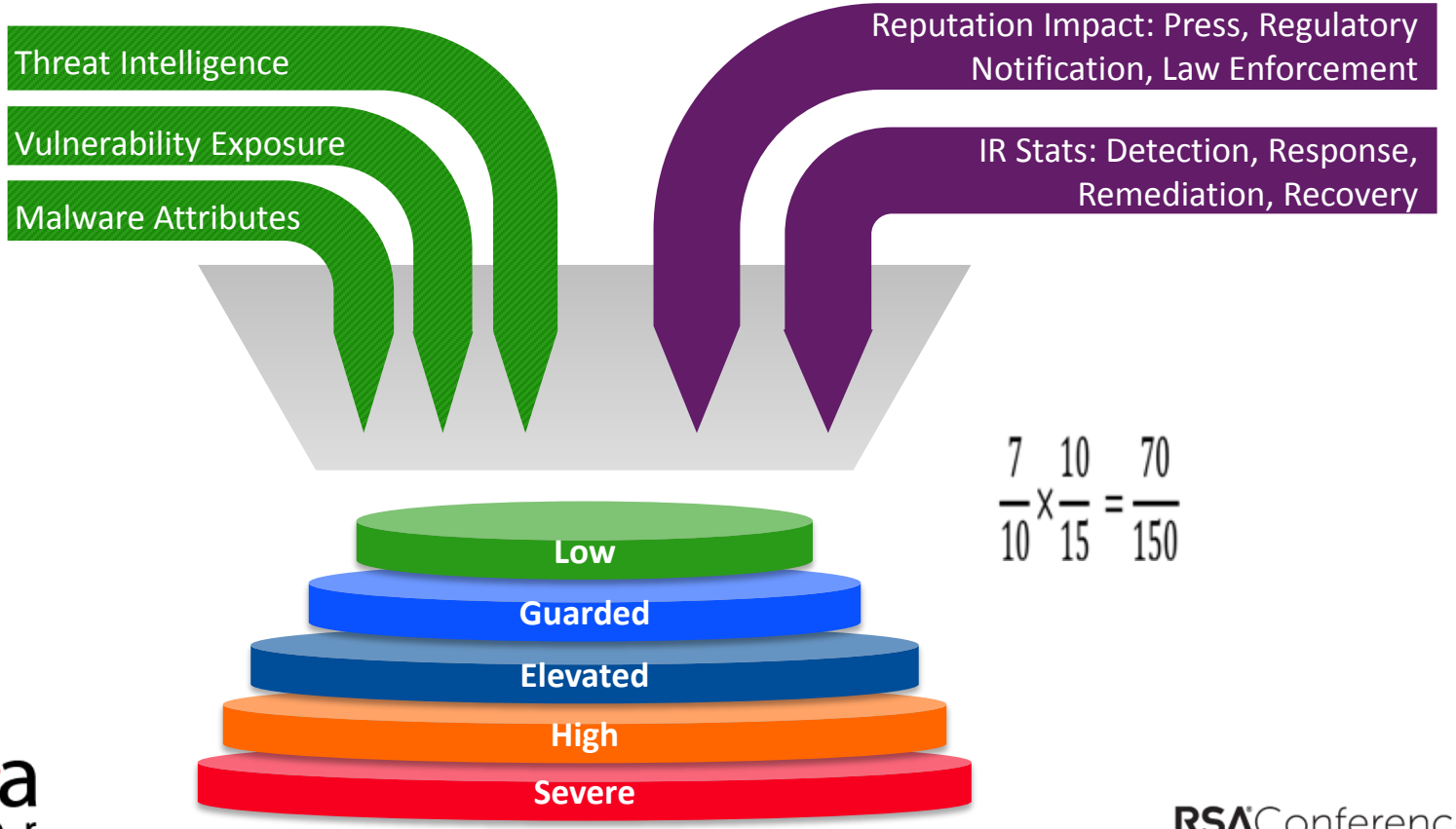
$$\frac{80}{11} = 7.27$$

Total number of attributes = 11

Attack Attributes	Score (0-10)
Prolific spreading (viral)	10
Polymorphic	10
Lateral movement	0
Zero day	0
Entity vulnerability exists	10
Lack of visibility to detect	8
Lack of intelligence	7
Lack of forensic evidence	5
Mission information exfiltration	10 (unknown)
Command and Control of internal machines	10 (unknown)
Spamming Campaign	10
Total	**80**

mk·a cyber

Cyber Risk Score - not just the SOC



$$\frac{7}{10} \times \frac{10}{15} = \frac{70}{150}$$

mk:a cyber

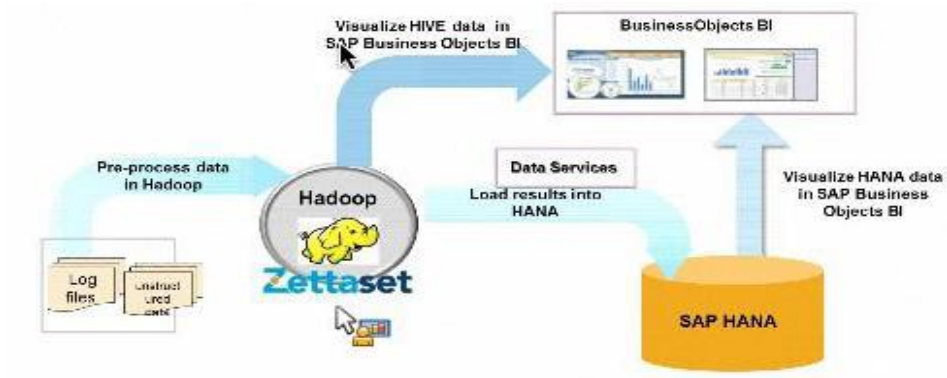
Data and Analytics – the Achilles' Heel

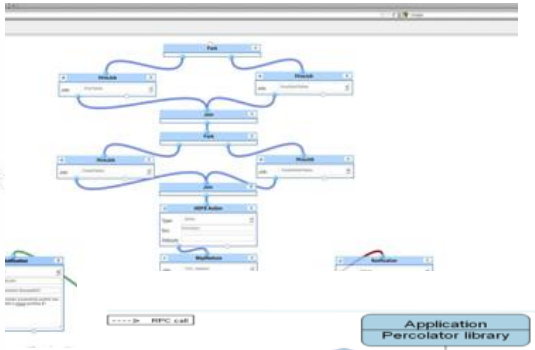
- Massive amount of Data – just sensors – not including remediation/compliance
  - 165,000 end users – 6000 servers
  - 3 core enterprise domains
  - 10 internet gateways – 4 OC-12s, 6 OC-3s
  - 1B+ Log Events daily

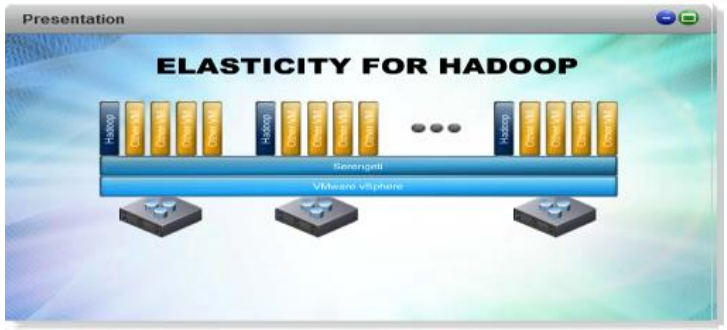
Active Data Collection	Daily	Monthly	Quarterly
Log Aggregation	6TB	120	260
SIEM	1TB	30	90
Full packet (Selective Traffi	15TB	210	630
IDS (W/Payload)	1TB	30	90
Firewall	.5TB	15	45
Malware Protection	.5TB	15	45
Totals	***24TB***	***720TB***	***2160Tb***
			2.1Pb
			w/20% surge
			2.5Pb per Qtr

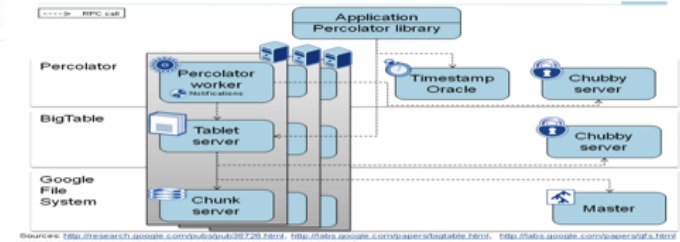
mka cyber

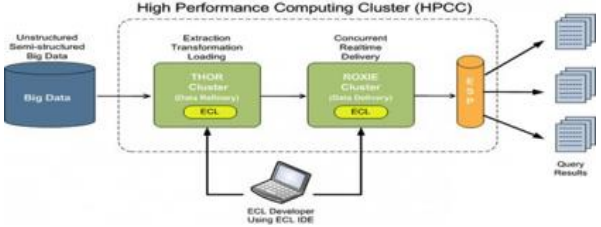
Pulling the Data Together











mk·a cyber

Challenges

Technical

- Fast Analysis Engine – In Memory
- Agile Data Model - Simple Modifications
- Mapping Attack to Vuln to Control/Policy

Communicate

- Reporting - Technical, Managerial, Executive
- Metrics - Technical, Managerial, Executive

Logistical

- Data Storage
- Data Access
- Data Sources

Organizational

- Budget
- Policy – Keeping up with the Adversary
- Understanding Impact/Risk to Business

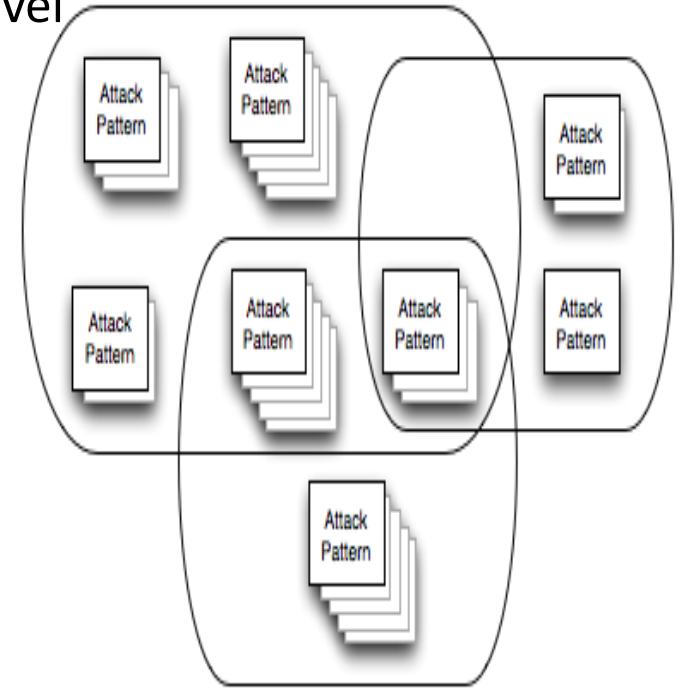
mka cyber

The Future Wish List

- Shared Pattern Libraries – on the meta data level
- Vulnerability management based on patterns

  not just one for one
- One data format
- Acceptance and tools to manage other data

  storage formats
- Shared Analyst pools
- Mission participation in Risk Analysis



mk:a cyber

Apply – What Can I Do?

- Help the SOC understand the business mission they protect
- Get the SOC access to asset data – what business process it supports, vulnerability state, configuration hygiene state
- Review your IR plan – what is the escalation and communication plan? Who is included? HR? Legal? PR? Business Units?
- Work with IR stakeholders to tune the Cyber Risk Score algorithm to your organization
- Use it to track risk in your next incident or IR exercise

Summary

- Today's SOC must be driven by internal and external intelligence to clearly understand both the threat and the risk
- The entire organization MUST understand the threat and participate in assessing the risk from the business perspective in order to accept the risk
- Risk must be derived from Business Risk , IT Risk, as well as Security Vulnerability
- IR is more than understanding the attack – and loss of data – but what it takes to get back to business or even – JUST SURVIVE
- Targeted is scary – but a business that is crippled is just as scary
- We have all the data – now how do we look at it…

mk·a cyber

Q&A

Mischel Kwon

Justin Monti

info@mkacyber.com
+1 (703) 291-1331
2700 Prosperity Ave, Suite 262
Fairfax, VA 22031
USA

mk:a cyber