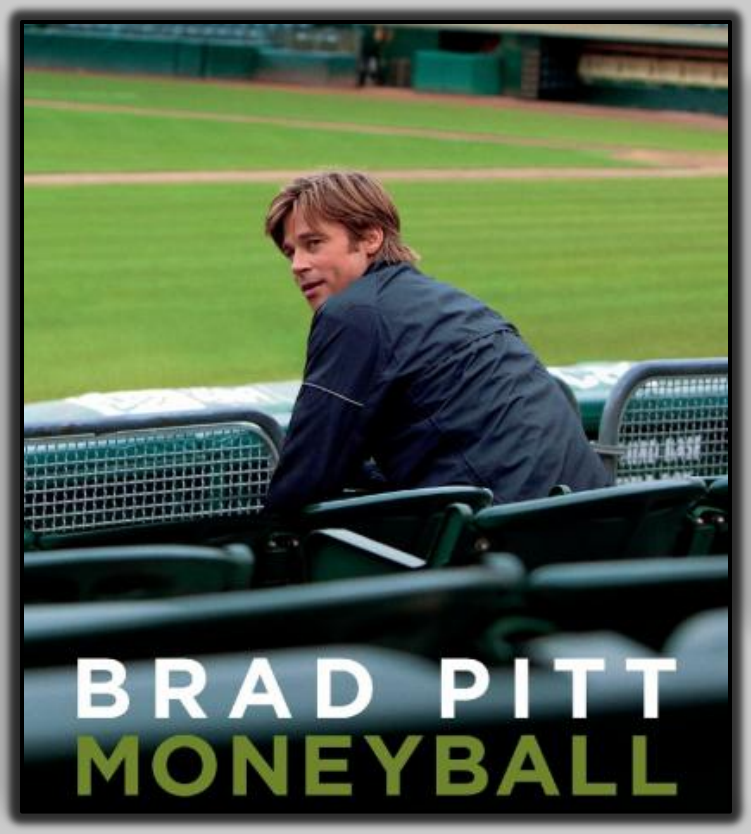
Embracing the Uncertainty of Advanced Attacks using Big Data Analytics

Eddie Schwartz
CISO, RSA


BRAD PITT
MONEYBALL


ANONYMOUS
We are Legion. We do not Forgive. We do not Forget.


.249

Last	First	AB	R	H	2B	3B	HR	RBI	BB	SO	SB	BA	OBP	SLG	OPS
Ortiz	David	560	113	162	37	1	41	130	109	129	0	.289	.406	.577	.983
Ramirez	Manny	486	93	144	32	1	33	105	84	111	0	.297	.400	.567	.967
Drew	J.D.	406	77	116	27	3	15	61	70	88	4	.285	.392	.476	.868
Pena	Wily Mo	378	55	104	23	1	20	66	30	111	3	.276	.336	.504	.840
Youkilis	Kevin	523	90	142	37	2	18	76	84	106	4	.271	.376	.456	.832
Crisp	Coco	509	84	158	27	3	13	63	40	75	21	.310	.361	.452	.814

Crisp Coco 509 84 158 27 3 13 63 40 75 21 .310 .361 .452 .814

Hinske	Eric	279	41	73	18	2	10	41	30	69	5	.263	.336	.446	.782
Lowell	Mike	482	64	131	33	1	15	74	42	59	2	.273	.333	.441	.774
Lugo	Julio	473	74	134	29	3	8	51	44	74	19	.284	.347	.406	.753
Mirabelli	Doug	124	13	27	7	0	5	17	12	38	0	.218	.294	.386	.680
Cora	Alex	212	26	54	8	2	2	20	15	27	5	.254	.313	.333	.646

Giambi	Jason	395	84	100	18	0	29	81	102	99	2	.252	.413	.518	.930

Giambi Jason 395 84 100 18 0 29 81 102 99 2 .252 .413 .518 .930

Jeter	Derek	585	110	189	32	4	12	71	59	93	23	.322	.390	.452	.843
Abreu	Bobby	474	95	131	28	2	16	65	86	107	22	.277	.389	.447	.835
Damon	Johnny	548	94	158	30	4	18	73	62	76	14	.289	.362	.458	.821
Cano	Robinson	533	76	164	36	3	16	80	30	65	5	.308	.345	.472	.817
Posada	Jorge	405	65	105	21	1	17	65	65	84	2	.259	.365	.443	.808
Phillips	Andy	286	37	74	15	2	11	45	21	60	2	.259	.313	.441	.754
Cabrera	Melky	514	74	145	27	3	10	59	45	65	10	.282	.341	.408	.749
Mientkiewicz	Doug	232	29	58	13	1	5	30	26	38	1	.251	.328	.382	.710
Cairo	Miguel	179	22	46	8	1	2	16	9	23	8	.258	.300	.343	.643
Fasano	Sal	130	10	29	6	0	4	16	6	37	0	.220	.260	.352	.612


AUDIT CHECKLIST
Audit Satisfactory
Nonconformances Found
Observations Made


CERTAINTY
INTERNATIONAL
CERTIFICATIONS
ISO
27001


FAIL
UNCERTAINTY
CERTAINTY
UNCERTAINTY
fallblog.org

CERTAINTY??

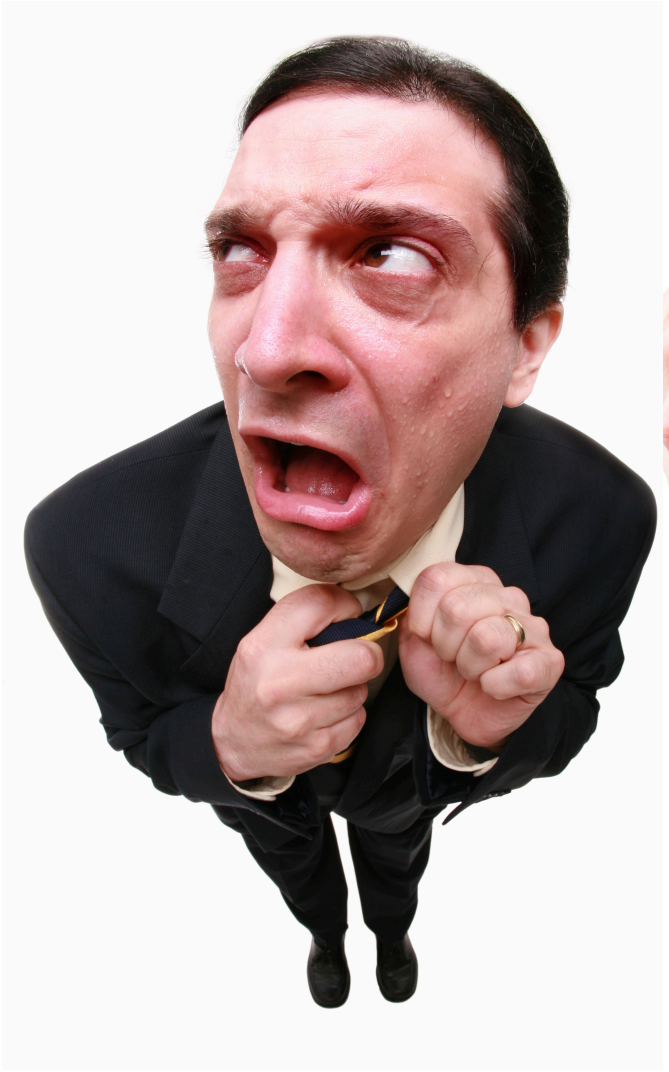
Just a question on signatures...

From an AV Forum

Does the signature team not do Zeus/ZBot configuration files? We have submitted a number (20+) of ".bin" files over the last 6-8 weeks but have yet to see these files detected using "Official" signatures. Should we not submit these files?

Tom

FEAR

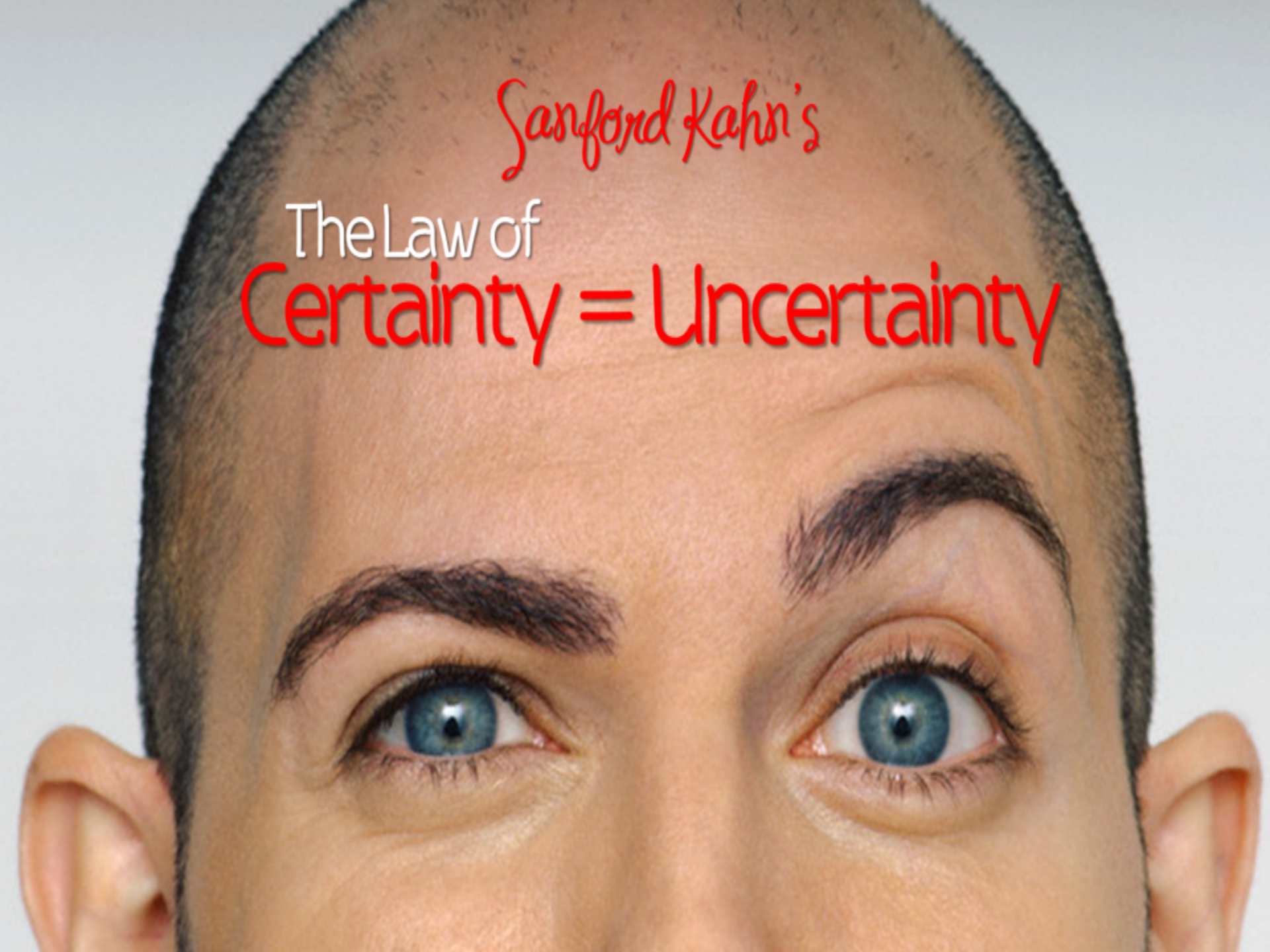


UNCERTAINTY

DOUBT

THE IDES OF MARCH

"Caesar recognized the omens, he just didn't think they applied to HIM." - Nate Silver

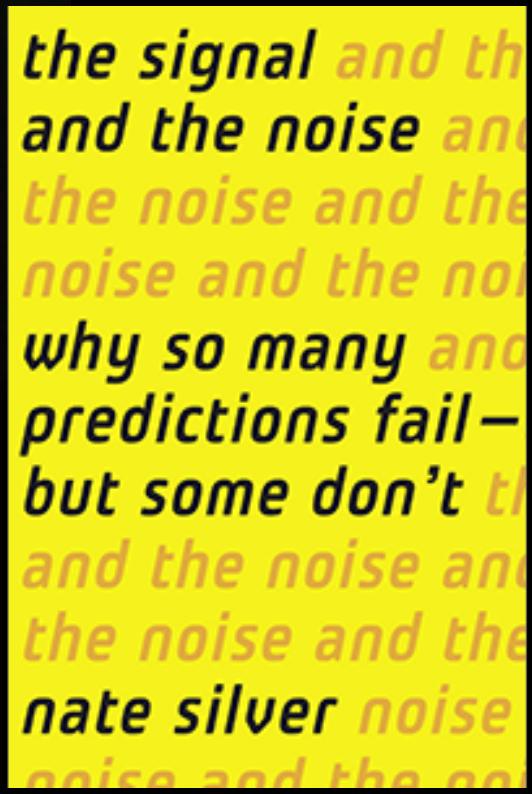

Sanford Kahn's
The Law of
Certainty = Uncertainty

without much

regard for the distortions that this causes. We think we want information when we really want knowledge.

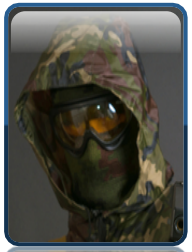
The signal is the truth. The noise is what distracts us from the truth. This is a book about the signal and the noise.

340 highlighters

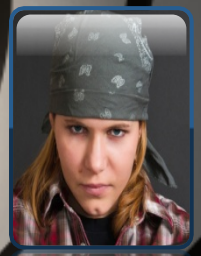


Organized crime

Nation states



Insiders



Cyber-terrorists / Hacktivists

Others…

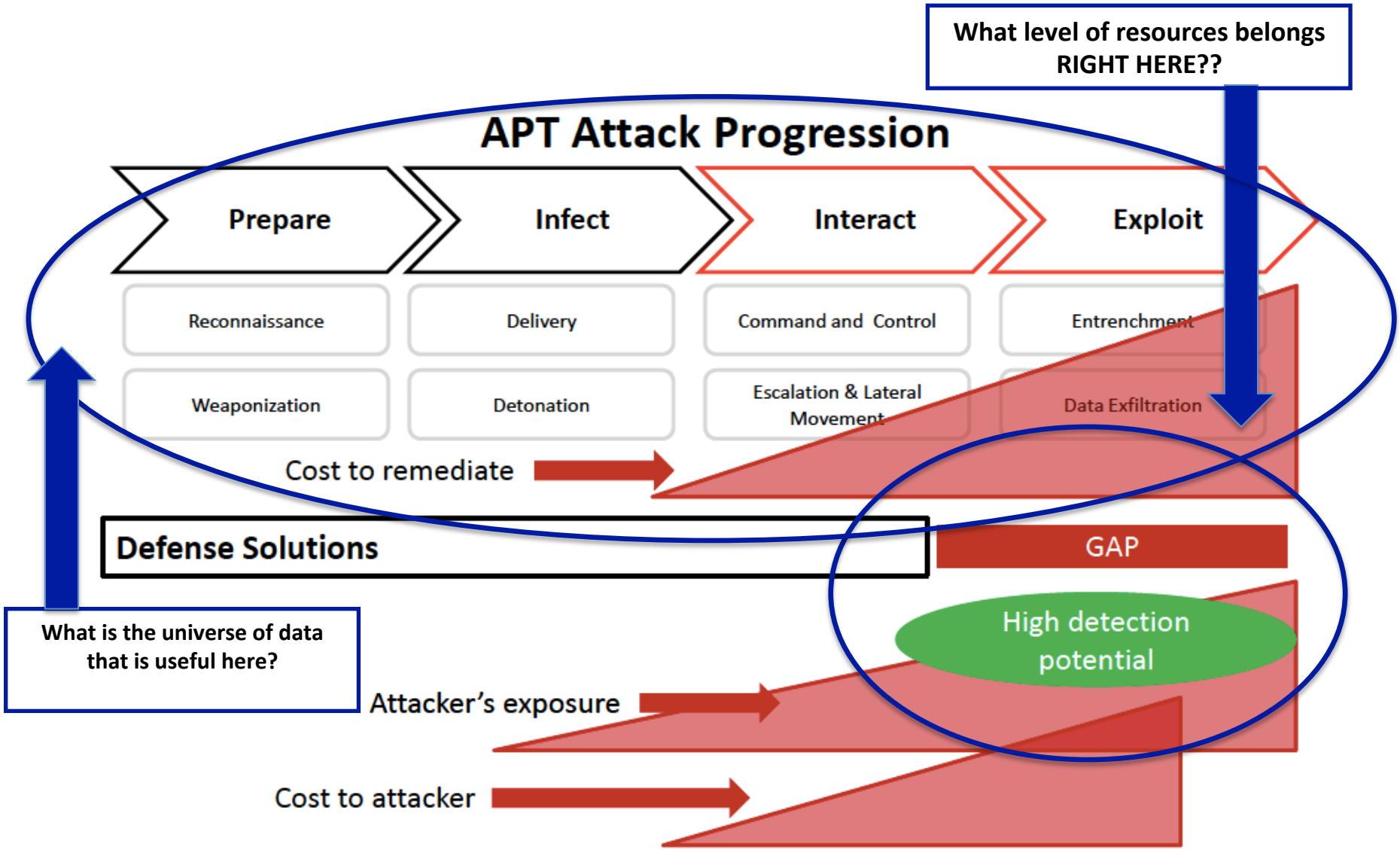
APT 2:

Exposing one China's most BIZARRE cyber espionage units

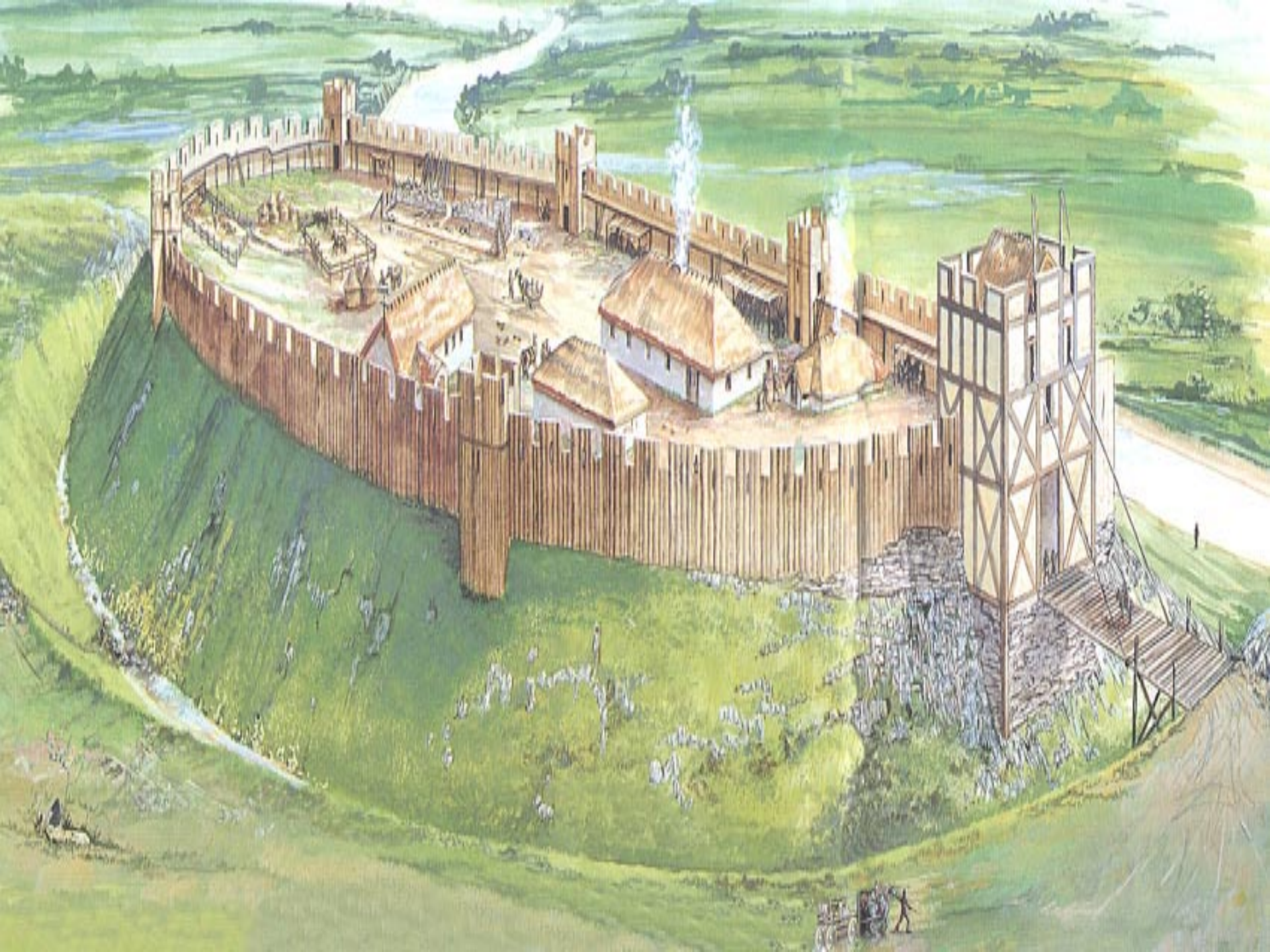
MANDIANT

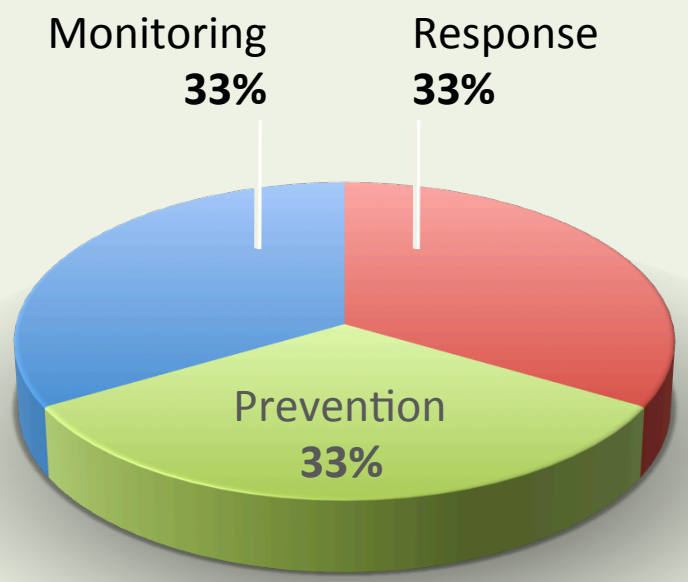
ſ

∞

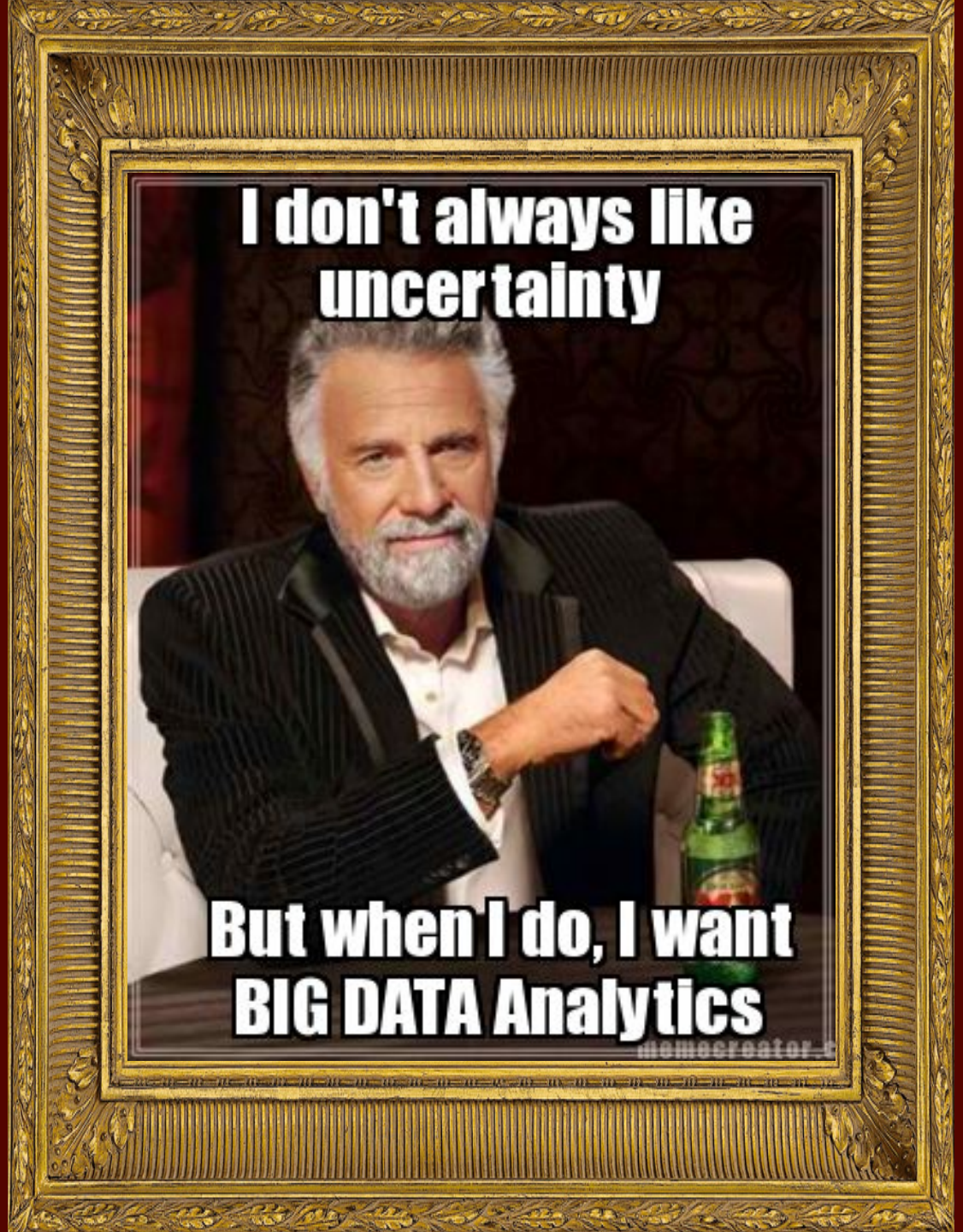


Source: Greg Hogland

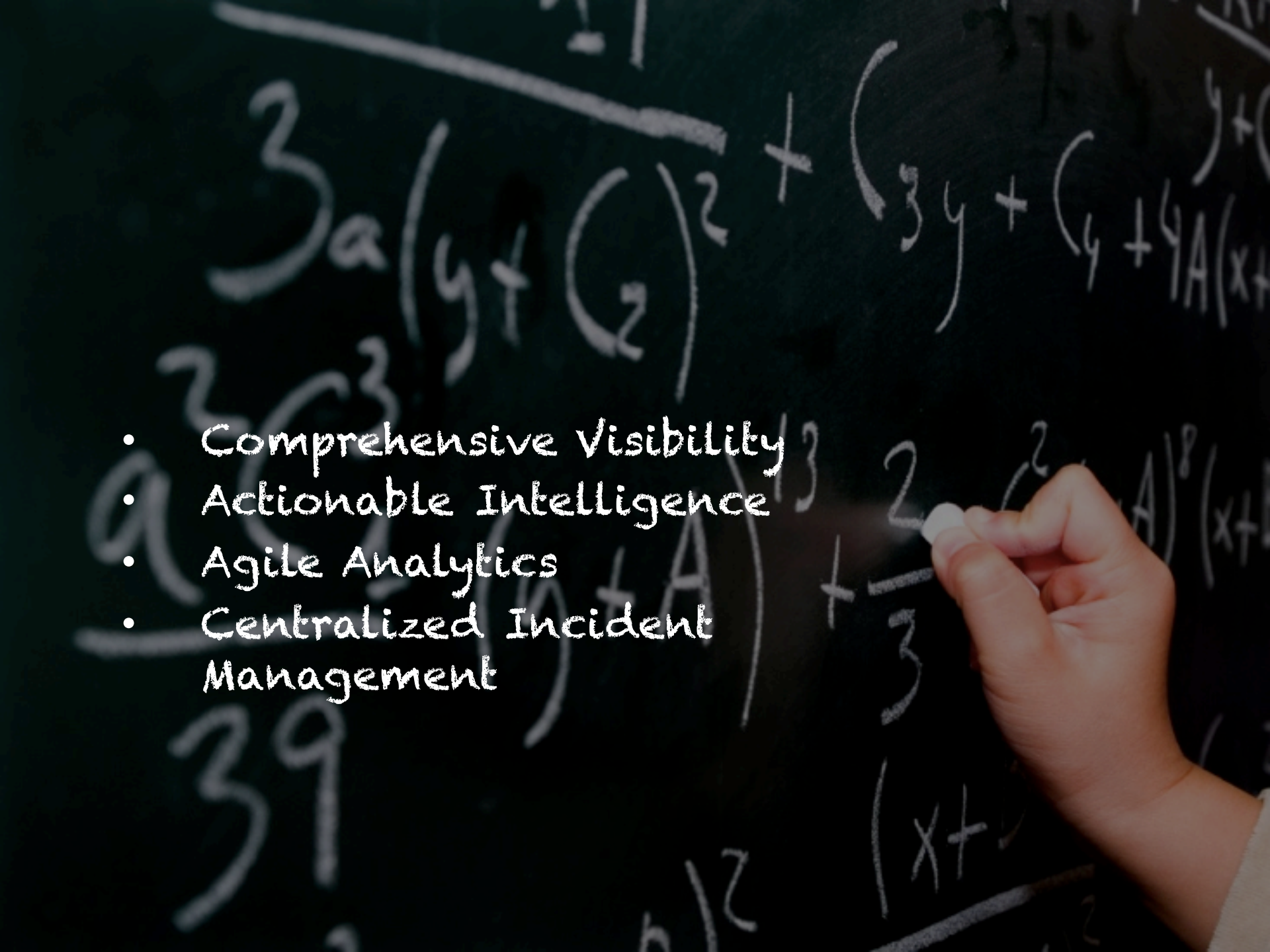



Monitoring
33%
Response
33%
Prevention
33%


The Rise of Big Data

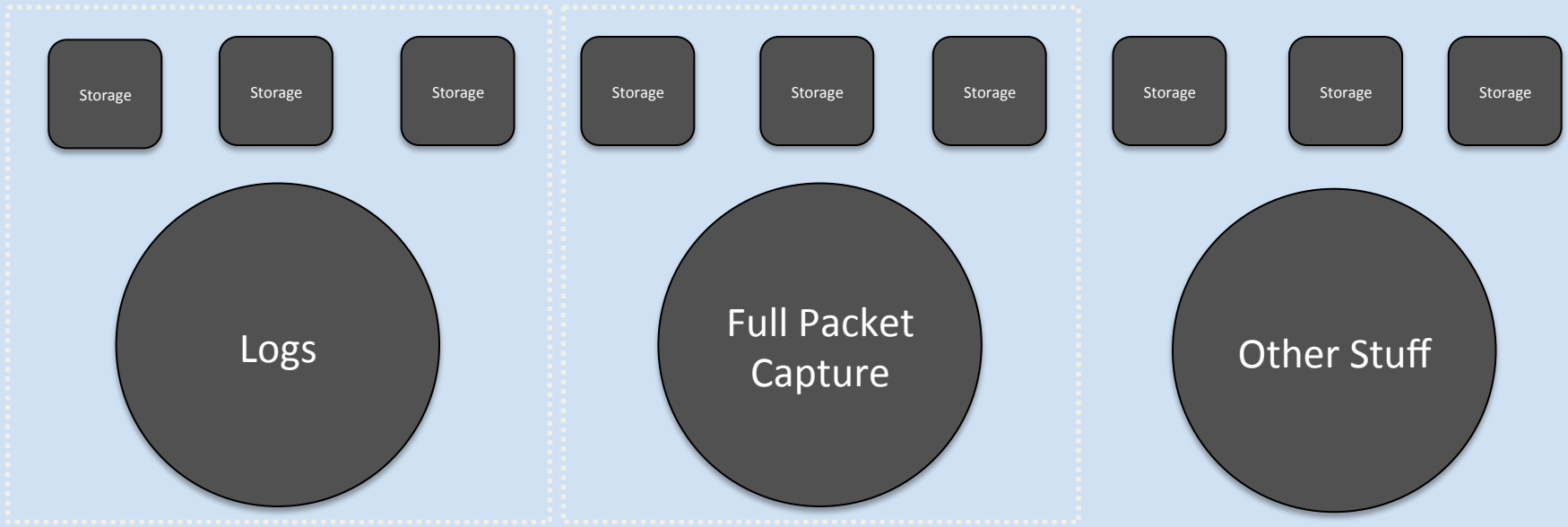

I don't always like uncertainty
But when I do, I want BIG DATA Analytics


BIG DATA
TRANSFORMS
SECURITY



- Comprehensive Visibility
- Actionable Intelligence
- Agile Analytics
- Centralized Incident Management

A ∩ B, etc.

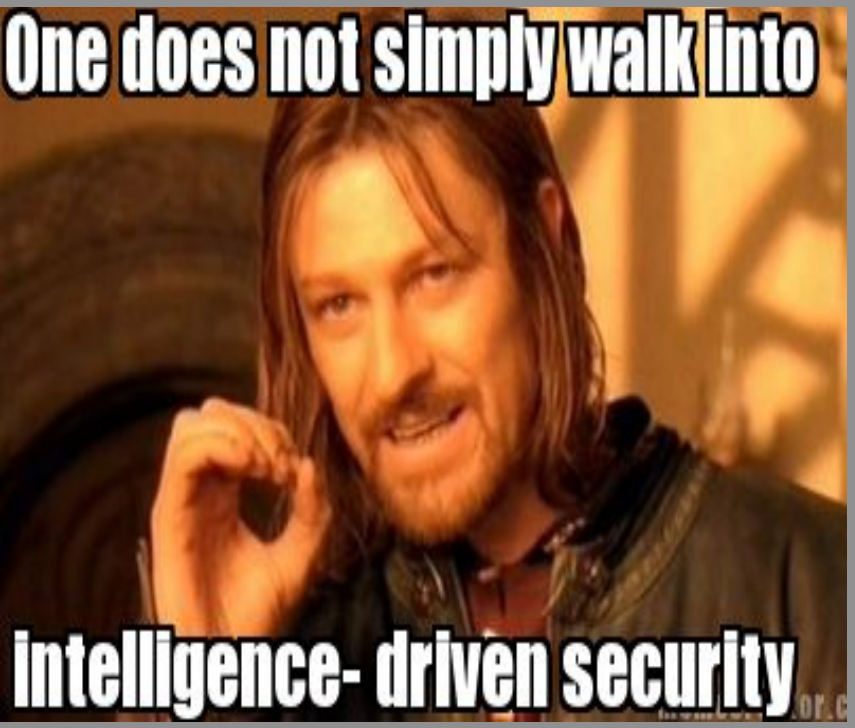


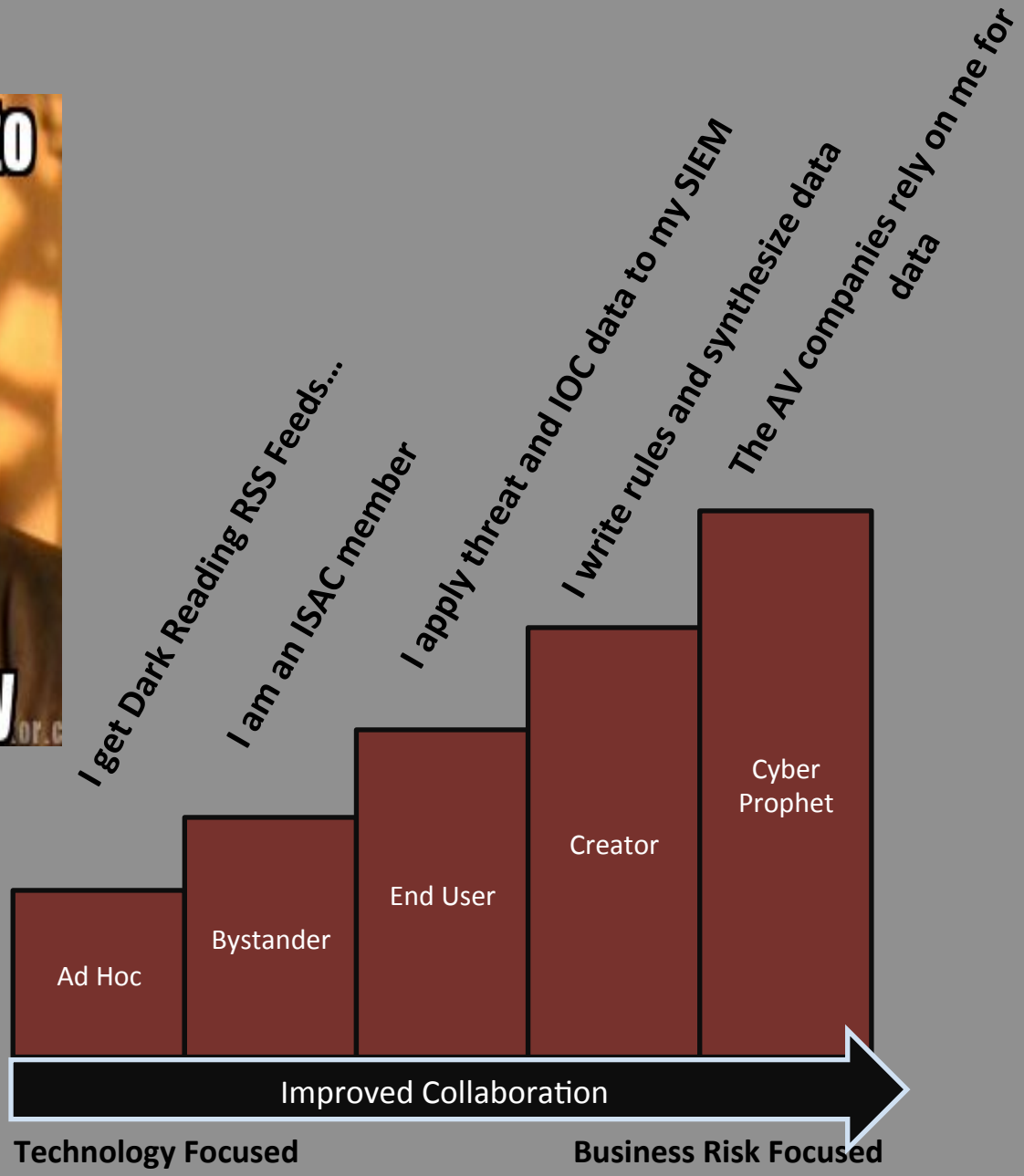
Event Management

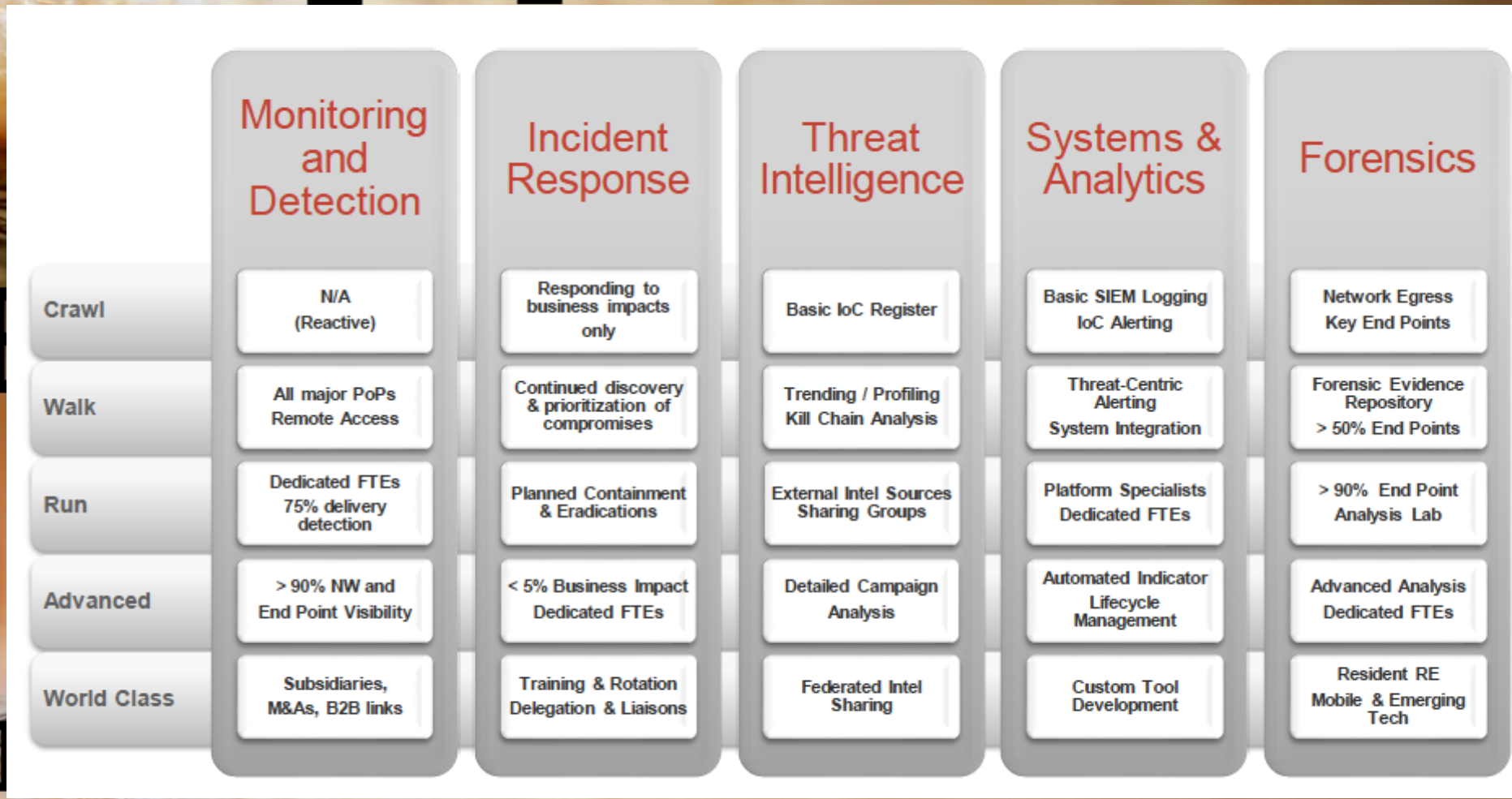
Search Tools

Intel

	SOC	CIRC
Tasks	•Tool Administration •Vulnerability Scanning •Tier 1 Event Support •Break-Fix	•Incident Investigation •Threat Intelligence •Malware Analytics •Response Coordination
Skill set required	•Intermediate security knowledge •Good tool & process knowledge •Generic company knowledge	•Deep threat knowledge •Advanced technical capability •Investigative experience •Deep company knowledge
Role of a service provider	•Can successfully be outsourced to an MSSP	Tough to outsource as a standalone function
Bottom Line	•Waiting for a smack on the head	Hunting bad guys


One does not simply walk into
intelligence- driven security


I get Dark Reading RSS Feeds...
I am an ISAC member
I apply threat and IOC data to my SIEM
I write rules and synthesize data
The AV companies rely on me for data
Ad Hoc
Bystander
End User
Creator
Cyber Prophet
Improved Collaboration
Technology Focused
Business Risk Focused


Monitoring and Detection
Incident Response
Threat Intelligence
Systems & Analytics
Forensics
Crawl
N/A (Reactive)
Responding to business impacts only
Basic IoC Register
Basic SIEM Logging
IoC Alerting
Network Egress
Key End Points
Walk
All major PoPs
Remote Access
Continued discovery & prioritization of compromises
Trending / Profiling
Kill Chain Analysis
Threat-Centric Alerting
System Integration
Forensic Evidence Repository
> 50% End Points
Run
Dedicated FTEs
75% delivery detection
Planned Containment & Eradications
External Intel Sources
Sharing Groups
Platform Specialists
Dedicated FTEs
> 90% End Point
Analysis Lab
Advanced
> 90% NW and End Point Visibility
< 5% Business Impact
Dedicated FTEs
Detailed Campaign Analysis
Automated Indicator Lifecycle Management
Advanced Analysis
Dedicated FTEs
World Class
Subsidiaries, M&As, B2B links
Training & Rotation
Delegation & Liaisons
Federated Intel Sharing
Custom Tool Development
Resident RE
Mobile & Emerging Tech

D F T P Z E L O D B

Critical Incident Response Center

Cyber Threat Intelligence

- Open/All Source Actor Attribution
- Attack Sensing & Warning
- Social Media
- High Value Target (HVT)

Advanced Tools, Tactics & Analysis

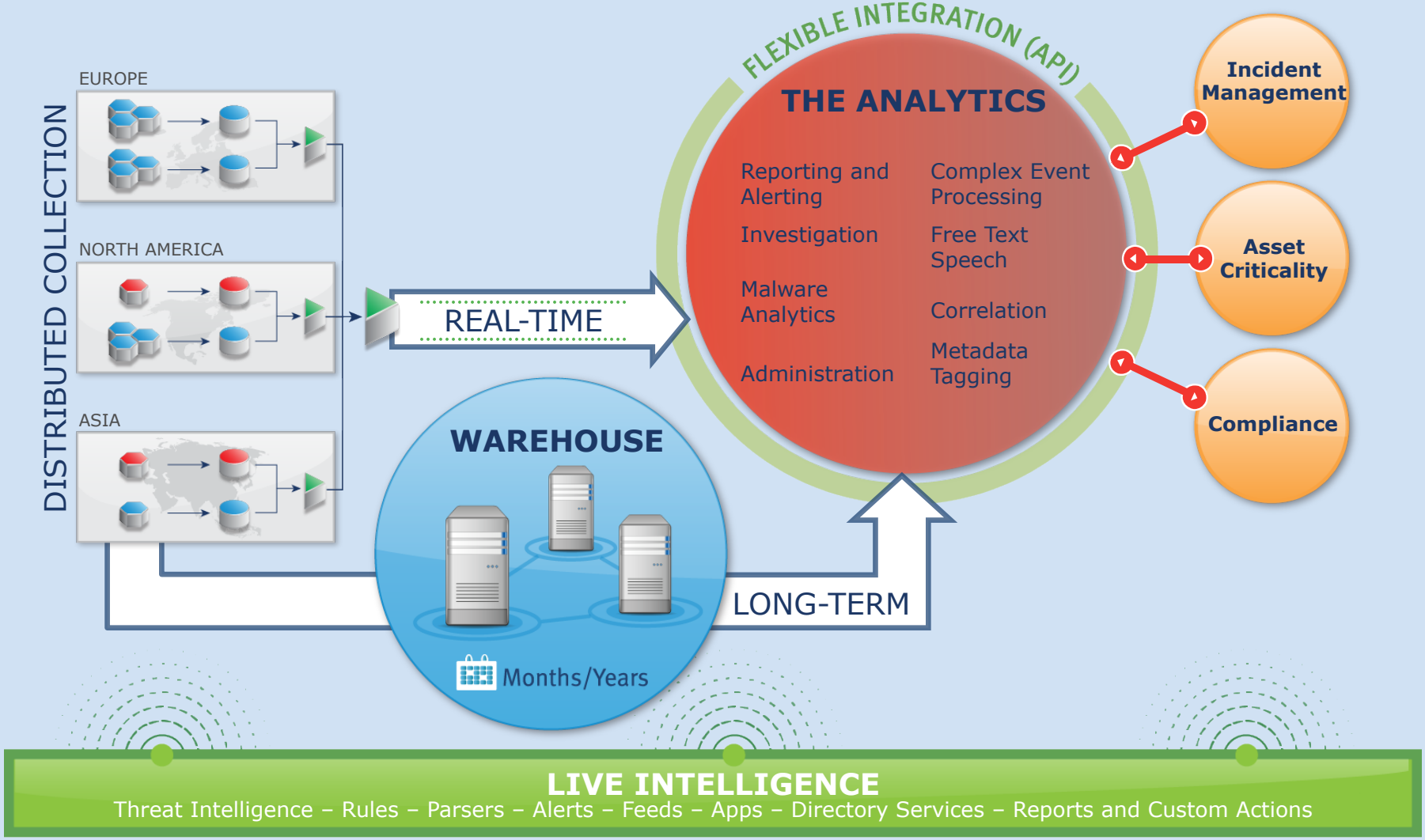
- Reverse Malware Engineering
- Host & Network Forensic
- Cause & Origin Determination
- Email operations

Critical Incident Response Team

- Eyes-on-Glass
- End User Intake
- Event Triage
- Incident Containment
- 24x7 Coverage

Advanced Specialists

- Integration & Content Development
- Strategic Planning


DISTRIBUTED COLLECTION
EUROPE
NORTH AMERICA
ASIA
REAL-TIME
FLEXIBLE INTEGRATION (API)
THE ANALYTICS
Reporting and Alerting
Complex Event Processing
Investigation
Free Text Speech
Malware Analytics
Correlation
Administration
Metadata Tagging
Incident Management
Asset Criticality
Compliance
WAREHOUSE
Months/Years
LONG-TERM
LIVE INTELLIGENCE
Threat Intelligence – Rules – Parsers – Alerts – Feeds – Apps – Directory Services – Reports and Custom Actions

All Network Traffic & Logs

Downloads of executables

Type does not match extension

!

Terabytes of data - 100% of total

Thousands of data points – 5% of total

Hundreds of data points – 0.2% of total

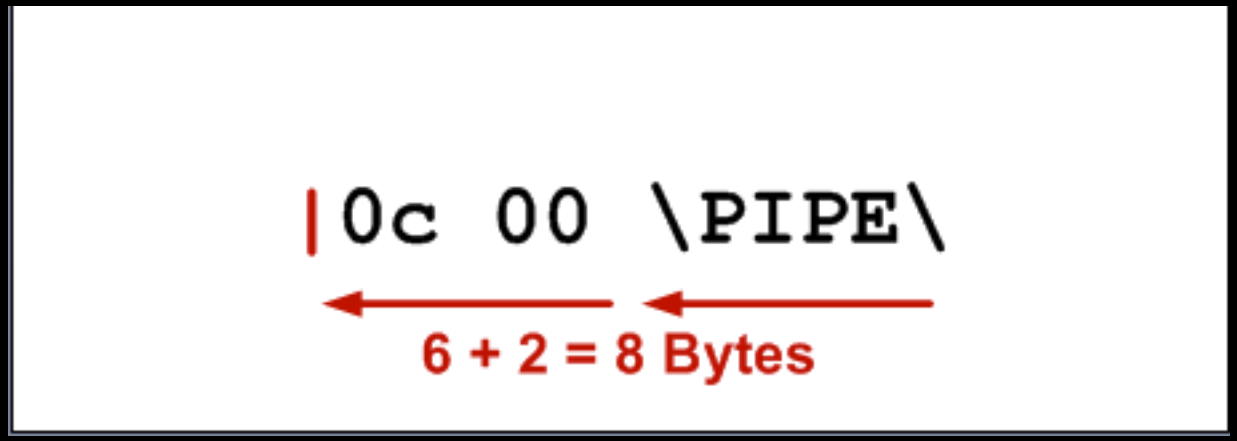
<u>Create alerts to/from critical assets</u>
A few dozen alerts

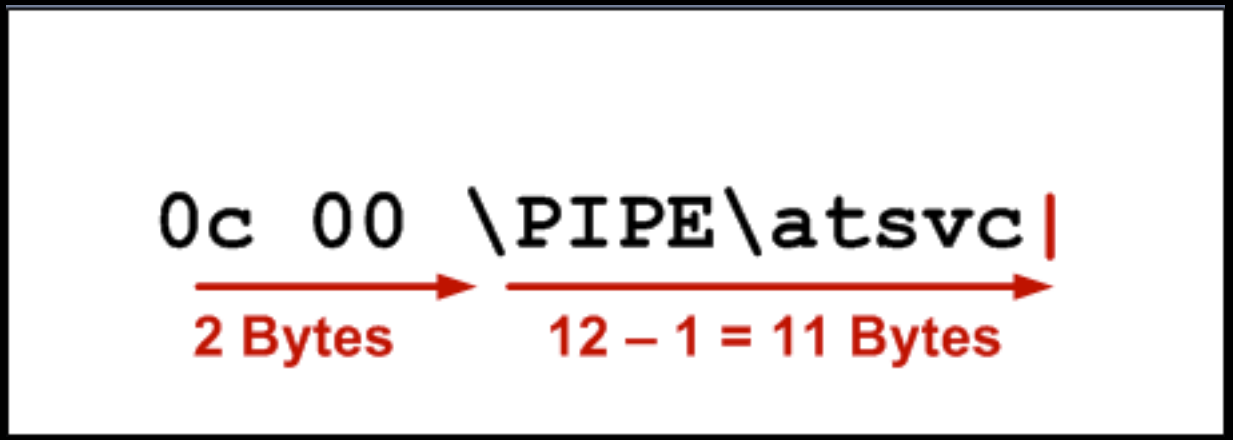
- Named Pipes -> OS Construct for Inter-process Communication.
- Can be used as an endpoint for IPC across the network (e.g. \PIPE\ATSVC)
- Process that owns the Named Pipe must have NT AUTHORITY\NETWORK
- OS interrogates the caller's security context
- Widely used; enumerate Named Pipes with Mark Russinovich's Pipelist:

```
C:\Documents and Settings\user\Desktop>pipelist

PipeList v1.01
by Mark Russinovich
http://www.sysinternals.com

Pipe Name                                  Instances      Max Instances
---------                                  ---------      -------------
TerminalServer\AutoReconnect                   1              1
InitShutdown                                   2             -1
lsass                                          3             -1
protected_storage                              2             -1
ntsvcs                                         4             -1
scerpc                                         2             -1
SfcApi                                         2             -1
net\NtControlPipe1                             1              1
net\NtControlPipe2                             1              1
net\NtControlPipe3                             1              1
net\NtControlPipe4                             1              1
Winsock2\CatalogChangeListener-3d8-0           1              1
net\NtControlPipe5                             1              1
net\NtControlPipe0                             1              1
net\NtControlPipe6                             1              1
net\NtControlPipe7                             1              1
atsvc                                          2             -1
```

```
<match name="pipe">
  <if name="state" equal="1" >
    <!-- move back past the \PIPE\ string and two length bytes -->
    <move value="-8" />

    <!--read LSB of PIPE length ; assume max pipe length of 255 (FF)-->
    <read name="pipe_name_len" length="1" />

    <!-- move past second len byte -->
    <move value="1" />

    <!-- decrement the pipe length to account for null byte-->
    <decrement name="pipe_name_len" value="1" />

    <!-- read the full pipe name without null byte -->
    <read name="full_pipe_name" length="$pipe_name_len" />


    <!--read next byte-->
    <read name="check_byte" length="1"/>

    <!--
  this is the "sanity checking" part.  if the byte read is the null byte, we have more assurance we
  just read a complete string, probably for a pipe length
  -->
    <if name="check_byte" equal="&#00;">
      <register name="alert" value="$full_pipe_name" />
    </if>
  </if>
</match>
```


\PIPE\|


|0c 00 \PIPE\
6 + 2 = 8 Bytes


0c 00 \PIPE\atsvc|
2 Bytes
12 – 1 = 11 Bytes


0c 00 \PIPE\atsvc 00
NULL Byte?

0c

00

Named Pipes on the

Alerts (11 items)

pipe_exists (1,473) - \pipe\lsass (1,342) - \pipe\browser (113) - \pipe\srvsvc (13) - \pipe\winreg (9) - \pipe\ntsvcs (4) - \pipe\hello (3) - disco_smb_at_command (2) - \pipe\spoolss (2) - \pipe\atsvc (2) - \pipe\wkssvc (1)

Named Pipes on the

Alerts (11 items)

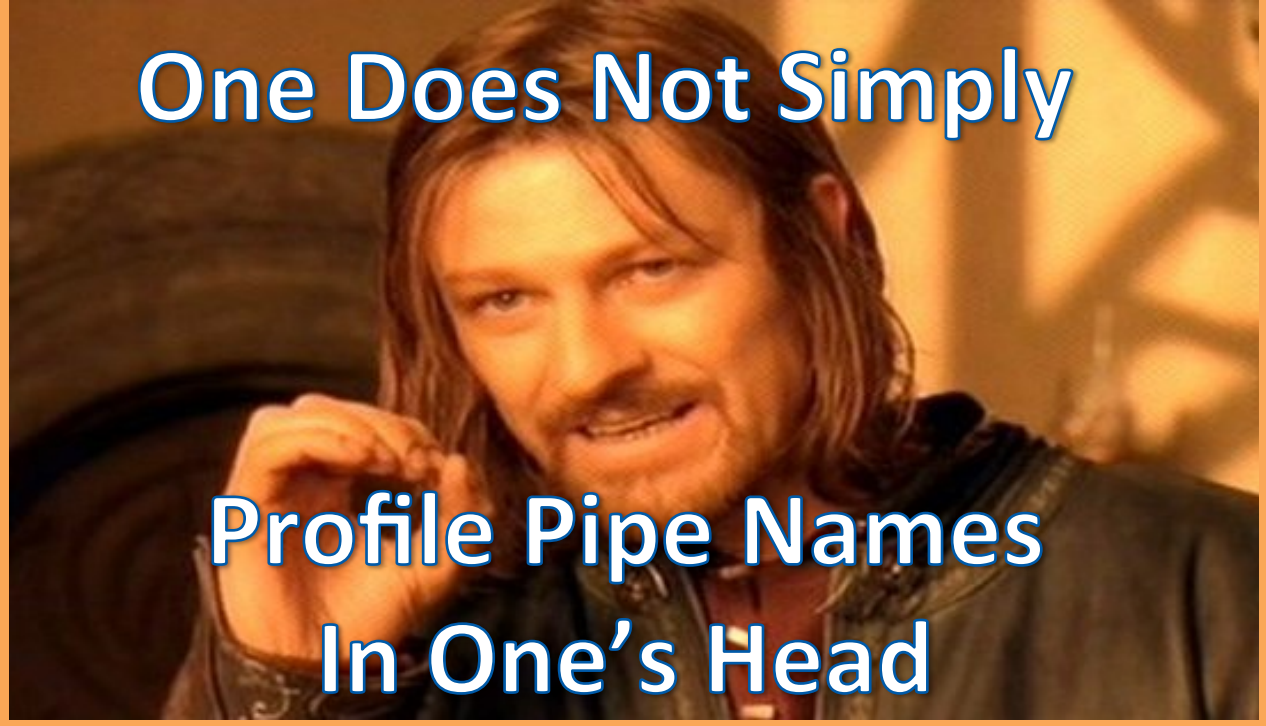
[redacted]3) - \pipe\lsass (1,342) - \pipe\browser (113) - \pipe\srvsvc (13) - \pipe\winreg (9) - \pipe\ntsvcs (4) - \pipe\hello (3) - [redacted]2) - \pipe\spoolss (2) - \pipe\atsvc (2) - \pipe\wkssvc (1)

Named Pipes on the 

Alerts (11 items)

[redacted]3) - \pipe\lsass (1,342) - \pipe\browser (113) - \pipe\srvsvc (13) - \pipe\winreg (9) - \pipe\ntsvcs (4) - \pipe\hello (3) - [redacted]2) - \pipe\spoolss (2) - \pipe\atsvc (2) - \pipe\wkssvc (1)

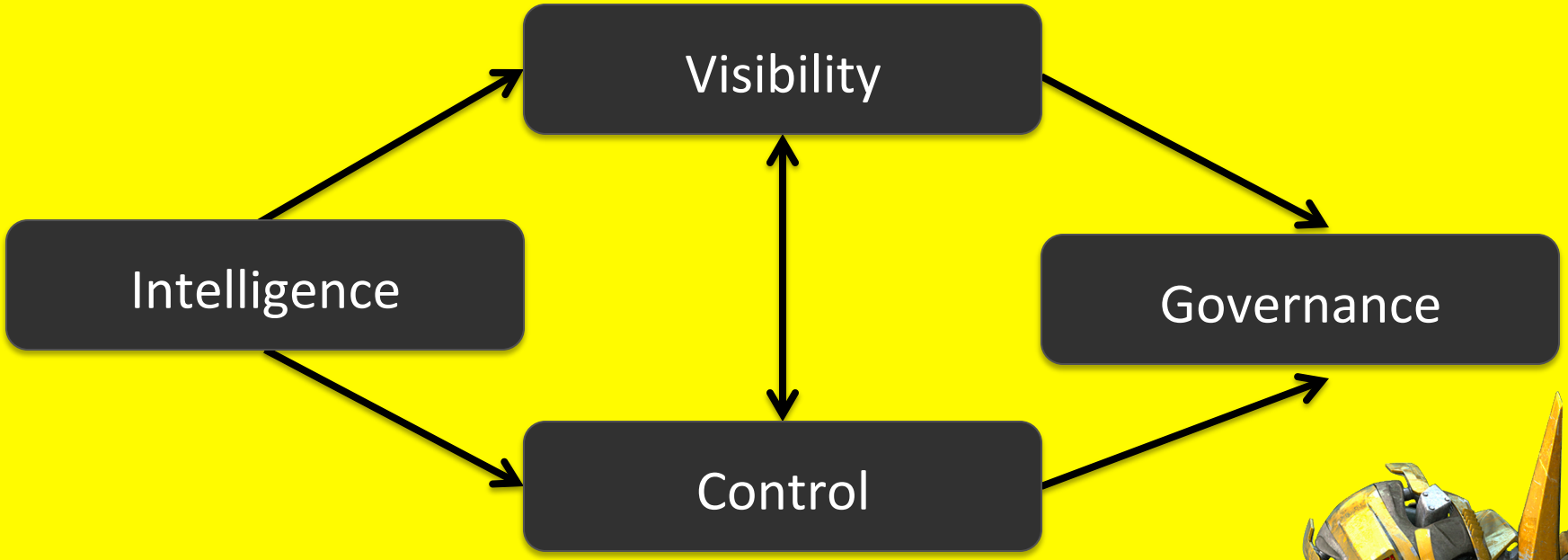
OH HAI DERE!

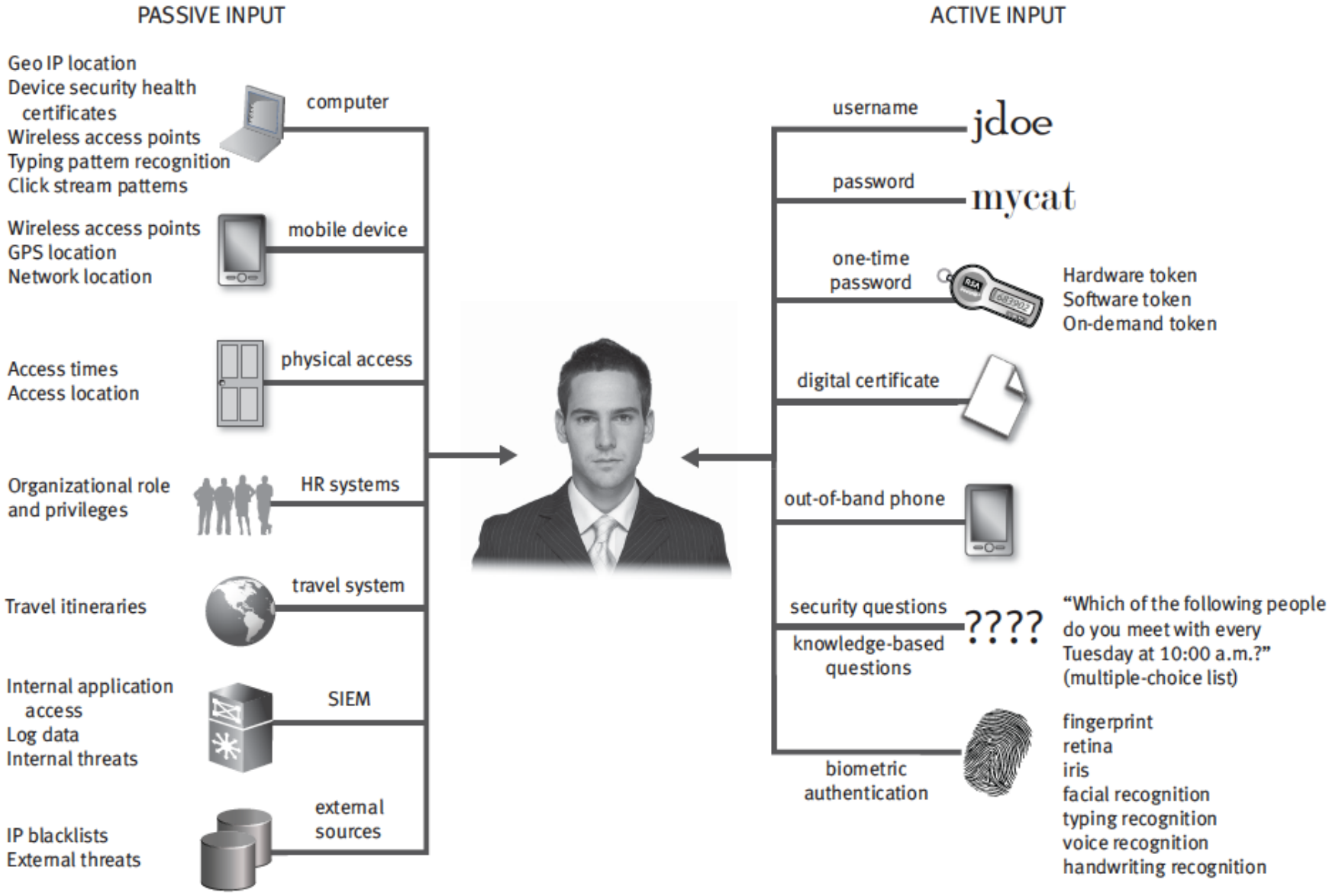


Next Steps:

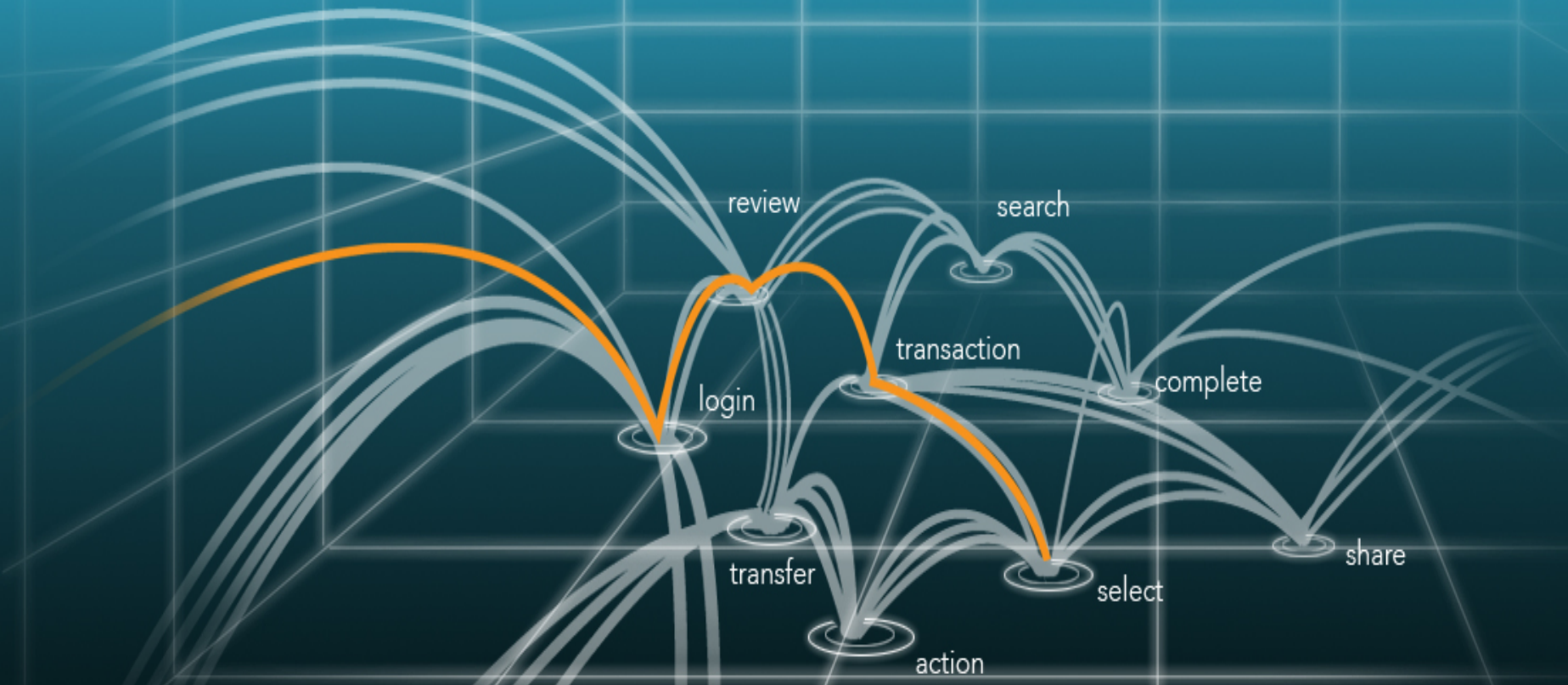
- Whitelists (lsass, samr, netlogon, browser, spoolss, wkssvc, winreg, srvsvc, atsvc, netlogon, sql\query)
- External intel joins (IOCs, etc.)
- What else can we learn from other standard Named Pipes, i.e. detect services configuration.
- UUID & SecondaryAddr mismatch?
- Anonymous Pipes, Other RPC Connection Modalities


Even MORE
Big Data Inside
URGENT


Visibility
Intelligence
Governance
Control

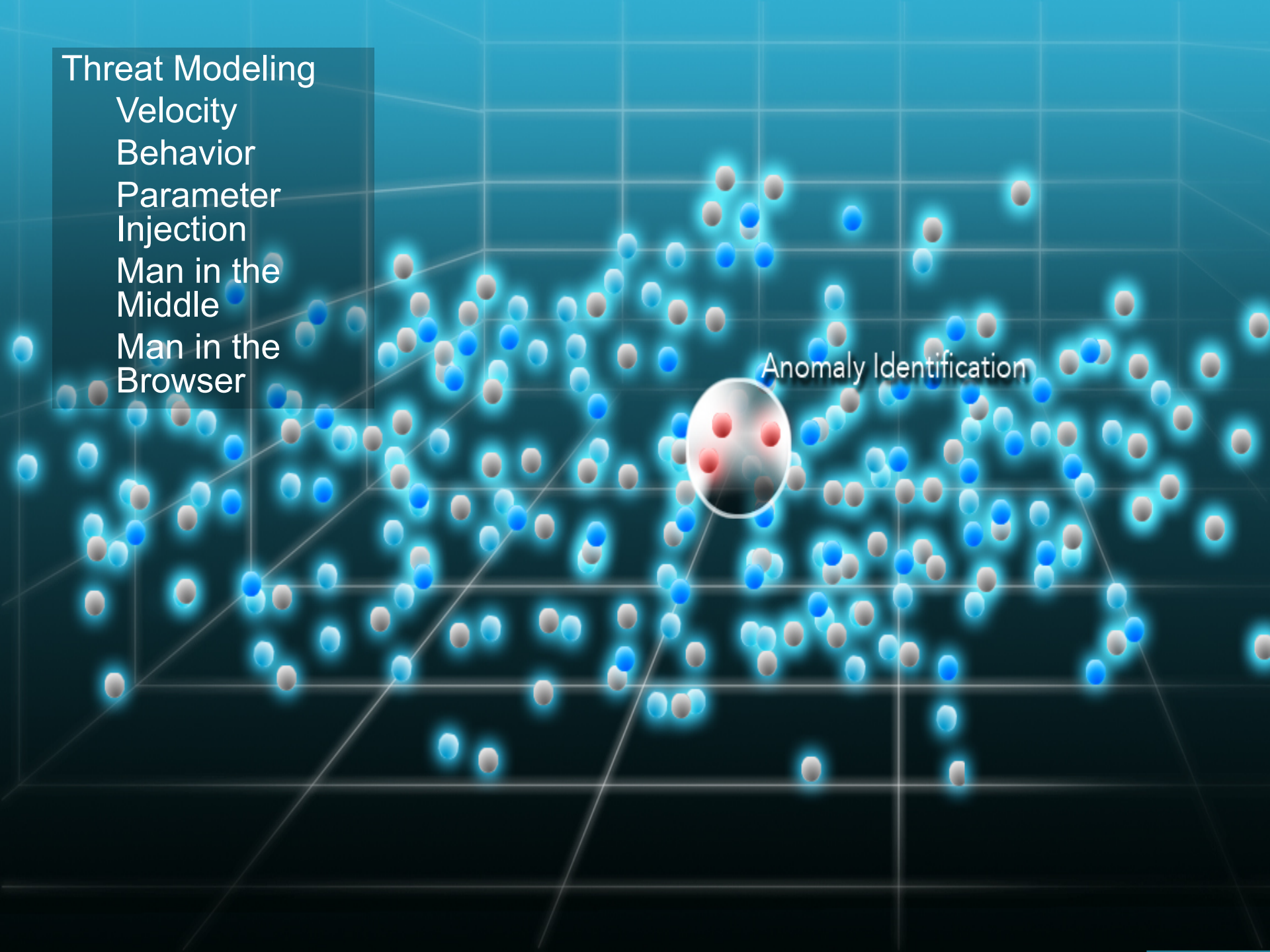

PASSIVE INPUT
ACTIVE INPUT
Geo IP location
Device security health certificates
Wireless access points
Typing pattern recognition
Click stream patterns
computer
Wireless access points
GPS location
Network location
mobile device
Access times
Access location
physical access
Organizational role and privileges
HR systems
Travel itineraries
travel system
Internal application access
Log data
Internal threats
SIEM
IP blacklists
External threats
external sources
username
jdoe
password
mycat
one-time password
Hardware token
Software token
On-demand token
digital certificate
out-of-band phone
security questions
knowledge-based questions
????
"Which of the following people do you meet with every Tuesday at 10:00 a.m.?" (multiple-choice list)
biometric authentication
fingerprint
retina
iris
facial recognition
typing recognition
voice recognition
handwriting recognition

Fraud Prevention

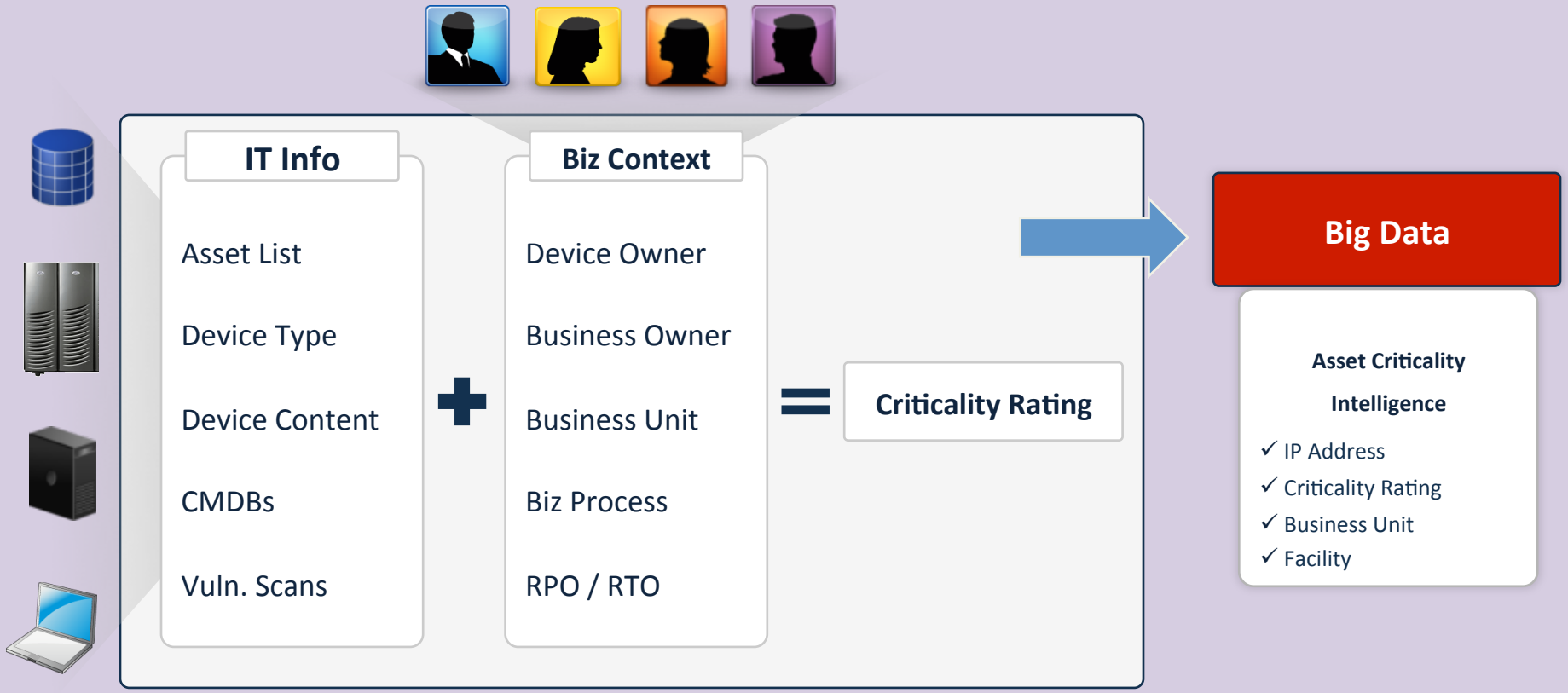


Criminals Look Different than Others..

- Velocity
- Page Sequence
- Origin
- Contextual Information


Threat Modeling
Velocity
Behavior
Parameter Injection
Man in the Middle
Man in the Browser
Anomaly Identification

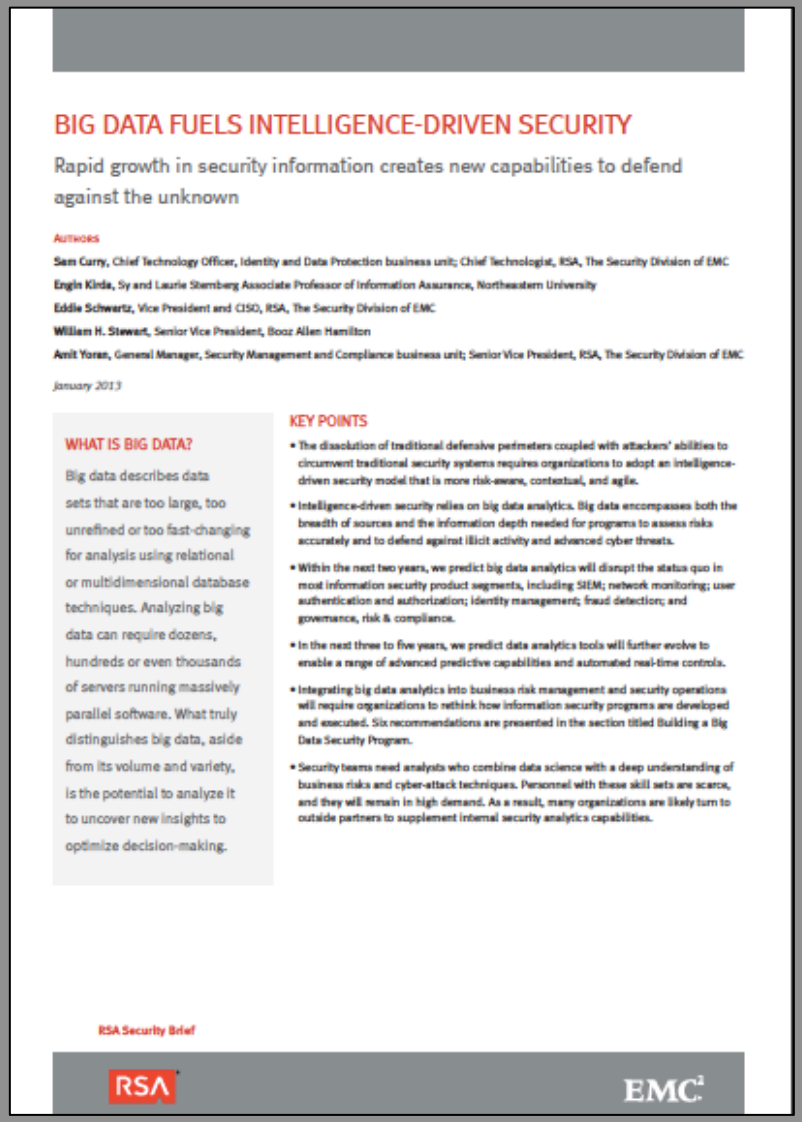

Threat Intelligence
Asset Intelligence
Analyst Prioritizations
Event Capture
Investigations


IT Info
Asset List
Device Type
Device Content
CMDBs
Vuln. Scans
Biz Context
Device Owner
Business Owner
Business Unit
Biz Process
RPO / RTO
Criticality Rating
Big Data
Asset Criticality Intelligence
✓ IP Address
✓ Criticality Rating
✓ Business Unit
✓ Facility

IGNORANCE

Sometimes it's best just not to know.


Big Data
Big Data
Big Data
Big Data
Big Data
Big Data
Big Data
Big Data
Big Data
Big Data?
Big Data?
Big Data
Big Data?
Big Data?
Big Data?
Big Data?
Big Data?
SOPHOS
Security Intelligence



BIG DATA FUELS INTELLIGENCE-DRIVEN SECURITY

Rapid growth in security information creates new capabilities to defend against the unknown

AUTHORS

Sam Curry, Chief Technology Officer, Identity and Data Protection business unit; Chief Technologist, RSA, The Security Division of EMC

Engin Kirda, Sy and Laurie Stemberg Associate Professor of Information Assurance, Northeastern University

Eddie Schwartz, Vice President and CISO, RSA, The Security Division of EMC

William H. Stewart, Senior Vice President, Booz Allen Hamilton

Amit Yoran, General Manager, Security Management and Compliance business unit; Senior Vice President, RSA, The Security Division of EMC

January 2013

WHAT IS BIG DATA?

Big data describes data sets that are too large, too unrefined or too fast-changing for analysis using relational or multidimensional database techniques. Analyzing big data can require dozens, hundreds or even thousands of servers running massively parallel software. What truly distinguishes big data, aside from its volume and variety, is the potential to analyze it to uncover new insights to optimize decision-making.

KEY POINTS

- The dissolution of traditional defensive perimeters coupled with attackers' abilities to circumvent traditional security systems requires organizations to adopt an intelligence-driven security model that is more risk-aware, contextual, and agile.
- Intelligence-driven security relies on big data analytics. Big data encompasses both the breadth of sources and the information depth needed for programs to assess risks accurately and to defend against illicit activity and advanced cyber threats.
- Within the next two years, we predict big data analytics will disrupt the status quo in most information security product segments, including SIEM; network monitoring; user authentication and authorization; identity management; fraud detection; and governance, risk & compliance.
- In the next three to five years, we predict data analytics tools will further evolve to enable a range of advanced predictive capabilities and automated real-time controls.
- Integrating big data analytics into business risk management and security operations will require organizations to rethink how information security programs are developed and executed. Six recommendations are presented in the section titled Building a Big Data Security Program.
- Security teams need analysts who combine data science with a deep understanding of business risks and cyber-attack techniques. Personnel with these skill sets are scarce, and they will remain in high demand. As a result, many organizations are likely turn to outside partners to supplement internal security analytics capabilities.

RSA Security Brief

RSA EMC²

eddie.schwartz@rsa.com

http://www.linkedin.com/in/eddieschwartz/

Thank you!