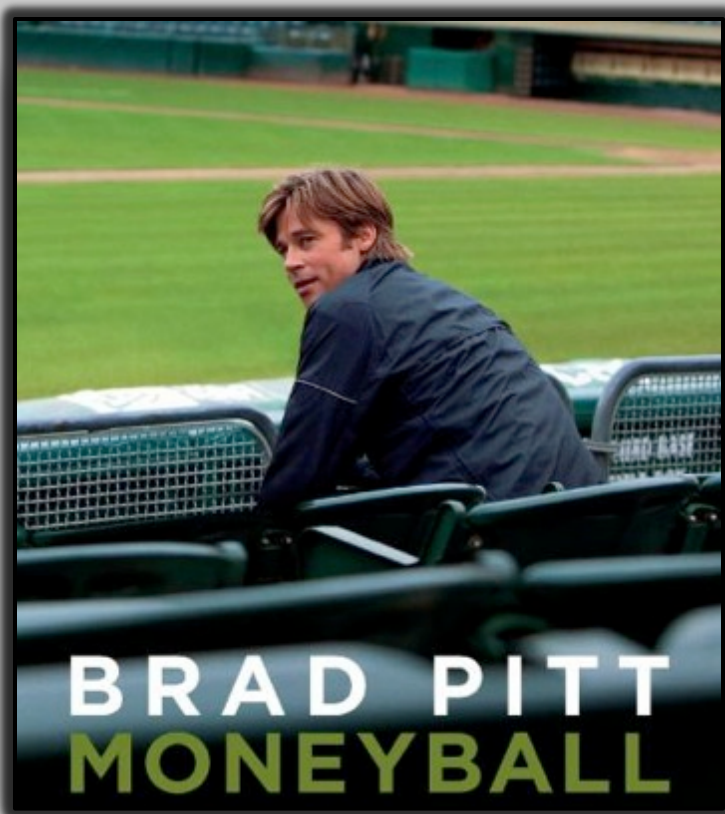


Transforming Your ~~SOC~~ CIRC for Big Data Analytics

Eddie Schwartz
VP/CISO, RSA





.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

Feola	Dustin	491	71	144	30	2	9	60	47	59	1	.294	.380	.491	.791
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
Rodriguez	Alex	555	108	160	30	2	24	104	84	131	14	.288	.385	.523	.916

Giambi

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

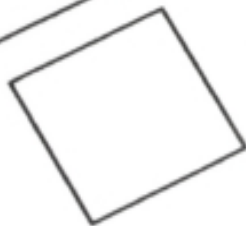
Jeter	Derek	585	110	189	32	4	12	71	59	93	23	.322	.390	.452	.843
Abreu	Bobby	474	95	131	28	2	16	65	86	107	22	.277	.389	.447	.835
Damon	Johnny	548	94	158	30	4	18	73	62	76	14	.289	.362	.458	.821
Cano	Robinson	533	76	164	36	3	16	80	30	65	5	.308	.345	.472	.817
Posada	Jorge	405	65	105	21	1	17	65	65	84	2	.259	.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**



**ISO
27001**

FAIL

UNCERTAINTY

CERTAINTY?

UNCERTAINTY

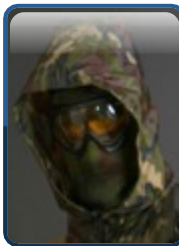
...without much
regard for the distortions that this
causes. We think we want information when
we really want knowledge.

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

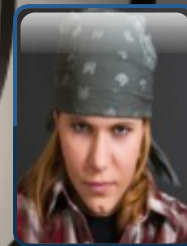
*the signal and the
and the noise and
the noise and the
noise and the no
why so many and
predictions fail—
but some don't th
and the noise and
the noise and the
nate silver noise
noise and the no*



Organized crime



Insiders



Cyber-terrorists /
Hacktivists



Others...

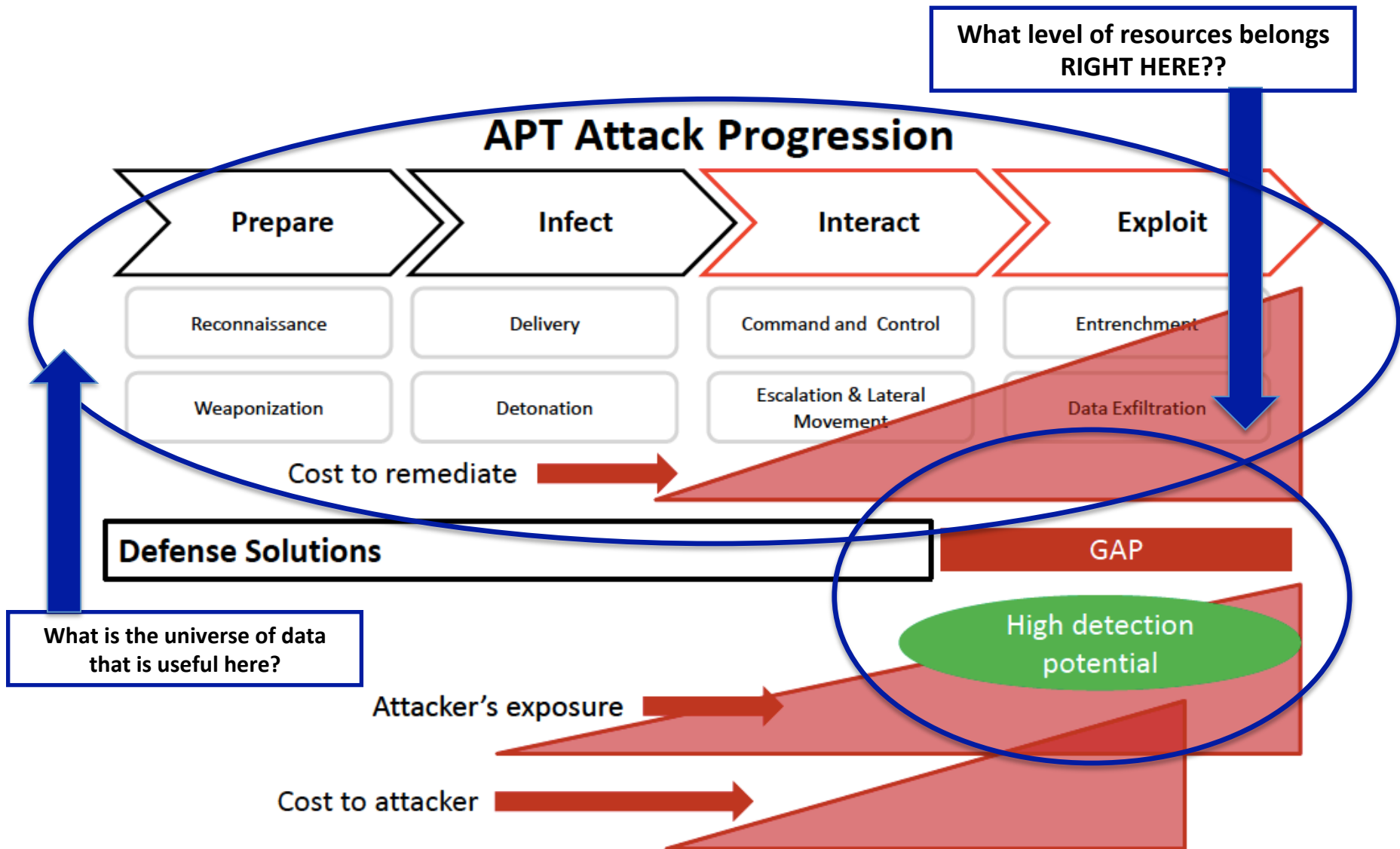


Nation states



f





The Rise of Big Data



- 
1. Security management
 2. Fraud prevention
 3. Identity and access management (IAM)
 4. Governance, risk and compliance (GRC)

**BIG DATA
TRANSFORMS
SECURITY**

Requirements for Big Data

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

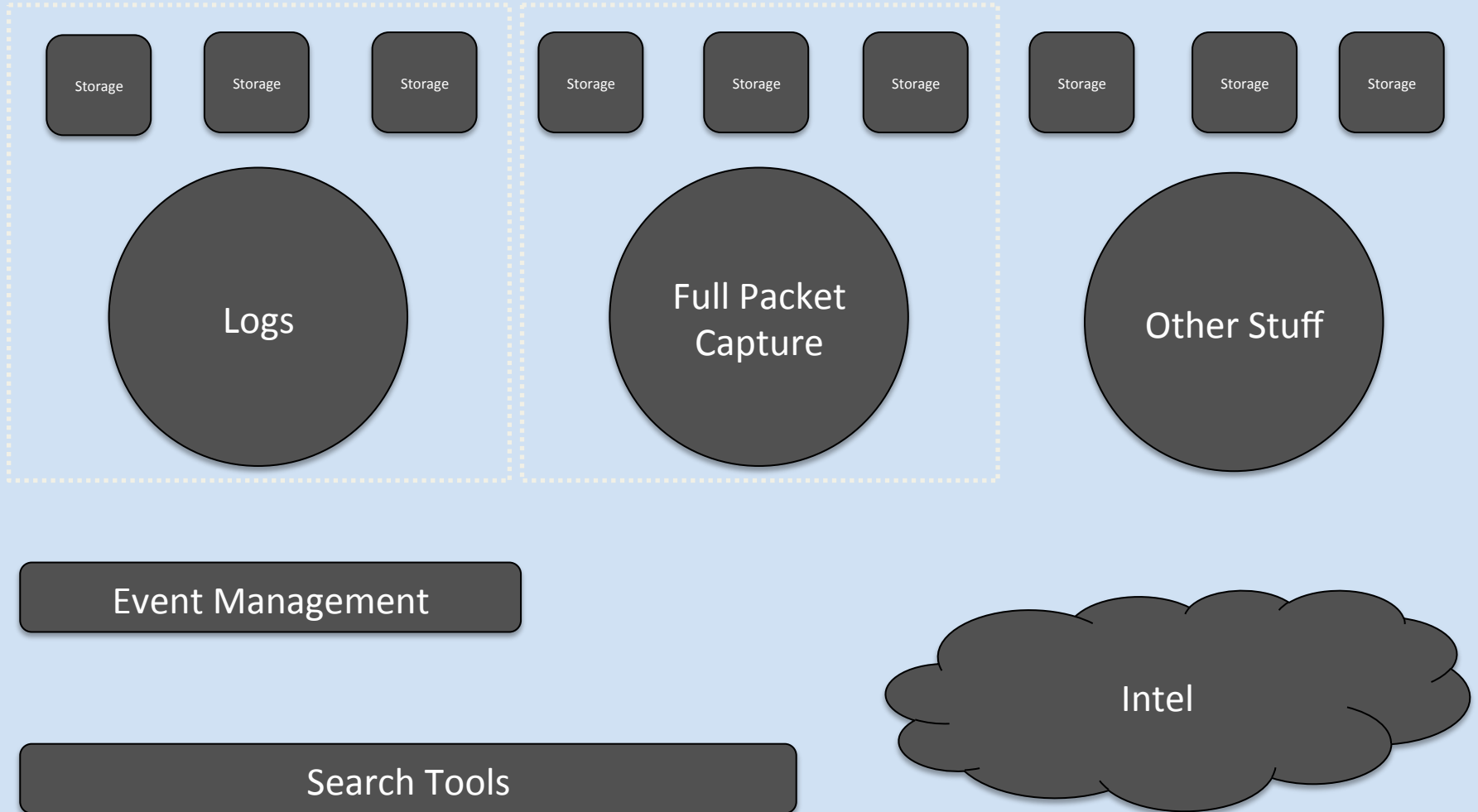
**I don't always like
uncertainty**



**But when I do, I want
BIG DATA Analytics**


memecreator.com

$A \cap B$, etc.



SIEM





SECURITY ANALYTICS

DISTRIBUTED COLLECTION

EUROPE



NORTH AMERICA



ASIA



REAL-TIME

WAREHOUSE



Months/Years

LONG-TERM

FLEXIBLE INTEGRATION (API)

THE ANALYTICS

Reporting and
Alerting

Investigation

Malware
Analytics

Administration

Complex Event
Processing

Free Text
Speech

Correlation

Metadata
Tagging

Incident
Management

Asset
Criticality

Compliance

LIVE INTELLIGENCE

Threat Intelligence – Rules – Parsers – Alerts – Feeds – Apps – Directory Services – Reports and Custom Actions

	SOC	CIRC
Tasks	<ul style="list-style-type: none"> • Tool Administration • Vulnerability Scanning • Tier 1 Event Support • Break-Fix 	<ul style="list-style-type: none"> • Incident Investigation • Threat Intelligence • Malware Analytics • Response Coordination
Skill set required	<ul style="list-style-type: none"> • Intermediate security knowledge • Good tool & process knowledge • Generic company knowledge 	<ul style="list-style-type: none"> • Deep threat knowledge • Advanced technical capability • Investigative experience • Deep company knowledge
Bottom Line	• Waiting for a smack on the forehead	• Hunting bad guys

	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

What Level is Required for You?

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

One does not simply walk into



intelligence-driven security



RSA SecurID Style Attack

ALERT!!!... Suspect Network Traffic

IP Address shows multiple connections tunneled over non-standard port

1



Authorized User Logged in to AD

AD Logs drill-down show user logged in from suspect IP with authorized credentials

2



3

Different user from same IP/Host logged into development test server, then the corporate file server

VPN & Host logs show a different set of authorized credentials used to log into VPN and multiple internal servers

4



Data ex-filtration

Encrypted ZIP file transferred out to Internet via FTP server



You Need to Understand EVERYTHING About the Attack...

Attack Step	Traditional SIEM	Security Analytics
Alert for access over non-standard port	No	Yes
Recreate activity of suspect IP address across environment	No	Yes
Show user activity across AD and VPN	Yes	Yes
Alert for different credentials used for AD and VPN	Yes	Yes
Reconstruct exfiltrated data	No	Yes

Understanding Potential Campaigns

Find compromised Server or Workstation acting as SPAM host

Multiple outbound SMTP connections from workstation.
Multiple internet DNS connections from workstation

1



Find out how the workstation got infected

User clicked on the link and got infected by Trojan from drive-by download.

2



Analyze malware

Determine whether targeted or vanilla malware in use

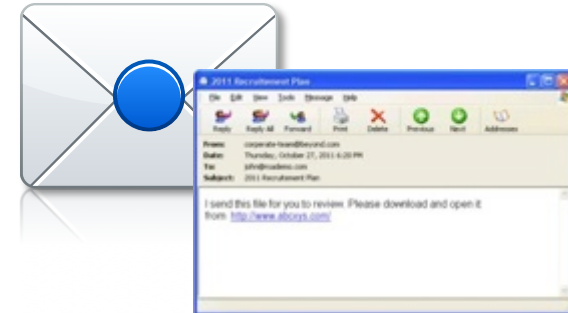
4



Recreate phishing e-mail message

Determine whether targeted phishing attack at play

3

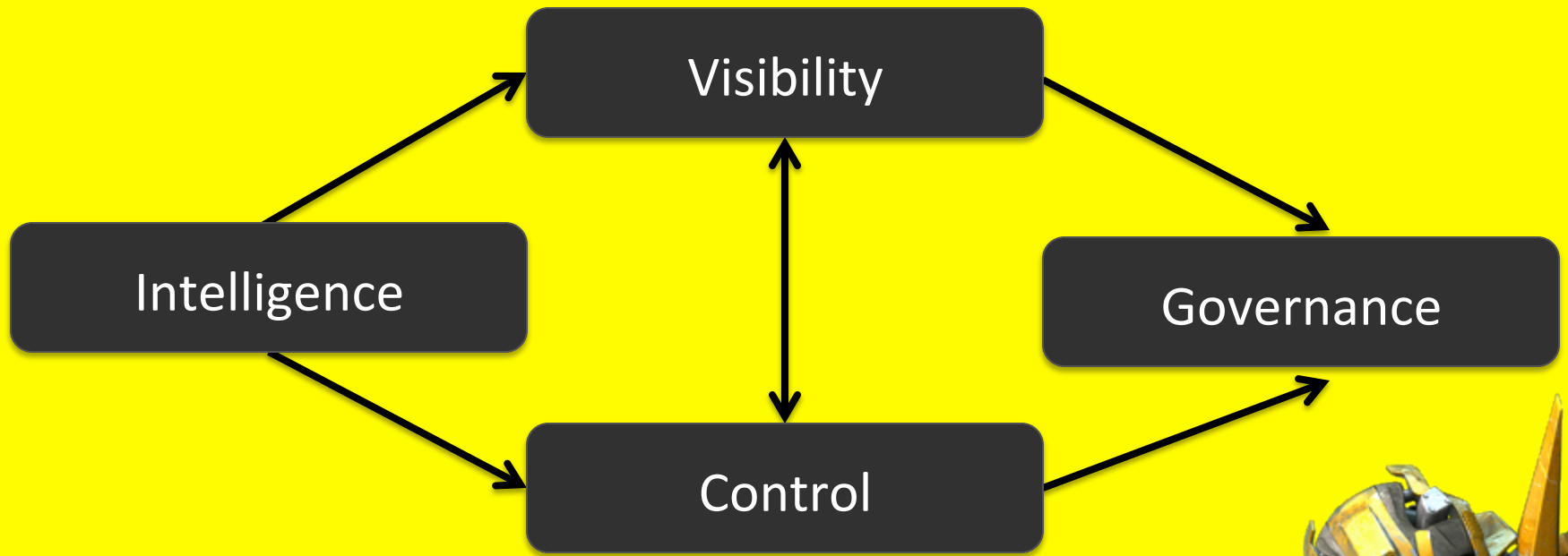


Big Data and Security Analytics Help Determine If This Is A Targeted Attack

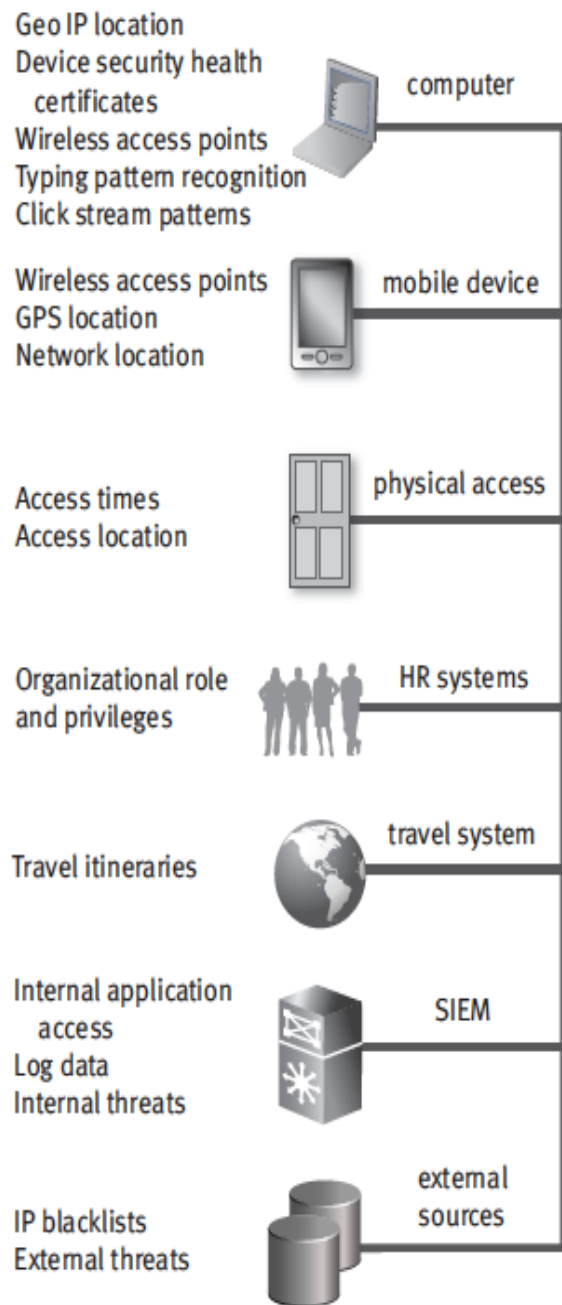
Attack Step	Traditional SIEM	Security Analytics
Alert for suspected SPAM host	Yes	Yes
Show all WWW requests where executable downloaded	No	Yes
Recreate email with suspect link	No	Yes
Analyze malware and incorporate community intelligence	No	Yes
Determine whether attack is part of a targeted campaign	No	Yes

**Even MORE
Big Data Inside**

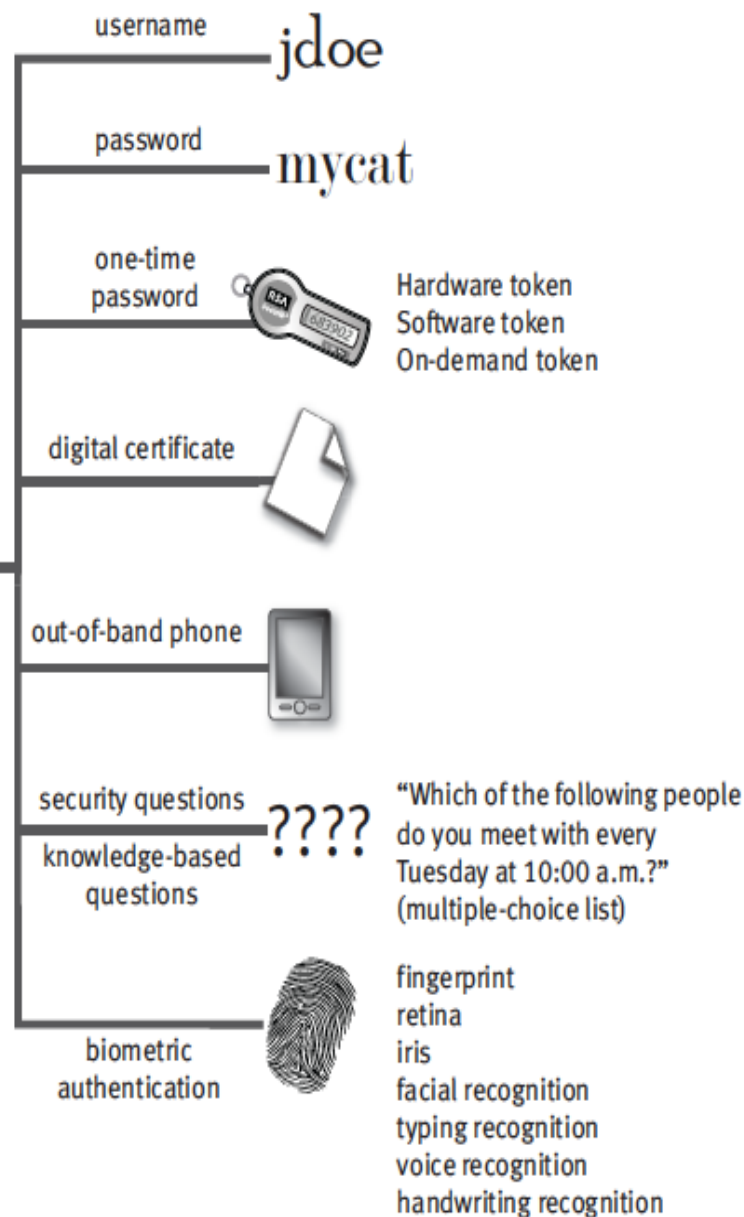
URGENT



PASSIVE INPUT

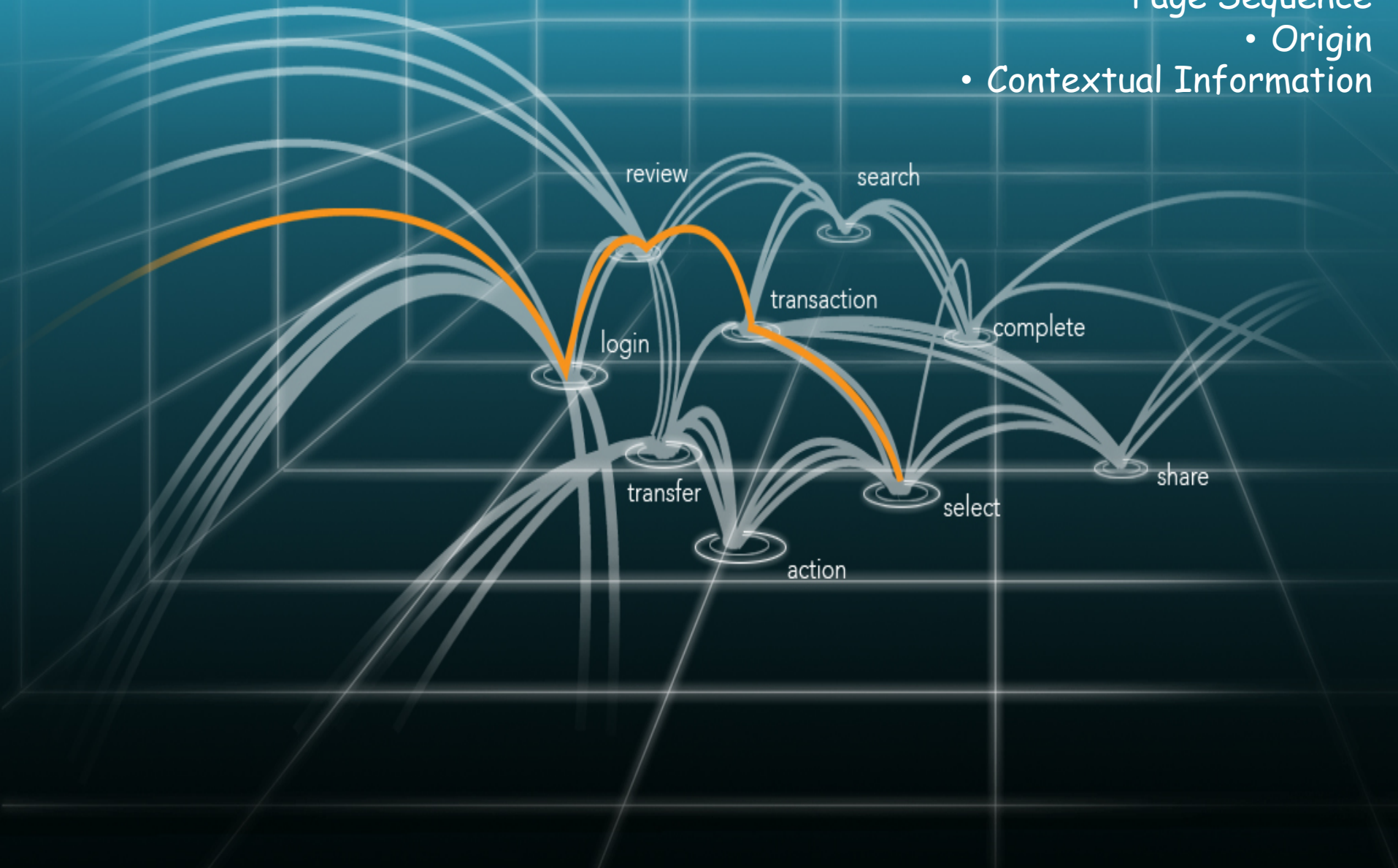


ACTIVE INPUT



Criminals Look Different than Others..

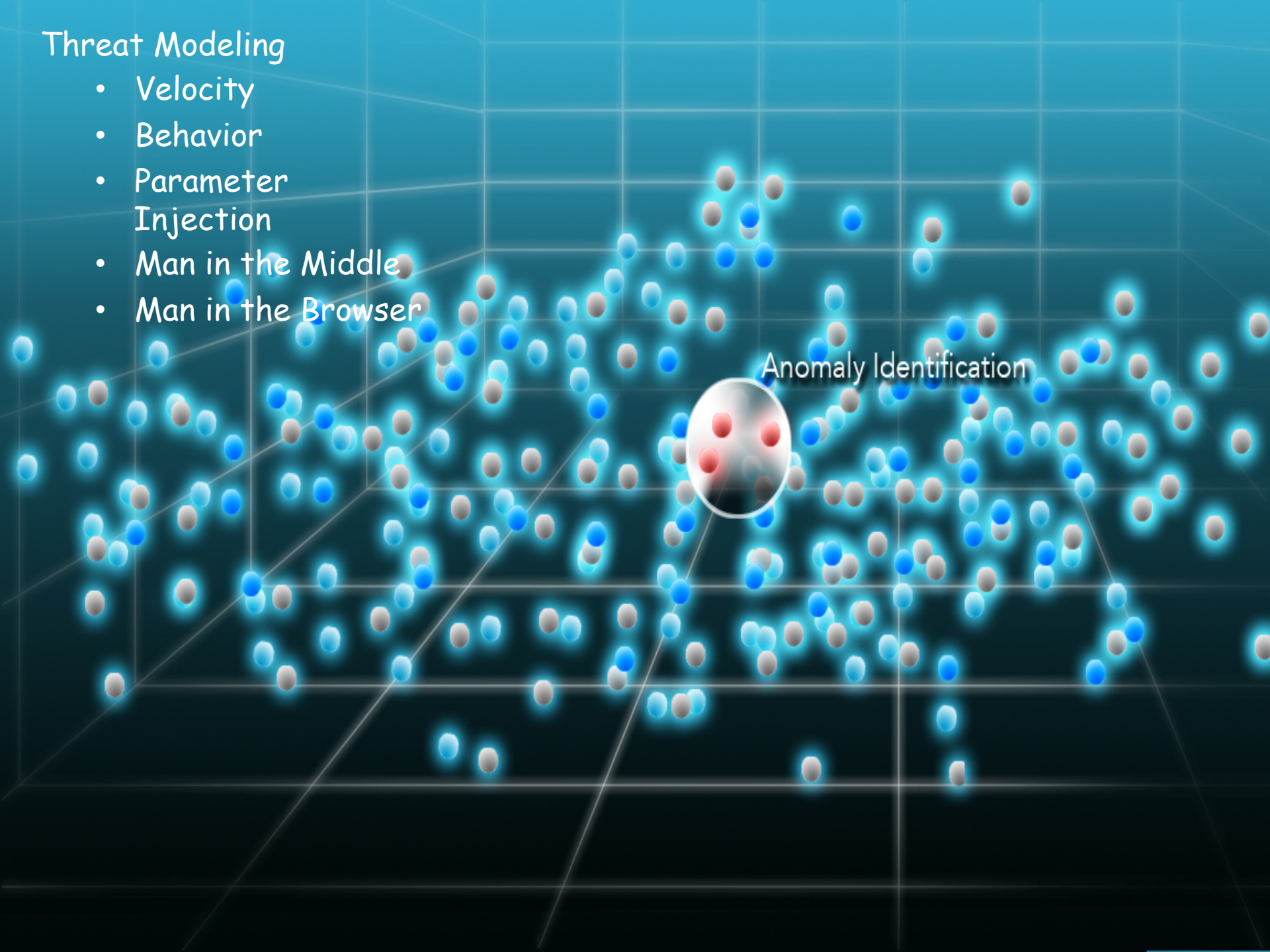
- Velocity
- Page Sequence
- Origin
- Contextual Information



Threat Modeling

- Velocity
- Behavior
- Parameter Injection
- Man in the Middle
- Man in the Browser

Anomaly Identification





Investigations

Asset Intelligence

**IT/ Analyst
Prioritizations**

Event Focus

**Threat
Intelligence**



IT Info

Asset List
Device Type
Device Content
CMDBs
Vuln. Scans

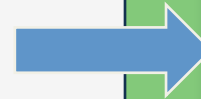


Biz Context

Device Owner
Business Owner
Business Unit
Biz Process
RPO / RTO



Criticality Rating



Big Data

Asset Criticality Intelligence

- ✓ IP Address
- ✓ Criticality Rating
- ✓ Business Unit
- ✓ Facility

“When forecasters ignore data, it’s a clear sign they’d rather ignore the truth that makes accurate predictions.”

- Nate Silver

The Signal and the Noise

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 Sternberg 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

Avrit 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



EMC²

eddie.schwartz@rsa.com
<http://www.linkedin.com/in/eddieschwartz/>

Thank you!