Security Analytics: The Game is On

Andrew Plato, CEO, Anitian

Professional Techniques – T22


ANITIAN
SECURITY ANALYTICS
THE GAME IS ON

Meet the Speaker – Andrew Plato

- President / CEO of Anitian
- Principal at TrueBit CyberPartners
- 20+ years of experience in security
- Discovered SQL injection in 1995
- Helped develop first in-line IPS engine (BlackICE)

ANITIAN

Vision: *Security makes the world a better place.*

Mission: *Build great security leaders.*

RiskNow®

Rapid Risk Assessment

VisionPath

Compliance Assessment

RING.ZERO

Next-Generation Penetration Testing

SHERLOCK

Managed Threat Intelligence

Overview

Intent

- Define *Security Analytics* market and technologies
- Provide insight into the current and future of Security Analytics

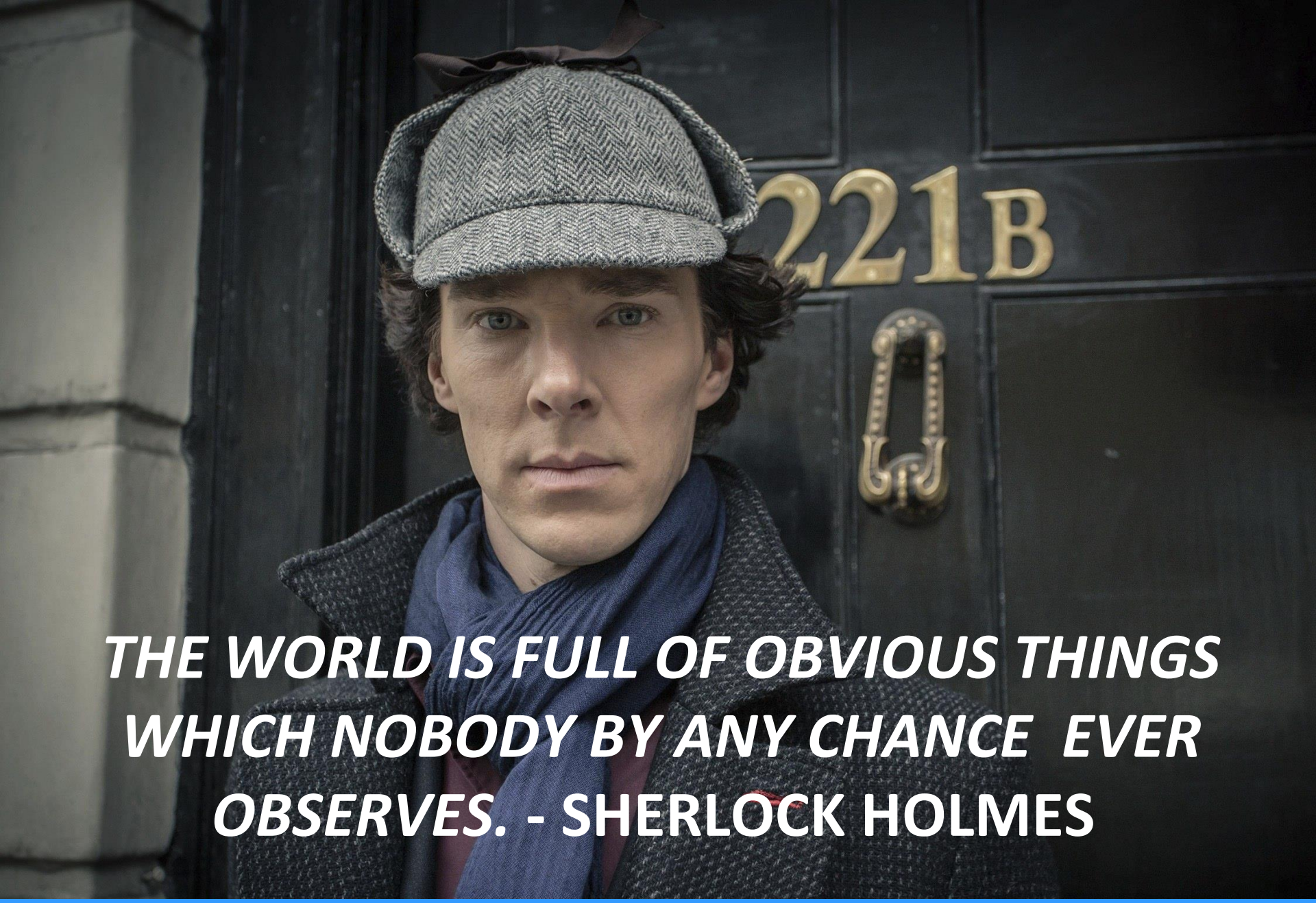
Outline

- Introduction
- What is Threat Intelligence
- Inside Security Analytics
- Deploying Security Analytics

Premises & Assumptions

- This is a *very* nascent market
- Our data comes from research beginning in 2014
- We do not sell products
- Security Analytics is a combination of many technologies coalescing into a market


INTRODUCTION



THE WORLD IS FULL OF OBVIOUS THINGS WHICH NOBODY BY ANY CHANCE EVER OBSERVES. - SHERLOCK HOLMES

We Know the Problem

- Vulnerabilities are widespread
- Detection and attribution are difficult
- The data are gigantic
- Technologies are only as good as the users
- Competing priorities within SecOps, Development, Sysadmin, etc.
- Breaches are accelerating

The Failure of AV

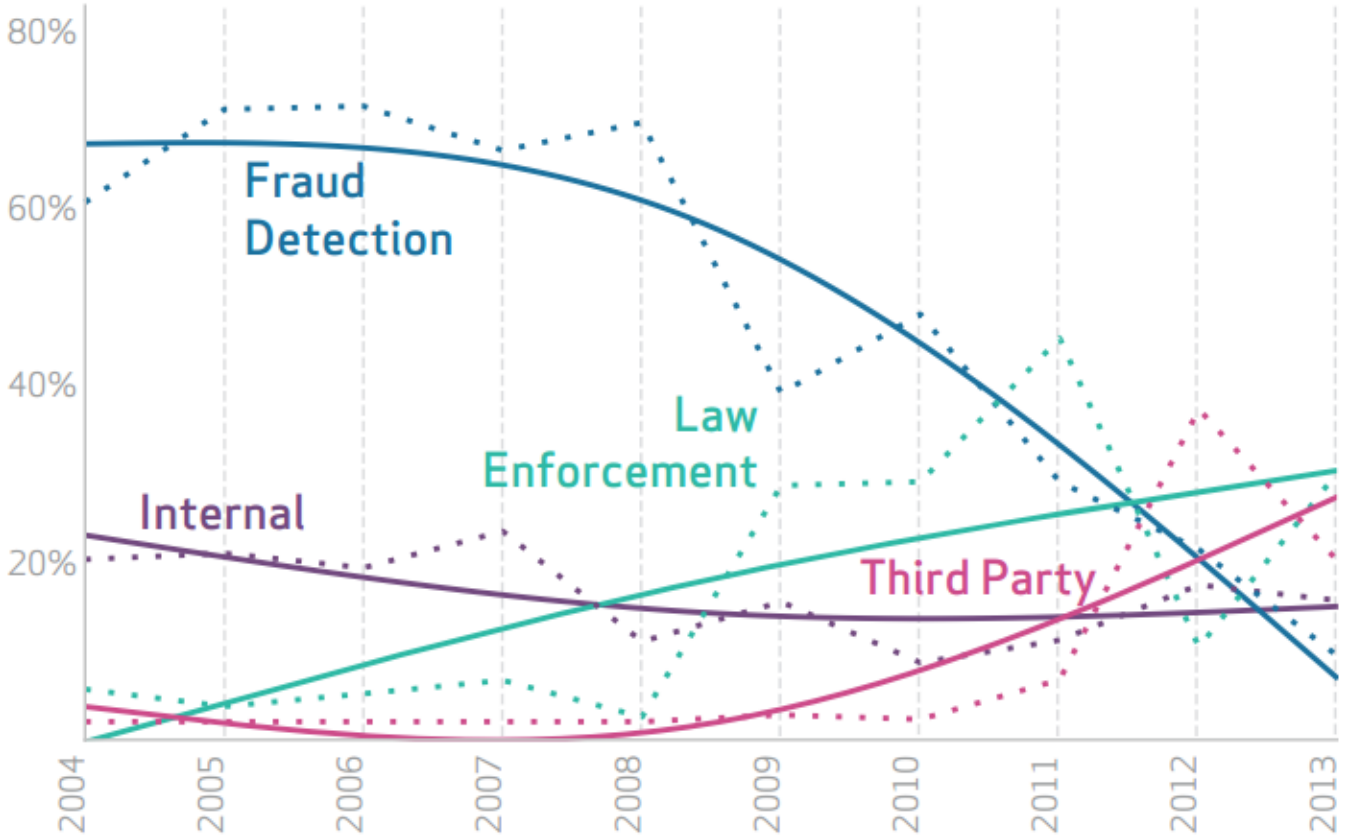
- Current AV is profoundly bad at detecting emerging threats
- Most AVs can only manage about 95% effective
- That 5% remaining is huge
- Symantec's own VP admitted that "AV is dead!"

The Failure of SIEM

- Big data
- Big complexity
- Most SIEM deployments are strictly to satisfy compliance requirements
- Immense barriers to *operationalization*

Failure of Incident Response

Figure 14.
Breach discovery methods over time



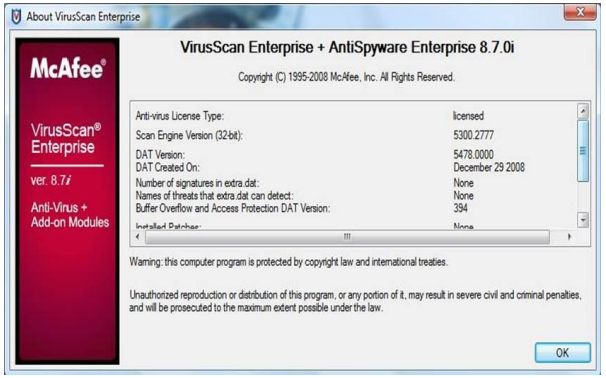
Verizon Data Breach Report - 2014

Failure of Incident Response

- Third parties are increasingly notifying organizations of their breach
- Nobody is watching the data, because there is too much of it
- Alerts go ignored, because there are too many of them
- Data is unavailable when there is a breach, because systems were never configured correctly

Data data data

SIEM



ENDPOINT

SANDBOX

NGFW

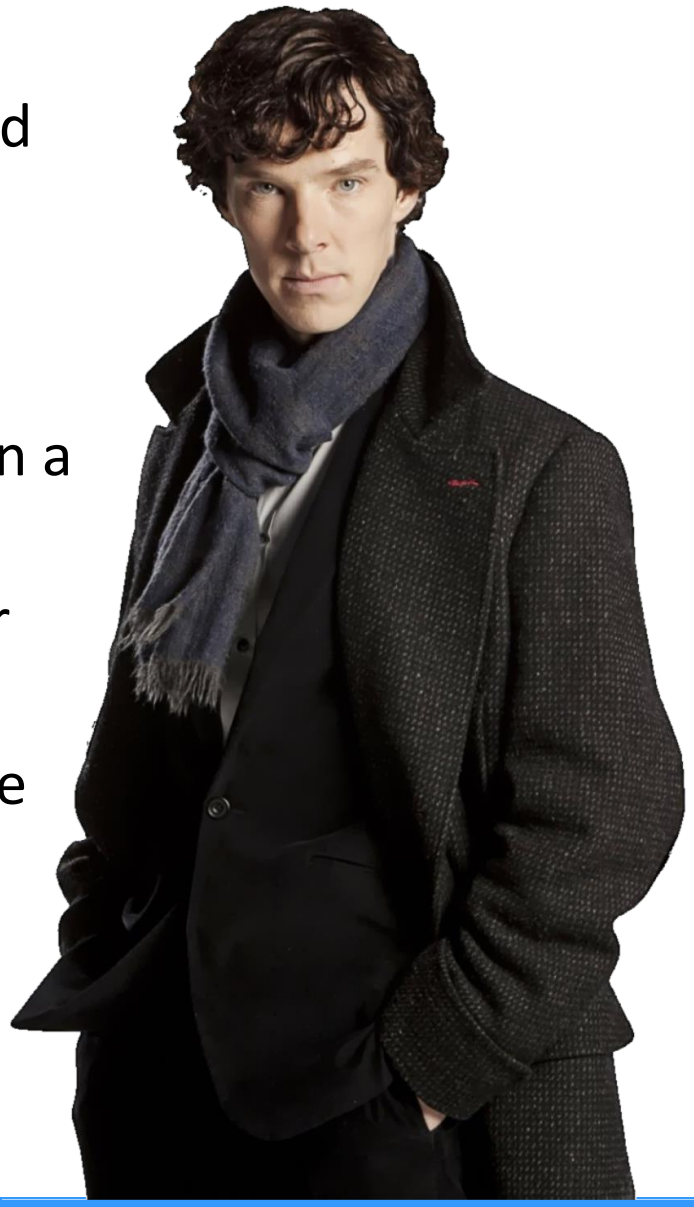
PACKET CAPTURE

VULNERABILITY MANAGEMENT


FUMBLING
IN THE DARK

We Need a Cyber-Sherlock

- Intelligence about the attacks, tactics, and targets
- Tools that can quickly differentiate an attack from noise
- Big data cruncher, that finds the needle in a stack of needles
- Incident handlers that can piece together the crime
- Processes that fuels faster, more accurate decision making and response
- This is security analytics…
  … sort of




WHAT IS THREAT
INTELLIGENCE?

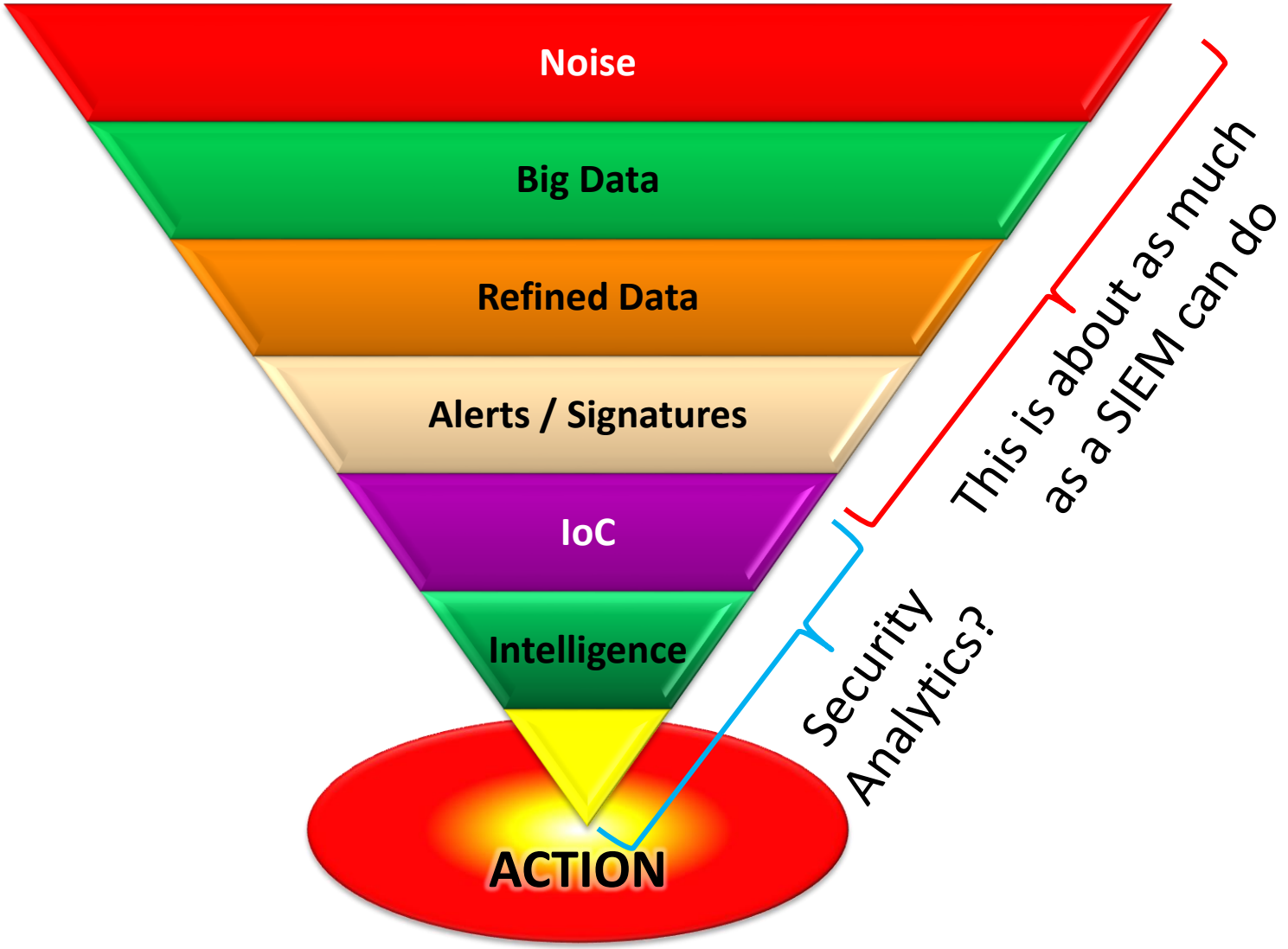
Elementary Threat

- A threat is something bad that *might* happen.
- Threat elements:

Motive:	A reason for that bad thing to exist
Capability:	Means to happen
Opportunity:	Weakness that enables the threat to happen

- Motive is not always malicious
- Capability is not always obvious
- Opportunity is the thing you have most control over
- Threat intelligence analyzes data in the context of these three elements

Where Does Threat Intelligence Come From?



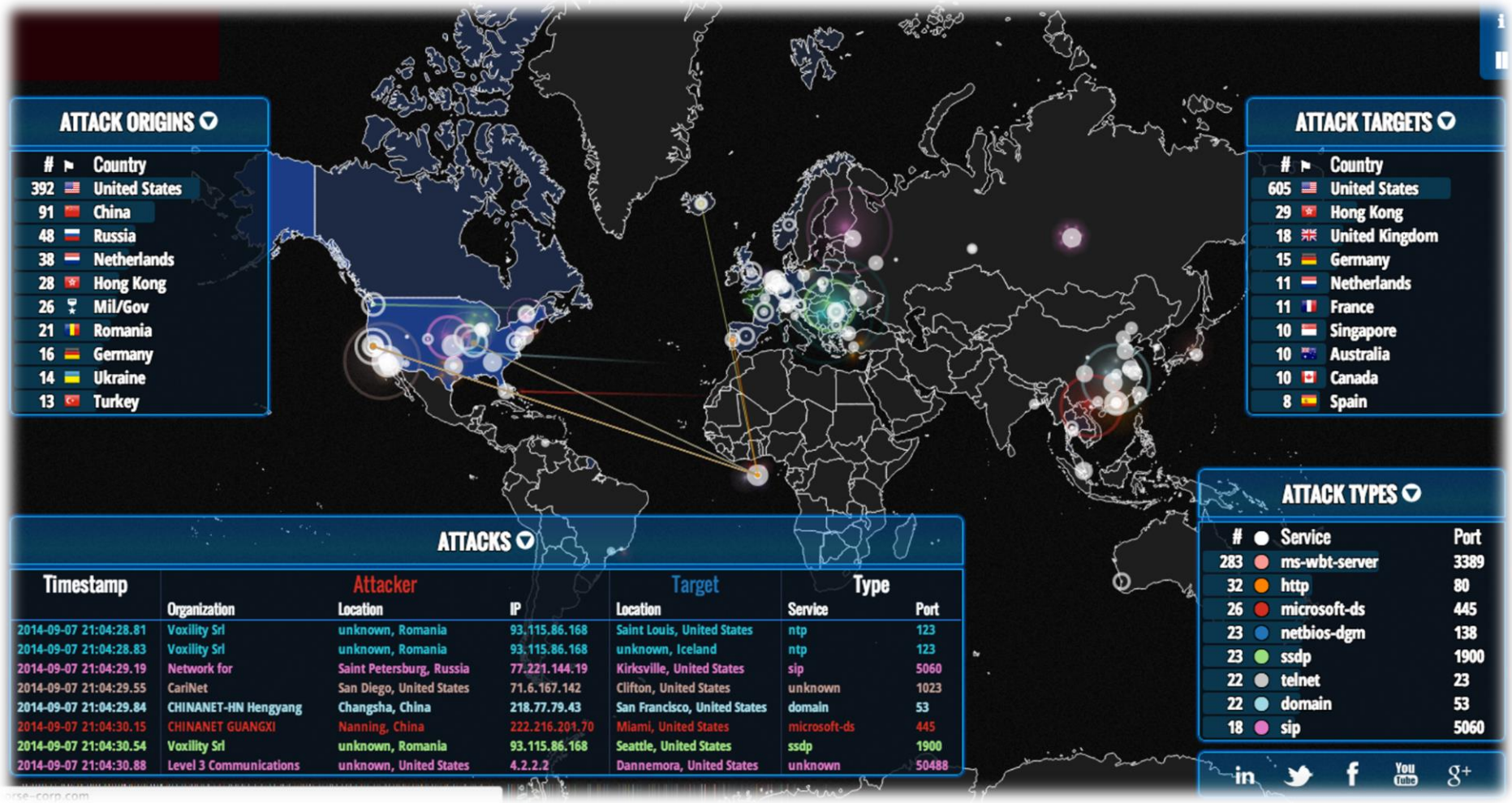
So What is Threat Intelligence, Really?

- Data, to help tune, optimize, or direct your security analytics
- Diverse sources: commercial, government, open source
- Diverse types: IoC, reputation, tactics
- Standards:
  - STIX: Structured Threat Information Expression
  - TAXII: Trusted Automated Exchange of Indicator Information

STIX Example

```
<stix:Observables cybox_major_version="1" cybox_minor_version="1">
    <cybox:Observable id="example:observable-c8c32b6e-2ea8-51c4-6446-7f5218072f27">
        <cybox:Object id="example:object-d7fcce87-0e98-4537-81bf-1e7ca9ad3734">
            <cybox:Properties xsi:type="AddressObject:AddressObjectType" category="ipv4-addr">
                <AddressObject:Address_Value>198.51.100.2</AddressObject:Address_Value>
            </cybox:Properties>
        </cybox:Object>
    </cybox:Observable>
    <cybox:Observable id="example:observable-b57aa65f-9598-04fb-a9d1-5094c36d5dc4">
        <cybox:Object id="example:object-f4fac80a-1239-47cc-b0e6-771b1a73f817">
            <cybox:Properties xsi:type="AddressObject:AddressObjectType" category="ipv4-addr">
                <AddressObject:Address_Value>198.51.100.17</AddressObject:Address_Value>
            </cybox:Properties>
        </cybox:Object>
    </cybox:Observable>
    <cybox:Observable id="example:observable-19c16346-0eb4-99e2-00bb-4ec3ed174cac">
        <cybox:Object id="example:object-174bf9a3-f163-4919-9119-b52598f97ce3">
            <cybox:Properties xsi:type="AddressObject:AddressObjectType" category="ipv4-addr">
                <AddressObject:Address_Value>203.0.113.19</AddressObject:Address_Value>
            </cybox:Properties>
        </cybox:Object>
    </cybox:Observable>
</stix:Observables>
<stix:TTPs>
    <stix:TTP xsi:type="ttp:TTPType" id="example:ttp-dd955e08-16d0-6f08-5064-50d9e7a3104d" timestamp="2014-02-20T09:00:00.000000Z">
        <ttp:Title>Malware C2 Channel</ttp:Title>
        <ttp:Resources>
            <ttp:Infrastructure>
                <ttp:Type>Malware C2</ttp:Type>
                <ttp:Observable_Characterization cybox_major_version="2" cybox_minor_version="1">
                    <cybox:Observable idref="example:observable-c8c32b6e-2ea8-51c4-6446-7f5218072f27"/>
                    <cybox:Observable idref="example:observable-b57aa65f-9598-04fb-a9d1-5094c36d5dc4"/>
                    <cybox:Observable idref="example:observable-19c16346-0eb4-99e2-00bb-4ec3ed174cac"/>
                </ttp:Observable_Characterization>
            </ttp:Infrastructure>
        </ttp:Resources>
    </stix:TTP>
</stix:TTPs>
```

This is NOT Threat Intelligence



This is eyecandy

The Problem

- Threat intelligence is highly specialized data
- It is not a product, per se
- It must be consumed and put into context
- A person and/or technology must consume and use the intelligence to find the actual evidence of compromise
- Integrating threat intelligence is both a *technical* challenge and *operational* challenge
- Wargames dashboards are meaningless
- The data are complex, difficult to use
- Executives will not understand this

Security Analytics is Here (Mostly)

Technical Advances

- Detect anywhere, defend everywhere
- Integrated platforms
- More sharing (STIX/TAXII and such)

Detection Improvements

- Advanced detections and AI
- Automated intelligence reactions

Human Intelligence

- Move from enforcement, to analysis
- Focus on operationalizing security
- Improved work-flow management

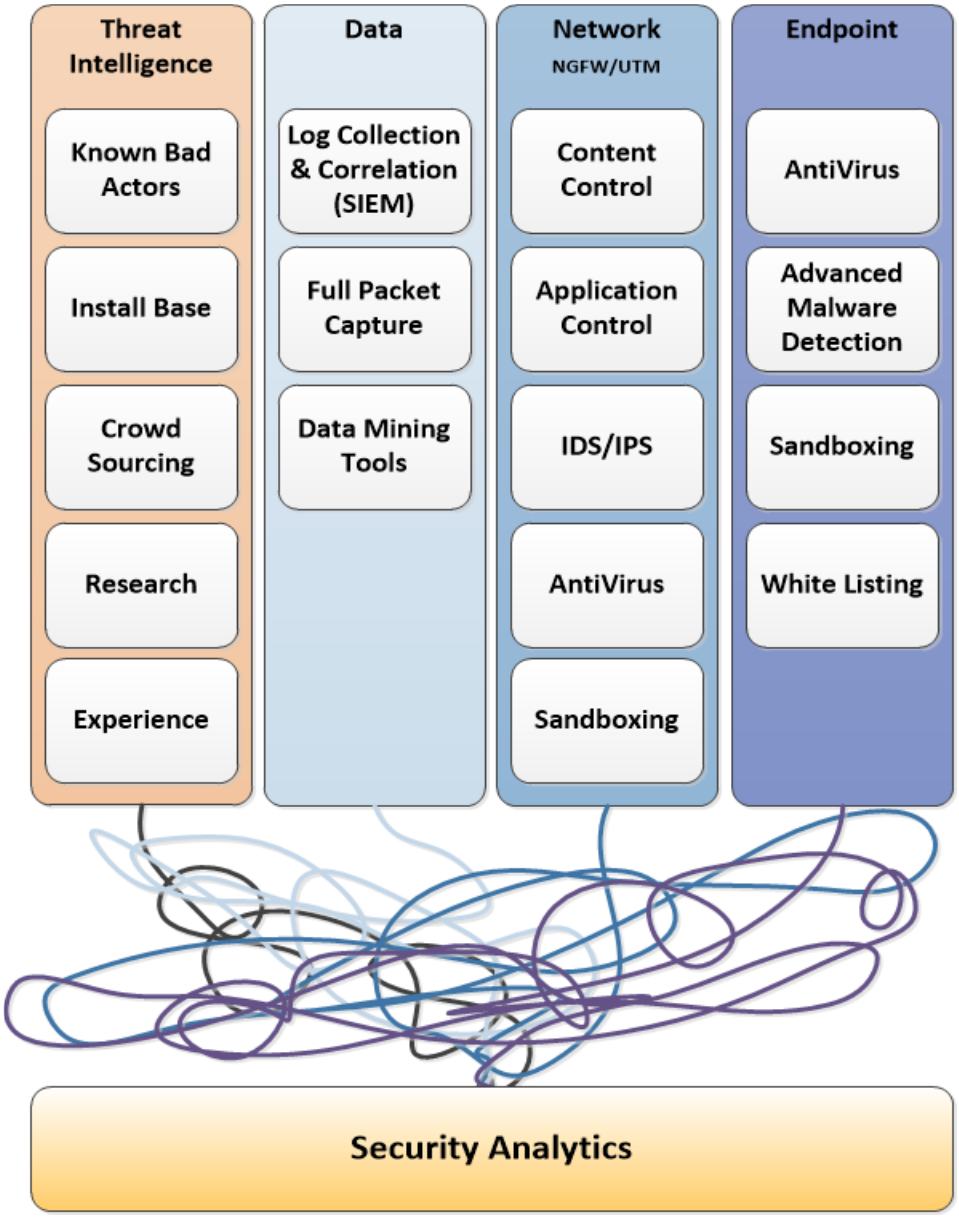

WHAT IS SECURITY
ANALYTICS?

What is Security Analytics?

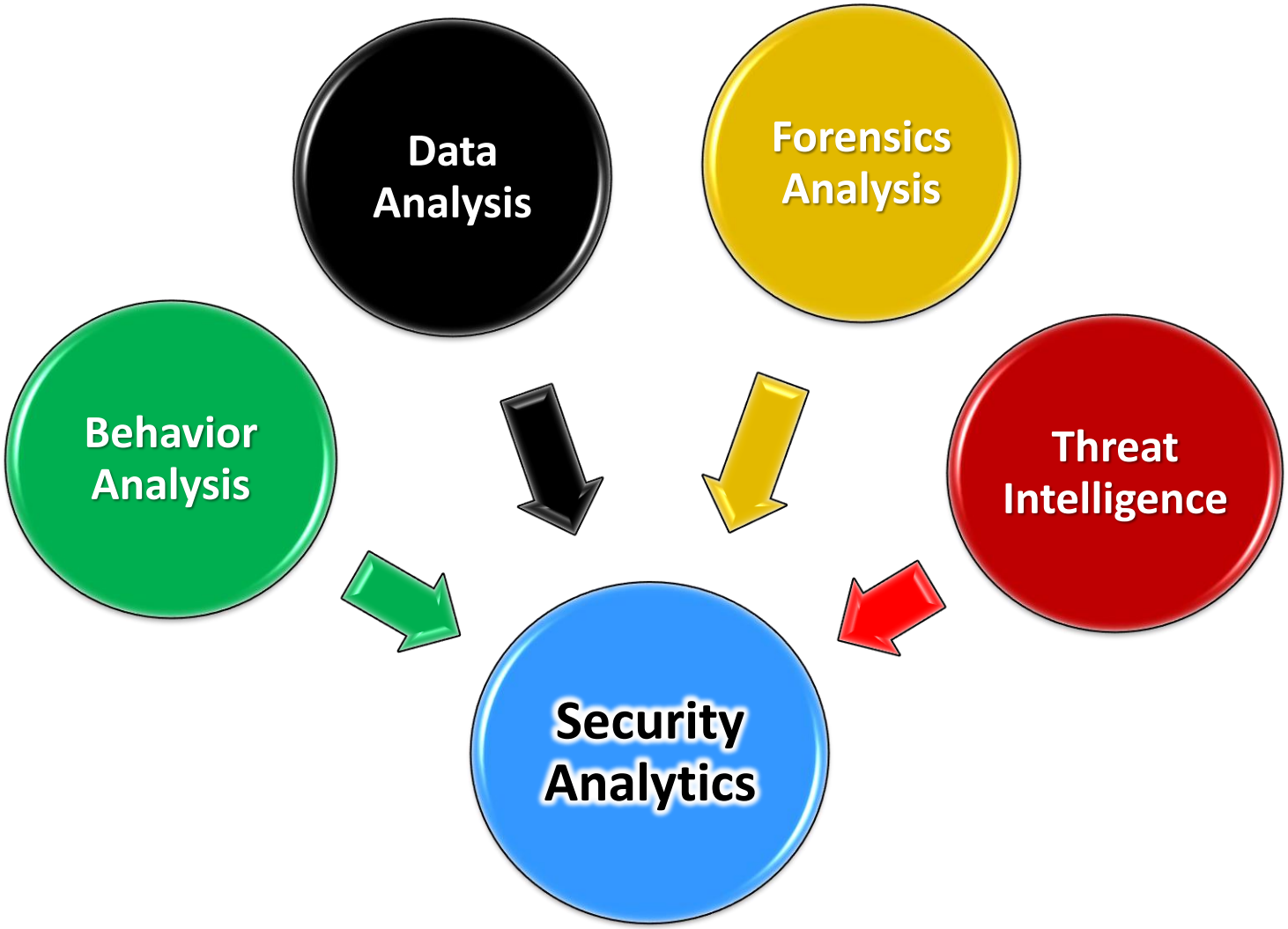
+ Threat Intelligence
+ SIEM/Log Data
+ Network Protection
+ Endpoint Protection
+ Cloud
+ User Identity
+ Incident Tools

= SECURITY ANALYTICS

well, sort of



Elementary Security Analytics

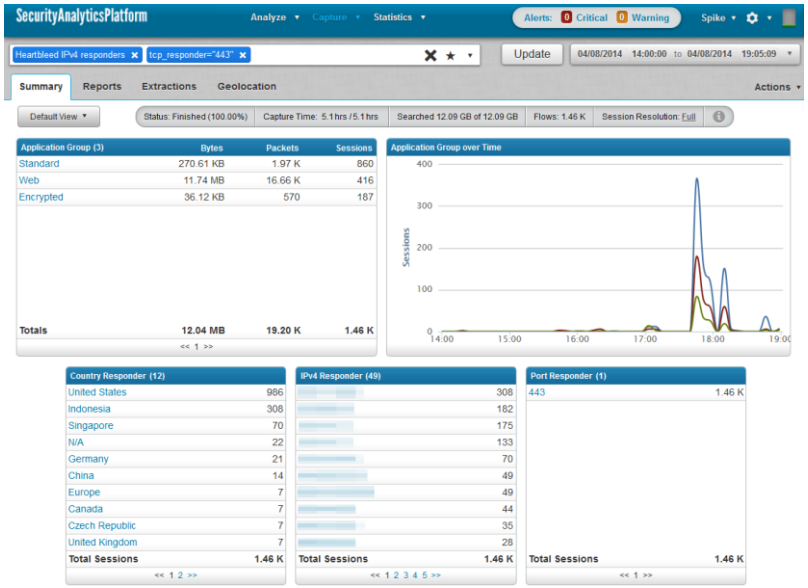


Behavior Analyzers (BA)

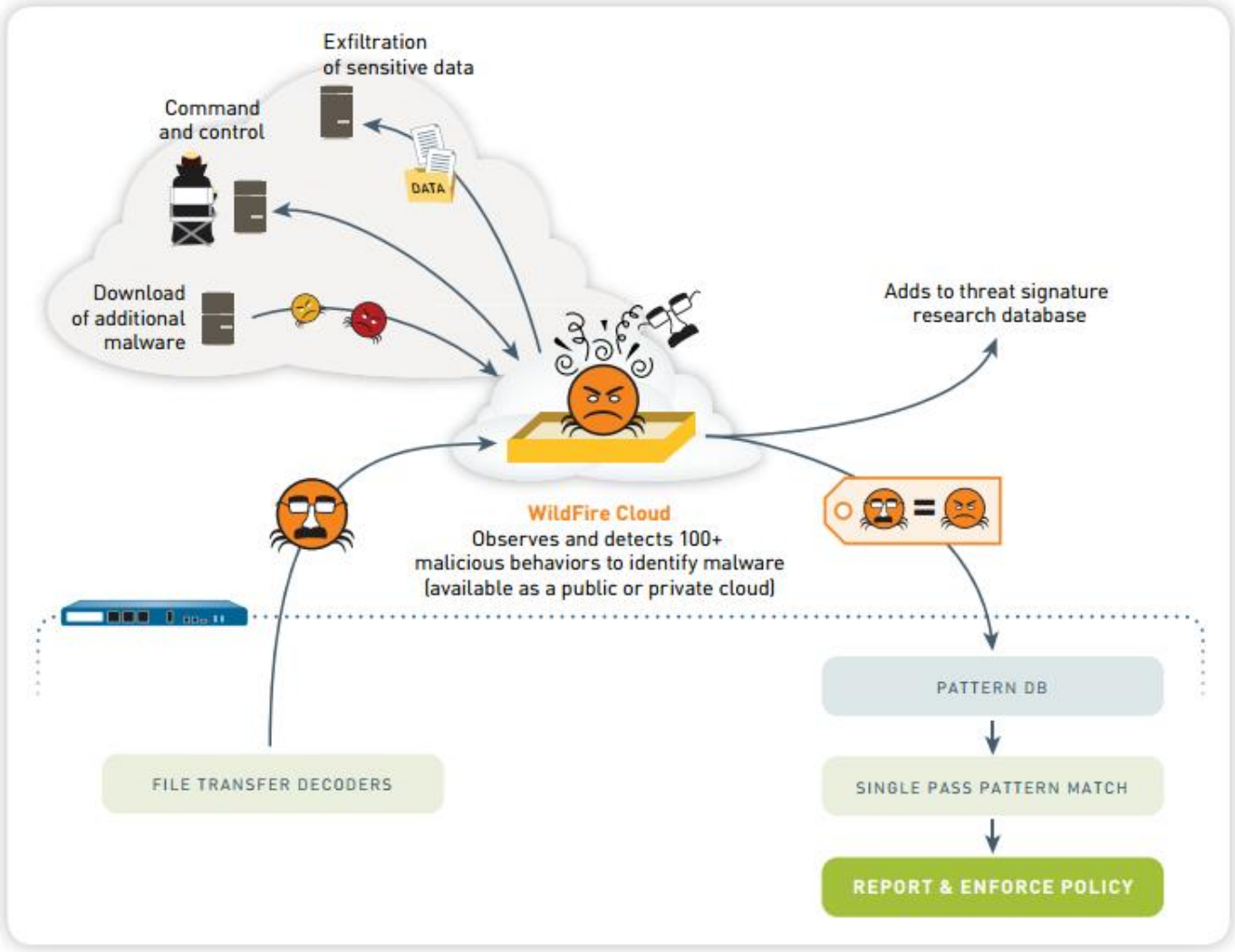
- AKA: *Breach Detection* or *Kill-Chain Analyzers*
- A class of technologies that analyzes behavior for indicators of compromise (IoC)
- Many different classes of BA products:
  - Network (Breach-detection)
  - Host (APT, advanced endpoint)
  - User Identity
  - Cloud
  - Dark-Web Intelligence
- Uses threat intelligence to be more accurate
- BA is not DLP, and DLP is not BA – but they are close

BA: Network-Based / Full-Packet Capture

- Sniff packets, look for bad stuff
- Competing technologies
  - Sandboxing: trap files and pull them apart
  - Network Behavior: Track activity on the network
  - Packet Capture: Retain full packet capture
- Hardware and processor intensive products
- Greatly beneficial in IR and forensics



BA: Sandboxing Example



Source: Palo Alto Networks

BA: Host-Based

A very busy area for competing tech:

- **Sandboxing**: trap files and pull them apart
- **System behavior**: track system calls, watch for series of suspicious calls
- **Application whitelisting**: allow only trusted applications to run
- **Statistical Analysis**: probability analysis of files being malware
- **Memory / Kernel Monitoring**: Watchdog core OS
- Classic Endpoint: AV, IPS, App Control, USB Control
- **Data Loss Prevention**: monitor for sensitive content
- **Endpoint Activity**: Full screen capture of use behavior

BA: Identity-Based

- Track user logins and actions across networks, applications
- Creates baseline of user behavior, spots anomalies
- Requires endpoint or directory services integration
- Has benefits for internal operations as well
- Cloud-based access brokers are a form of identity-based BA
- Can connect with other IdM technologies

BA: Cloud-based

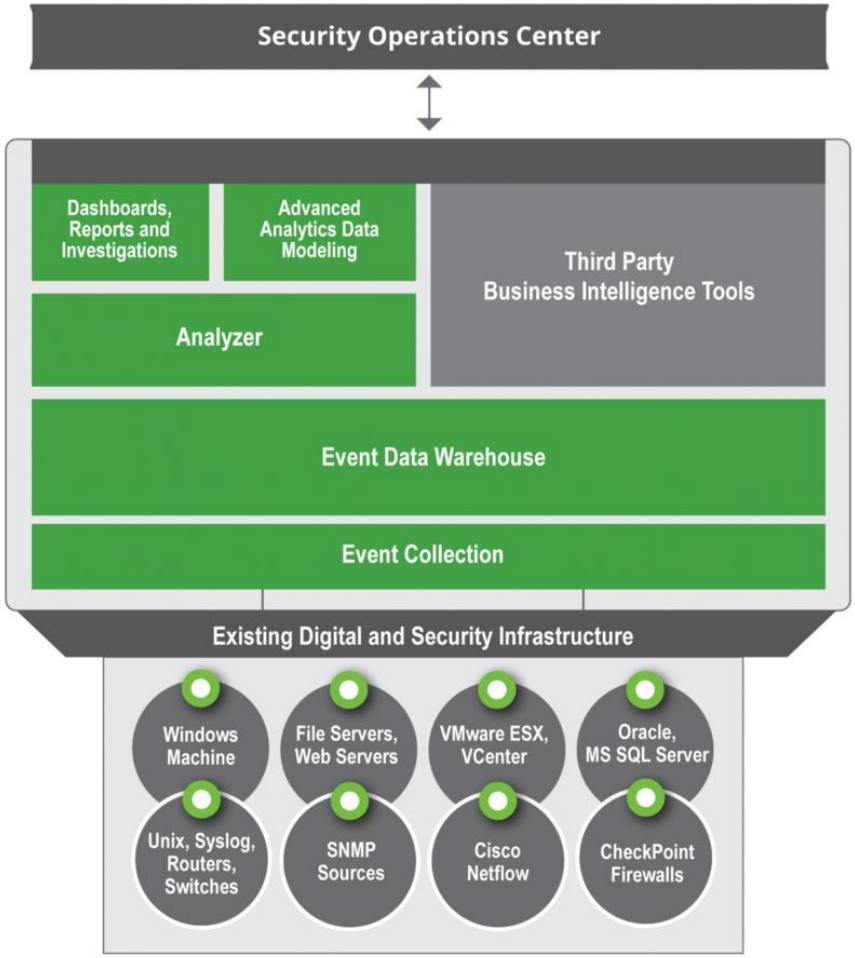
- Analytics ***in*** the cloud vs analytics ***of*** the cloud
- Messy myriad of technologies here
  - Cloud access and security brokers
  - Cloud web gateway products
  - Hybrid analytics platforms
  - SIEM-as-a-Service
- Cloud analysis is extremely difficult and dependent upon the vendor

Dark-Web Intelligence

- Actively monitors “dark web” for activity relevant to your business
  - Phishing attacks
  - PII in the wild
  - Threats against the company / executives
- Highly specialized service offerings
- Often used for brand protection and personnel security

Data Analyzers (DA)

- Crunch data to find evidence of an attack
- Evolution of SIEM correlations
- Log + network + vulnerability data
- Use threat intelligence to correlate events
- Needs a lot of data to work
- Storage and processing power are the constraining factors here



Incident Response Tools

- Many of these products can feed an incident response program (IRP)
- Many products include or offer IoC tracking and case management
- None of them can stand alone
- Data is extremely valuable in an incident
- Prerequisites
  - Solid incident response plan / program
  - Storage of data long enough to actually response
  - Real, live humans looking at the data
  - Organizational ability to handle incidents

Convergence Is Coming

- True Security Analytics will happen when these technologies fully converge into a common platform / framework
- *Detect once, defend everywhere*
- SIEM-centric solutions are the most mature
- NGFW/UTM and Web Gateways need to integrate
- There is no fully converged platform, yet


DEPLOYING SECURITY
ANALYTICS

Security Analytics Benefits

- Focus security operations on what really matters
- Integrated, set of tools that empower security teams to more quickly gather evidence and make decisions
- Seed governance and risk management practices with more relevant data
- Make SIEM more useful
- Gap coverage for weak anti-virus

Do You Need Security Analytics?

We need it for regulatory compliance

- No you don't

We don't know what we don't know

- …and security analytics may just deepen that hole.

We are worried about APT, state sponsored attacks

- You need a lot of other technologies first
- Focus on behavior based products

Our SIEM/IPS/DLP/AV can't protect us

- Neither can security analytics, really

We must stop the hackers!

- Security analytics cannot always stop things
- Many organizations refuse to configure for autoblocking

Are You Mature Enough to Handle Security Analytics?

- If you want SA to work, you must already have mastered:
  - NGFW / UTM
  - IDS/IPS
  - Web filtering
  - Application control
  - Endpoint AV
  - Vulnerability management
  - Patching
  - SIEM
  - Data loss prevention (maybe)
- In other words, you must have a very mature security program

Where Does the Threat Intelligence Come From?

Research team	Variable
Crowd sourced	Good idea but usually weak
Honeypots	Meh
Install-base	Very good
Experience	Very good
Third party	Who?
John McAfee's rants	Maybe he's on to something?

No black-box arguments here, make the vendor explain it

Do You Have the Resources?

- Security Analytics products are at least as complex (if not more so) than SIEM
- You need analysts:
  - 0-500 hosts: 1 half-time analyst
  - 500-2500 hosts: 1 full-time analyst
  - 2500-7500 hosts: 2 full-time analysts
  - 7500-15000 hosts: 3 full-time analysts
  - 15000+: analysis team
- Outsourcing SA is very difficult
- Very few talented analysts who can do this work
- If you cannot invest in the people, do not purchase the technology

Do I Need a SIEM?

- YES
- Will the technology integrate with it?
- What is the long term support?
- Hate your SIEM now? SA will make you hate it even more.
- How do you get data out of the platform?
- Many SIEM products have integrated TI feeds

Hardware Requirements?

- You will need boxes everywhere you want to capture data
- That's a lot of boxes!
- Virtual platforms help, but these are CPU and network intensive devices
- Without data collection, what's the point?

Storage Requirements?

- How much storage does it need?
- Triple whatever number the VAR/vendor tells you
- Log data uses up about 1/10th what network captures do
- Store at least 30 days worth
- You need way more storage than you think:
  - Log + Network Captures
    - 1 gig network, 1 month of storage = 500TB (minimum)
    - 10 gig, 1 month = 5 petabytes (5000 TB)
  - Log data only
    - 1TB per 500 hosts, per month

Use Cases You Need to See

- Vendor should be able to show you these use cases
- Behavior Analyzer / Breach Detection
  - Malware identification and blocking
  - Reporting and alerting
  - Integration with network / hosts
  - False positive tuning
  - Updating
- Data Analyzers
  - Querying and analysis
  - Walk through attack data
  - Incident response
  - Reporting & alerting

Ten Steps toward Security Analytics

1. Have the people and money to do this
2. Master your SIEM
3. Build an Incident Response Plan (IRP)
4. Strengthen your mobile / BYOD platform
5. Implement network-based breach detection capabilities
6. Augment outbound web filtering / proxy
7. Integrate threat intelligence into your SIEM
8. Upgrade or augment endpoint detection capabilities
9. Start storing full-packet captures (consider converged platform)
10. Update your IRP for the new technologies

Final Thoughts

- You want simplicity, not eye candy
- Endpoint products are an enormous headache to manage
- Perform a comprehensive risk assessment first, then drive your strategy from the risk assessment
- Look for products that support sophisticated workflows and specifically – campaigns
- Build a 12-24 month plan to roll out Security Analytics
- Keep any eye out for more acquisitions and mergers in this space

Thank You

EMAIL:	andrew.plato@anitian.com
WEB:	anitian.com
TWITTER:	@andrewplato @AnitianSecurity
BLOG:	blog.anitian.com
SLIDES:	http://bit.ly/anitian
CALL:	888-ANITIAN