

# Security Analytics: The Game is On

Andrew Plato, CEO, Anitian

Professional Techniques – T22



*Trust in, and value from, information systems*

**San Francisco Chapter**

The "CyberSizelT" logo is set against a background of a stylized city skyline with a bridge, likely the Golden Gate Bridge, in shades of yellow and orange. The word "CyberSizelT" is written in a large, bold, red font with a white outline. The "T" is significantly larger than the other letters and has a unique shape.

**CyberSizelT**

A silhouette of a person wearing a cap and holding a device, set against a dramatic sunset sky with orange and blue tones. The person is on the left side of the frame, looking towards the right.

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.*

The logo for RiskNow, featuring the word "Risk" in blue and "Now" in black, with a registered trademark symbol.

Rapid Risk Assessment

The logo for VISIONPATH, with "VISION" in teal and "PATH" in orange.

Compliance Assessment

The logo for RING.ZERO, with "RING" and ".ZERO" in bright green on a black background.

Next-Generation Penetration Testing

The logo for SHERLOCK, with "SHERLOCK" in red and white on a black background. The letter "O" is replaced by a circular icon containing binary code (0101, 100010, 0111).

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

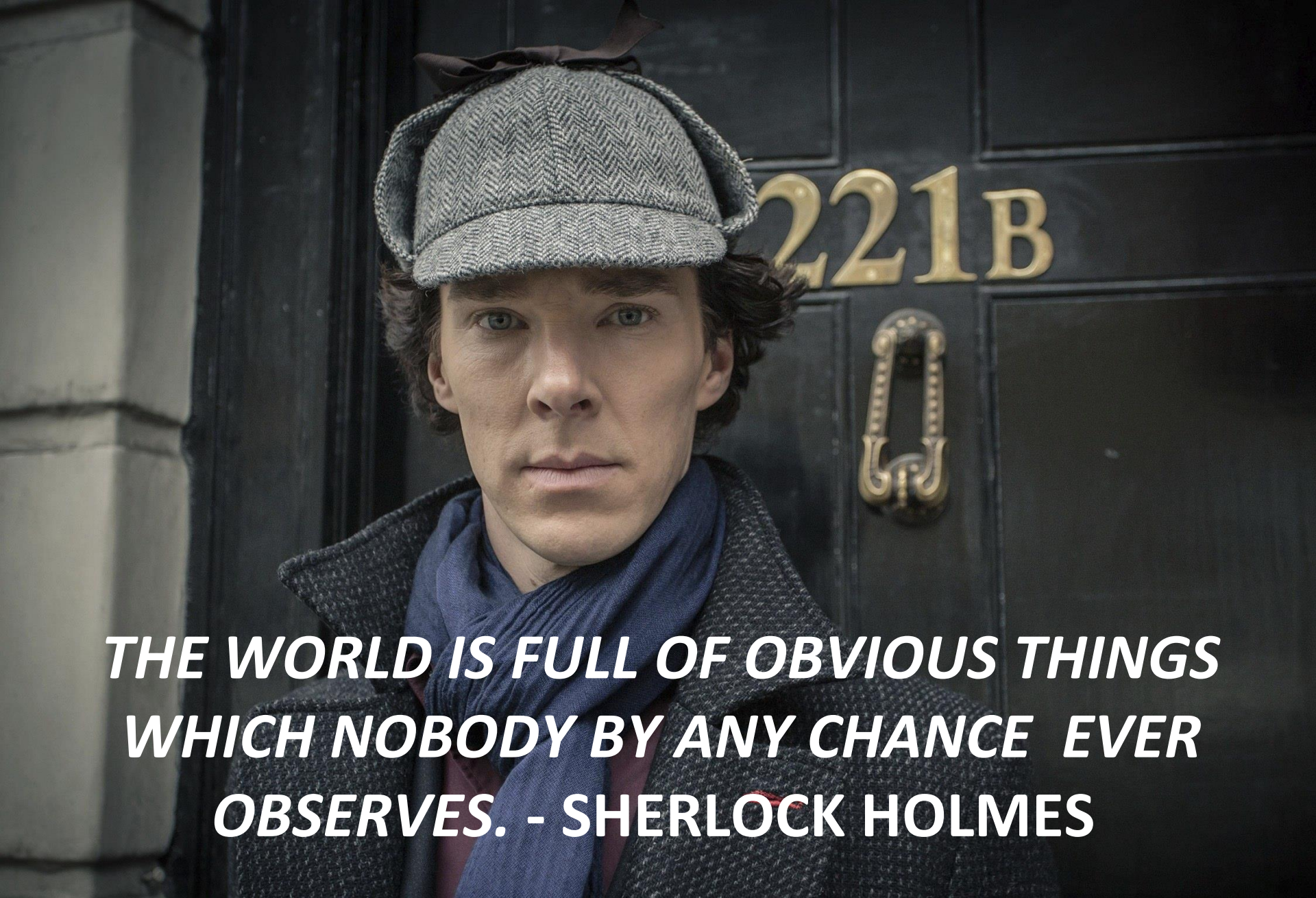
- This is a *very* nascent market
- Our data comes from research beginning in 2014
- We do not sell products
- Security Analytics is a combination of many technologies coalescing into a market



The background features a dark red, glowing grid pattern that recedes into the distance, creating a sense of depth. Overlaid on this grid are various digital elements, including vertical lines of light, horizontal data streams, and faint, illegible text or code. The overall aesthetic is high-tech and digital.

# 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 screenshot shows the top of an Ars Technica article. The header includes the 'ars technica' logo and navigation links for 'MAIN MENU', 'MY STORIES: 25', 'FORUMS', 'SUBSCRIBE', and 'JOBS'. The article title is 'Antivirus pioneer Symantec declares AV "dead" and "doomed to failure"', with a sub-headline 'Company concedes AV fails to catch majority of malicious attacks in circulation.' The author is 'by Dan Goodin - May 5 2014, 9:25am PDT'. There are social media share buttons for Facebook, Twitter, and a count of 155. The first paragraph of the article is visible, stating that Symantec has admitted the growing inability of scanning software to detect the majority of malware attacks.



The screenshot shows the top of a Schneier on Security article. The header includes the 'Schneier on Security' logo and navigation links for 'Blog', 'Newsletter', 'Books', 'Essays', 'News', 'Schedule', 'Crypto', and 'About Me'. The article title is 'The Failure of Anti-Virus Companies to Catch Military Malware'. The author is Mikko Hypponen of F-Secure, and the article discusses why anti-virus companies didn't catch Stuxnet, DuQu, and Flame. The first paragraph of the article is visible, stating that when digging through their archive for related samples of malware, they were surprised to find that they already had samples of Flame, dating back to 2010 and 2011, that they were unaware they possessed.

# The Failure of SIEM

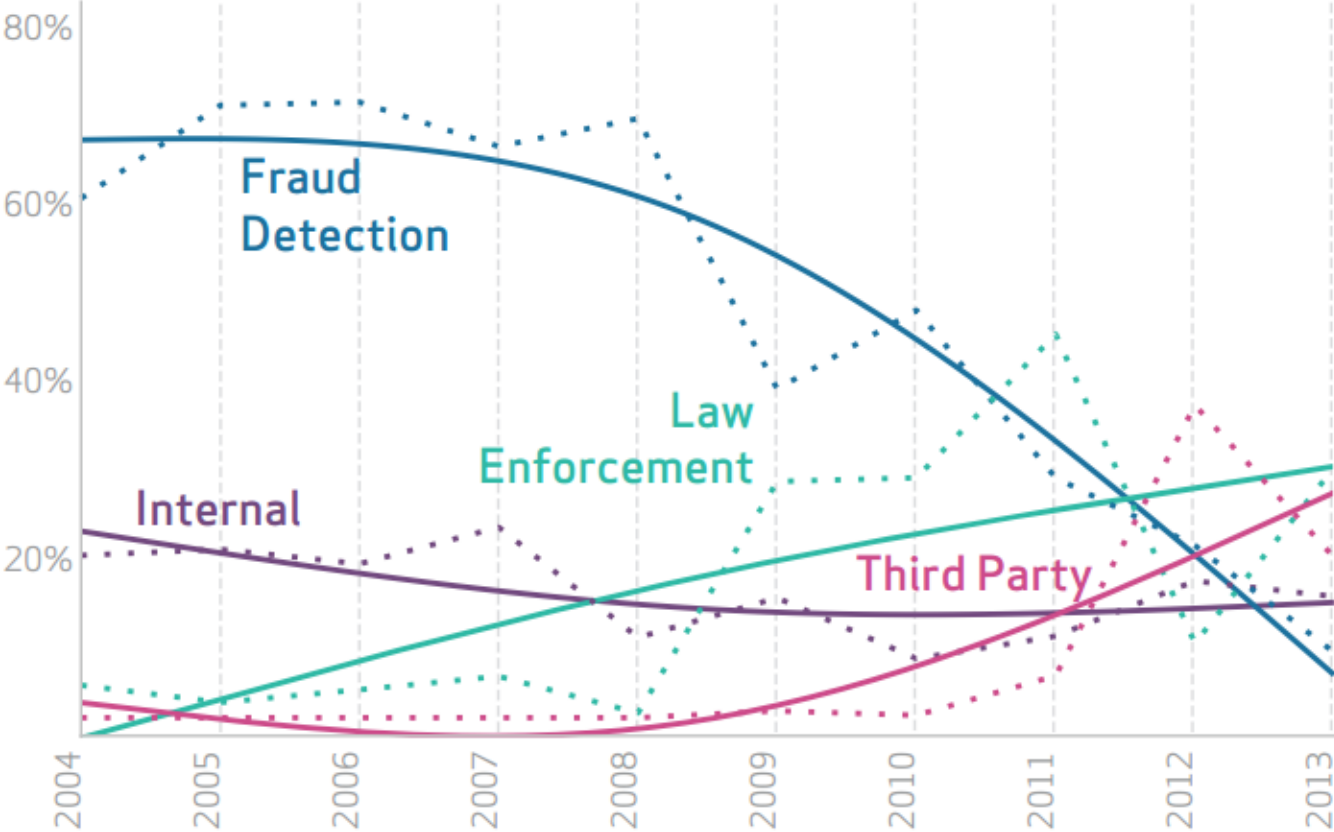
- Big data
- Big complexity
- Most SIEM deployments are strictly to satisfy compliance requirements
- Immense barriers to *operationalization*





# Failure of Incident Response

Figure 14.  
Breach discovery methods over time

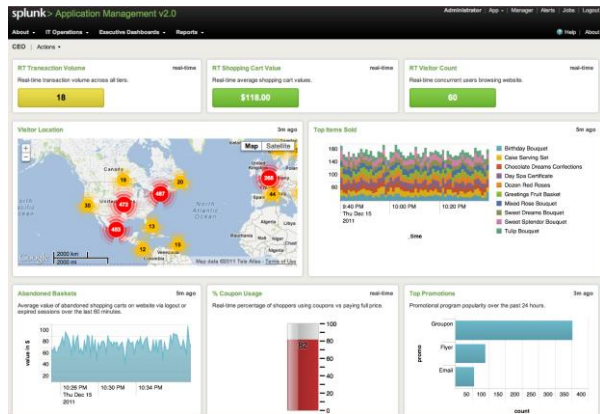


Verizon Data Breach Report - 2014

# 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

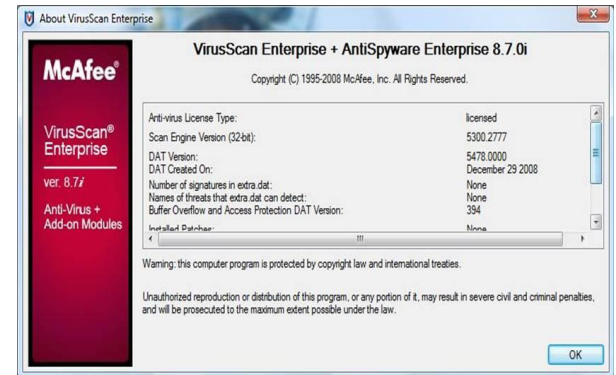
# Data data data



SIEM

ENDPOINT

SANDBOX



NGFW

PACKET  
CAPTURE



VULNERABILITY  
MANAGEMENT





# FUMBLING IN THE DARK

A person is standing in a dark, misty forest. The scene is dimly lit with a strong blue glow emanating from the background, creating a sense of mystery and uncertainty. The person is silhouetted against the light, and the trees are dark and indistinct.

# 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





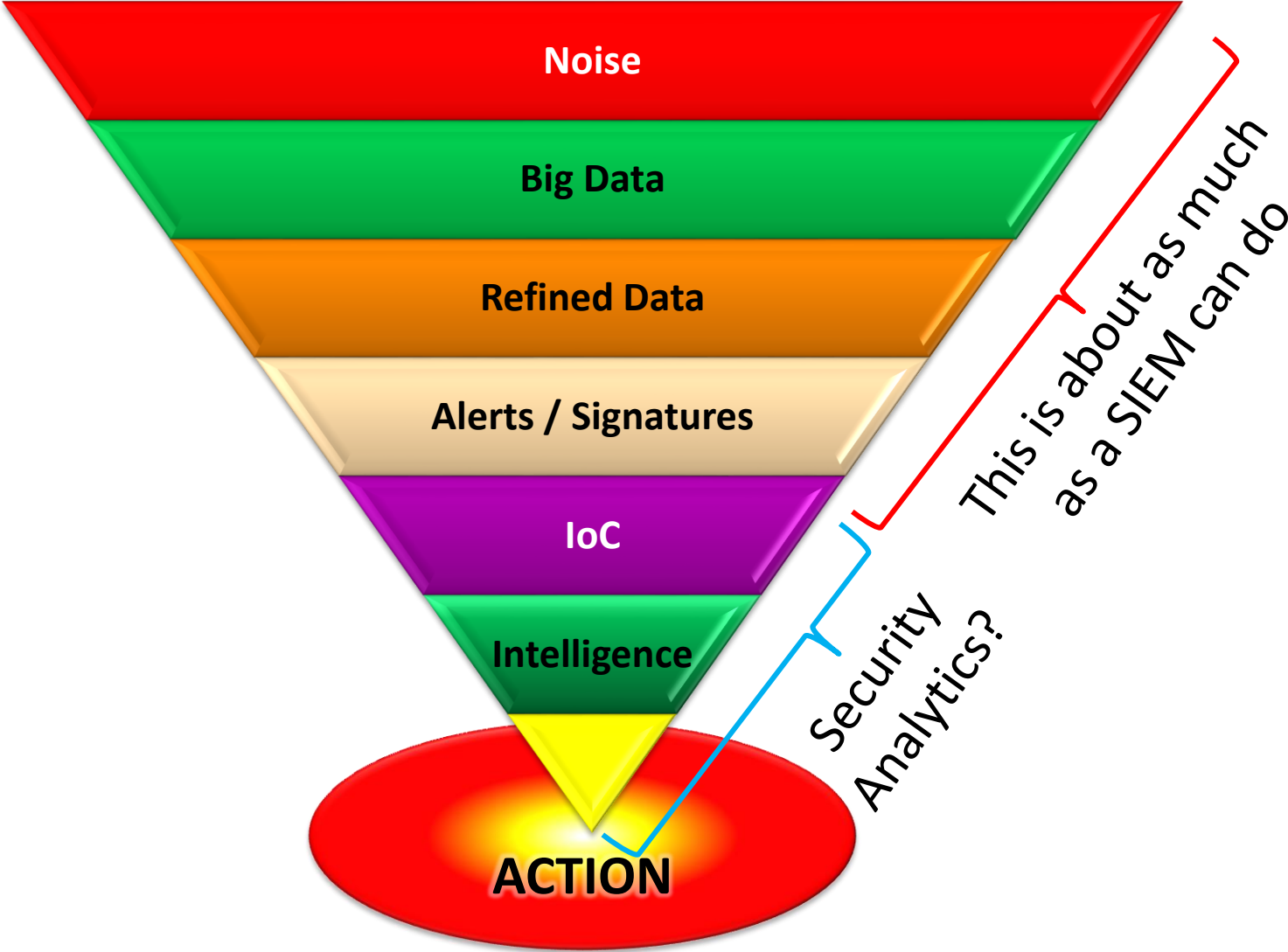
# WHAT IS THREAT INTELLIGENCE?



# 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?

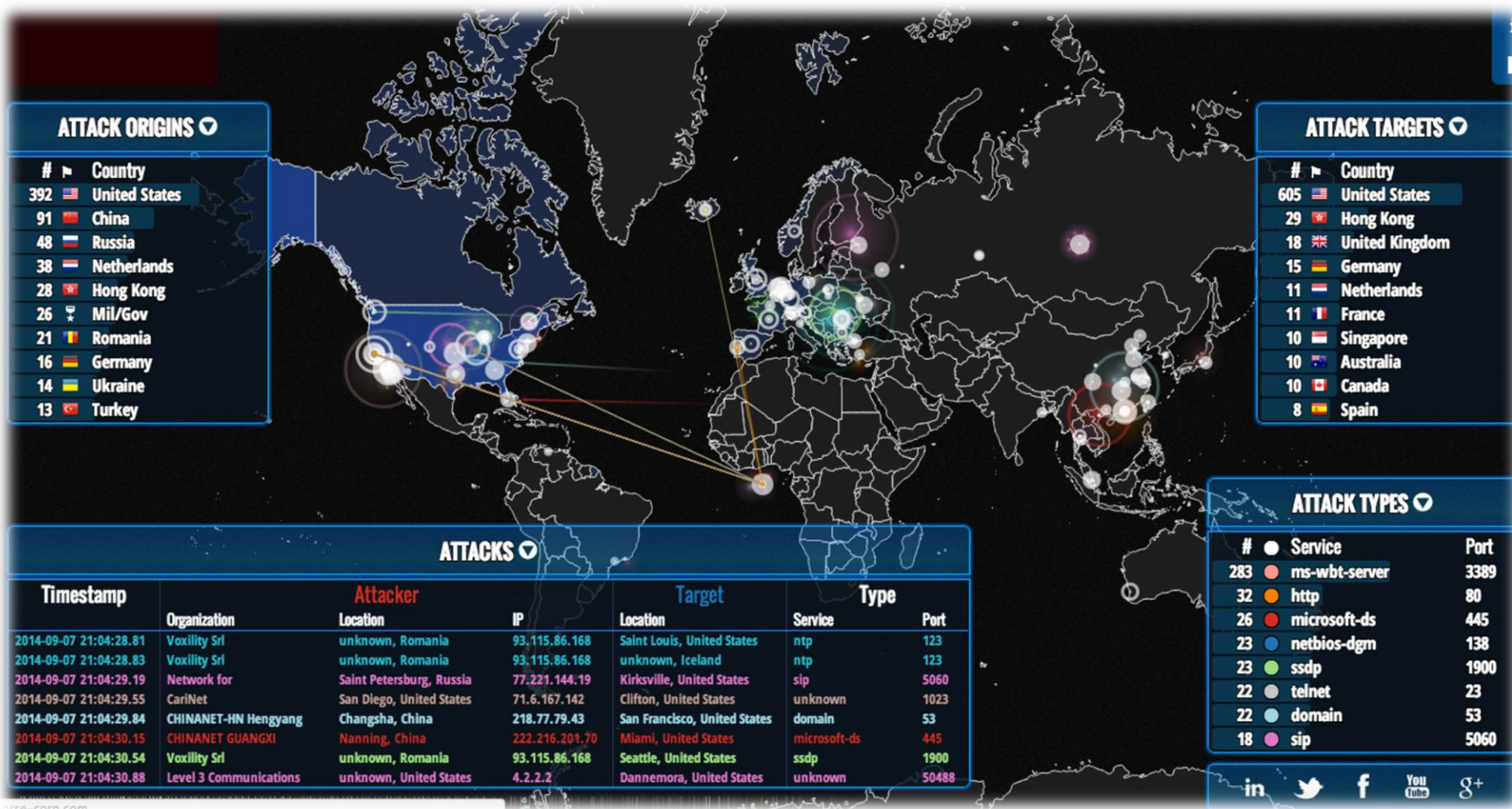
- Data, to help tune, optimize, or direct your security analytics
- Diverse sources: commercial, government, open source
- Diverse types: IoC, reputation, tactics
- Standards:
  - STIX: Structured Threat Information Expression
  - TAXII: Trusted Automated Exchange of Indicator Information

# STIX Example

```
1 <stix:Observables cybox_major_version="1" cybox_minor_version="1">
2   <cybox:Observable id="example:observable-c8c32b6e-2ea8-51c4-6446-7f5218072f27">
3     <cybox:Object id="example:object-d7fcce87-0e98-4537-81bf-1e7ca9ad3734">
4       <cybox:Properties xsi:type="AddressObject:AddressObjectType" category="ipv4-addr">
5         <AddressObject:Address_Value>198.51.100.2</AddressObject:Address_Value>
6       </cybox:Properties>
7     </cybox:Object>
8   </cybox:Observable>
9   <cybox:Observable id="example:observable-b57aa65f-9598-04fb-a9d1-5094c36d5dc4">
10    <cybox:Object id="example:object-f4fac80a-1239-47cc-b0e6-771b1a73f817">
11      <cybox:Properties xsi:type="AddressObject:AddressObjectType" category="ipv4-addr">
12        <AddressObject:Address_Value>198.51.100.17</AddressObject:Address_Value>
13      </cybox:Properties>
14    </cybox:Object>
15  </cybox:Observable>
16  <cybox:Observable id="example:observable-19c16346-0eb4-99e2-00bb-4ec3ed174cac">
17    <cybox:Object id="example:object-174bf9a3-f163-4919-9119-b52598f97ce3">
18      <cybox:Properties xsi:type="AddressObject:AddressObjectType" category="ipv4-addr">
19        <AddressObject:Address_Value>203.0.113.19</AddressObject:Address_Value>
20      </cybox:Properties>
21    </cybox:Object>
22  </cybox:Observable>
23 </stix:Observables>
24 <stix:TTPs>
25   <stix:TTP xsi:type="ttp:TTPType" id="example:ttp-dd955e08-16d0-6f08-5064-50d9e7a3104d" timestamp="2014-02-20T09:00:00.000000Z">
26     <ttp:Title>Malware C2 Channel</ttp:Title>
27     <ttp:Resources>
28       <ttp:Infrastructure>
29         <ttp:Type>Malware C2</ttp:Type>
30         <ttp:Observable_Characterization cybox_major_version="2" cybox_minor_version="1">
31           <cybox:Observable idref="example:observable-c8c32b6e-2ea8-51c4-6446-7f5218072f27"/>
32           <cybox:Observable idref="example:observable-b57aa65f-9598-04fb-a9d1-5094c36d5dc4"/>
33           <cybox:Observable idref="example:observable-19c16346-0eb4-99e2-00bb-4ec3ed174cac"/>
34         </ttp:Observable_Characterization>
35       </ttp:Infrastructure>
36     </ttp:Resources>
37   </stix:TTP>
38 </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



The background features a dark red grid pattern overlaid with various digital elements. On the left, there are faint, horizontal lines of code or data. On the right, there are vertical lines of code or data. The overall aesthetic is futuristic and technical.

# **WHAT IS SECURITY ANALYTICS?**



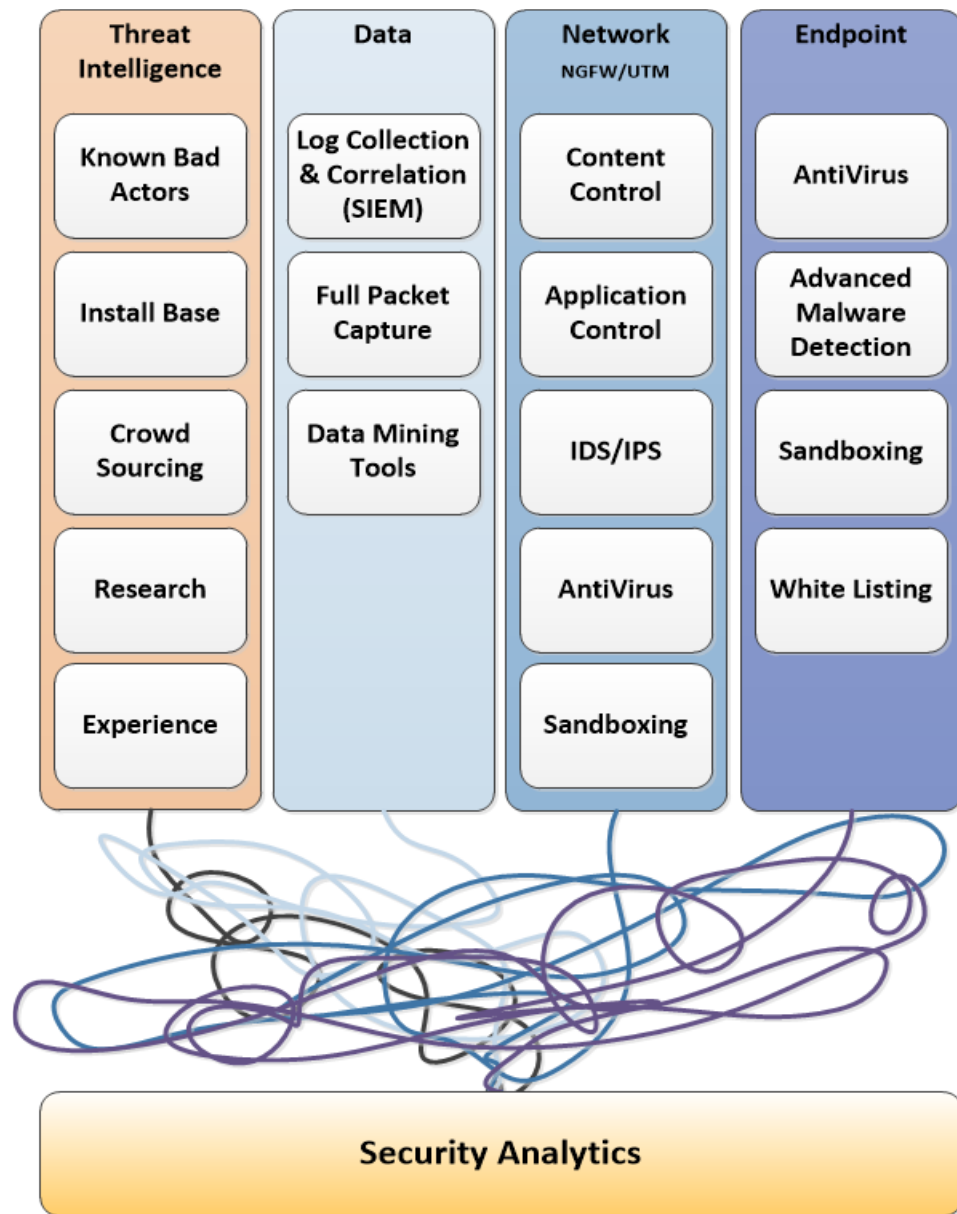
# What is Security Analytics?

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

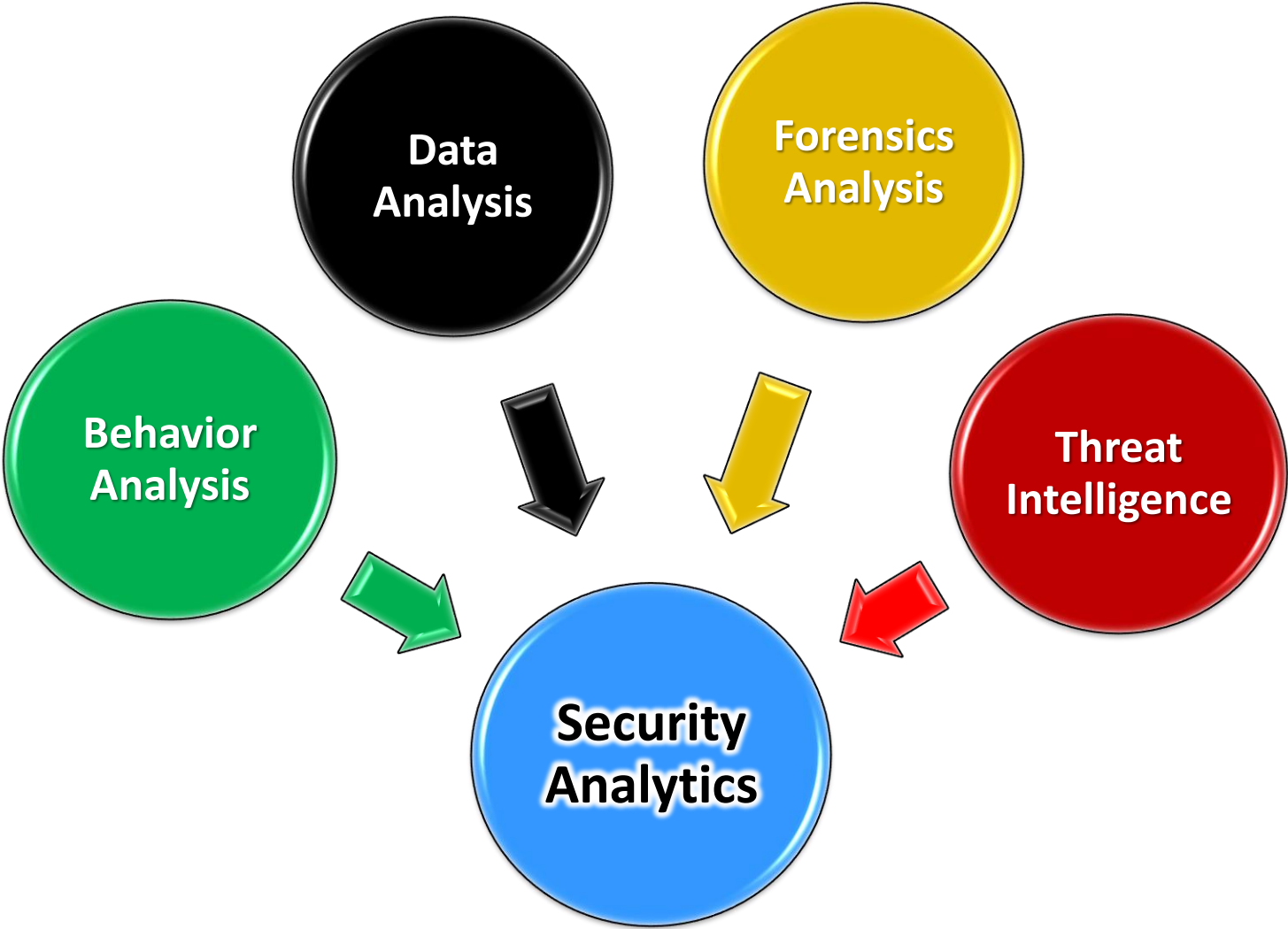
---

= SECURITY ANALYTICS

*well, sort of*



# Elementary Security Analytics

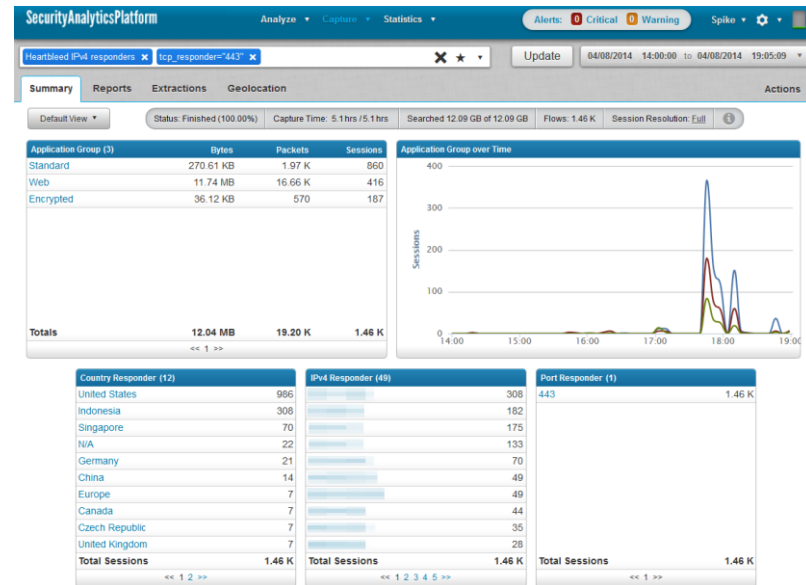


# Behavior Analyzers (BA)

- 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

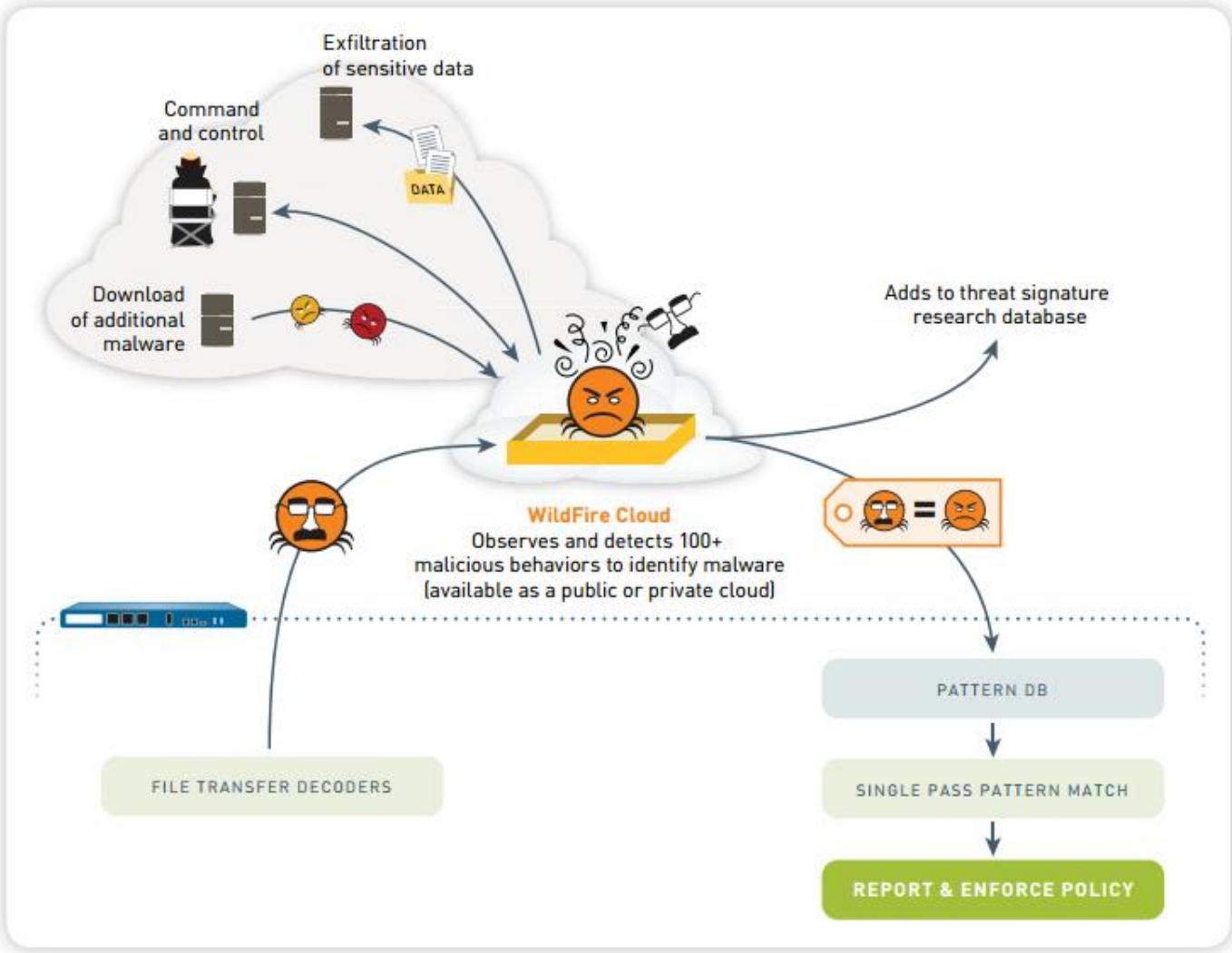
# BA: Network-Based / Full-Packet Capture

- 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

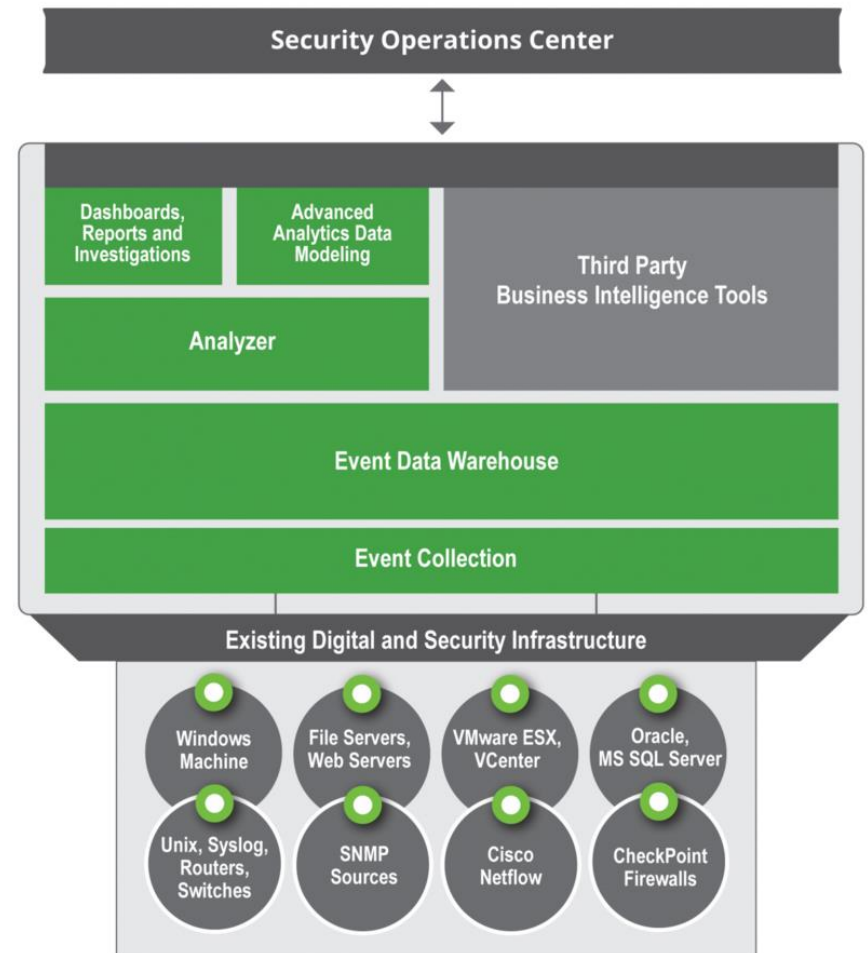
- Actively monitors “dark web” for activity relevant to your business
  - Phishing attacks
  - PII in the wild
  - Threats against the company / executives
- Highly specialized service offerings
- Often used for brand protection and personnel security





# 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

The background features a dark green grid with glowing green lines of code floating in a 3D space, creating a sense of depth and digital connectivity. The code is rendered in a monospaced font, typical of a terminal or programming environment.

# 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 1/10<sup>th</sup> 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](mailto:andrew.plato@anitian.com)

WEB: [anitian.com](http://anitian.com)

TWITTER: [@andrewplato](https://twitter.com/andrewplato)  
[@AnitianSecurity](https://twitter.com/AnitianSecurity)

BLOG: [blog.anitian.com](http://blog.anitian.com)

SLIDES: <http://bit.ly/anitian>

CALL: 888-ANITIAN