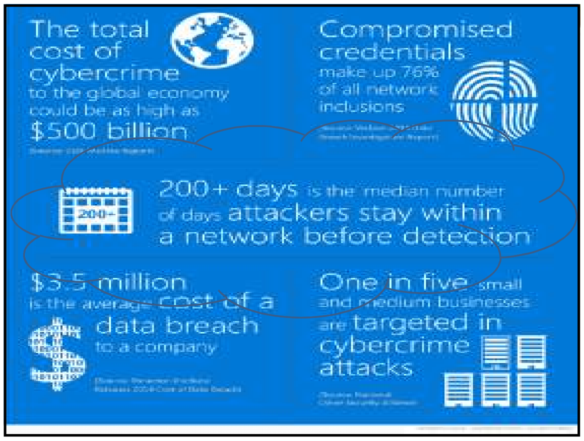
UBA
User Behavior Analytics

Interface Madison – September 22, 2016

Presented by:
Ken M. Shaurette, CISSP, CISA, CISM, CRISC
FIPCO Director IT Services

DISCLAIMER

- Covering topic in general terms, some products may provide options and cross over, but in generality many of the statements being made apply to the base industry category for SIEM/SEM or UBA/UEBA.
- I have not represented all products in the presentation and some areas such as DLP, advanced endpoint tools, advanced correlation of some SIEM may cross over into UEBA/UBA.



The total cost of cybercrime to the global economy could be as high as $500 billion

[illegible]

Compromised credentials make up 76% of all network inclusions

[illegible]

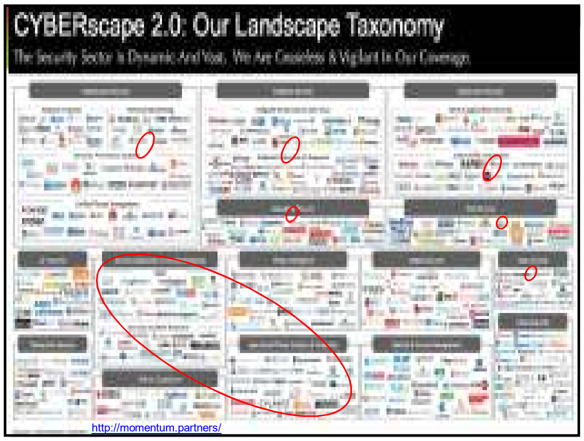
200+ days is the median number of days attackers stay within a network before detection

$3.5 million is the average cost of a data breach to a company

(Source: Ponemon Institute Releases 2014 Cost of Data Breach)

One in five small and medium businesses are targeted in cybercrime attacks

(Source: National Cyber Security Alliance)



CYBERscape 2.0: Our Landscape Taxonomy

The Security Sector Is Dynamic And Vast, We Are Ceaseless & Vigilant In Our Coverage.

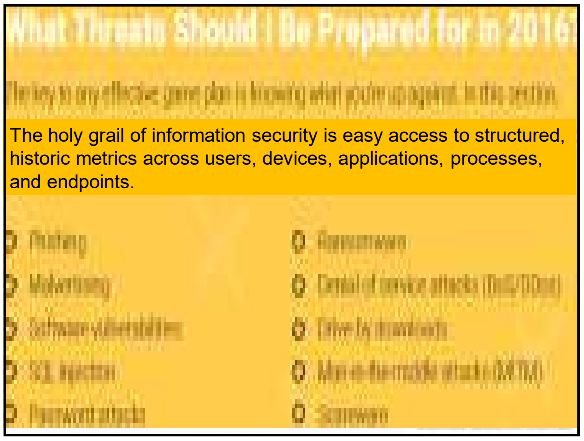
http://momentum.partners/

CYBERscape 2.0 – The Security Sector

- Information Security
- Endpoint Security
- Application Security
- Messaging Security
- Web Security
- IoT Security
- Security Operations & Incident Response
- Threat Intelligence
- Mobile Security
- Data Security
- Transaction Security
- Risk & Compliance
- Threat Analysis & UEBA
- Identity & Access Mgmt
- Cloud Security

- FORENSICS

5 FIPCO® © 2016

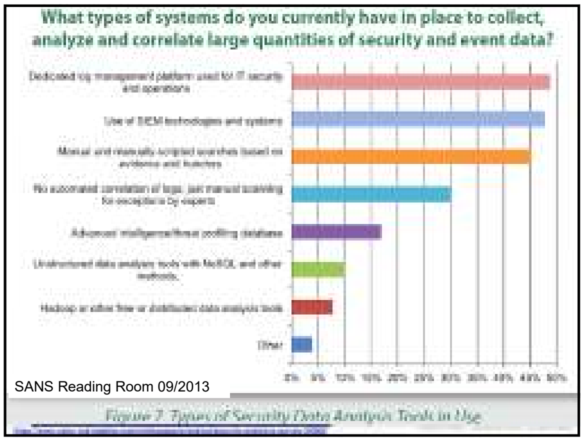


What Threats Should I Be Prepared for in 2016?

The key to any effective game plan is knowing what you're up against. In this section,

The holy grail of information security is easy access to structured, historic metrics across users, devices, applications, processes, and endpoints.

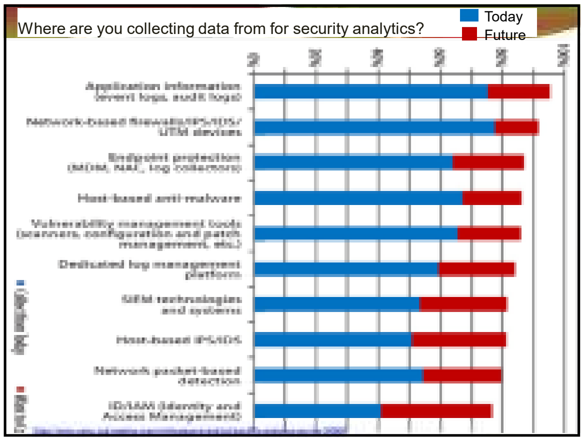
- Phishing
- Malvertising
- Software vulnerabilities
- SQL injection
- Password attacks
- Ransomware
- Denial of service attacks (DoS/DDoS)
- Drive-by downloads
- Man-in-the-middle attacks (MITM)
- Scareware



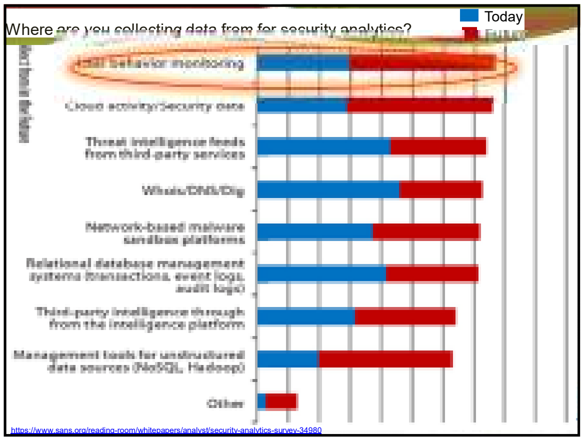
What types of systems do you currently have in place to collect, analyze and correlate large quantities of security and event data?

SANS Reading Room 09/2013

Figure 7. Types of Security Data Analysis Tools in Use



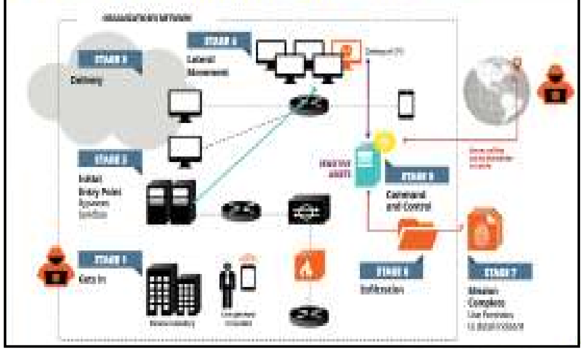
Where are you collecting data from for security analytics?



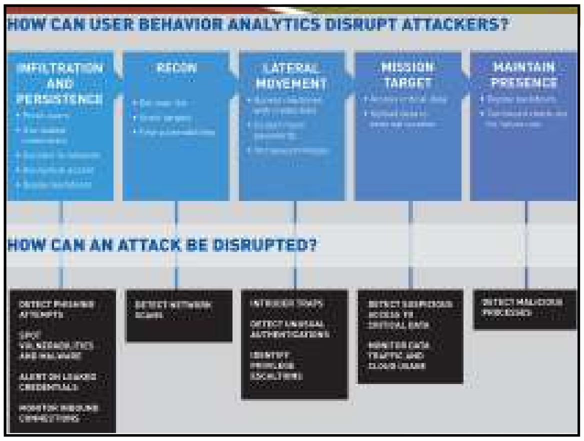
Where are you collecting data from for security analytics?

https://www.sans.org/reading-room/whitepapers/analyst/security-analytics-survey-34980

ANATOMY OF AN ATTACK CAMPAIGN



HOW CAN USER BEHAVIOR ANALYTICS DISRUPT ATTACKERS?



INFILTRATION AND PERSISTENCE
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]

RECON
- [illegible]
- [illegible]
- [illegible]

LATERAL MOVEMENT
- [illegible]
- [illegible]
- [illegible]

MISSION TARGET
- [illegible]
- [illegible]

MAINTAIN PRESENCE
- [illegible]
- [illegible]

HOW CAN AN ATTACK BE DISRUPTED?

DETECT PHISHING ATTEMPTS

SPOT VULNERABILITIES AND MALWARE

ALERT ON LEAKED CREDENTIALS

MONITOR INBOUND CONNECTIONS

DETECT NETWORK SCANS

INTRUDER TRAPS

DETECT UNUSUAL AUTHENTICATIONS

IDENTIFY PRIVILEGE ESCALATIONS

DETECT SUSPICIOUS ACCESS TO CRITICAL DATA

MONITOR DATA TRAFFIC AND CLOUD USAGE

DETECT MALICIOUS PROCESSES

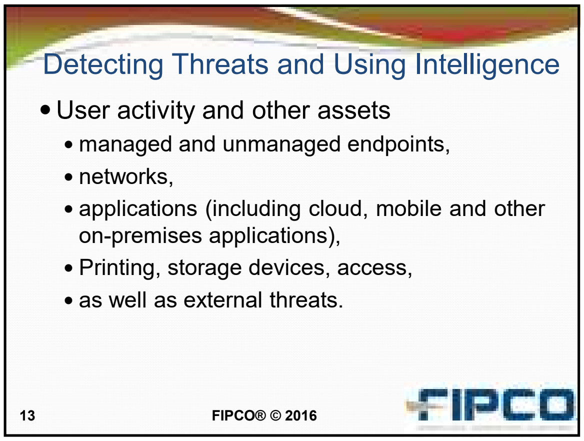
Address Behavior, Not Rules

- 200+ days = the average amount of time attackers reside inside a network before detection (188 days may be more current)

  If you can identify a baseline of what a user or device normally does daily, hourly, every minute…

  From a Baseline you can Begin to determine if something is different

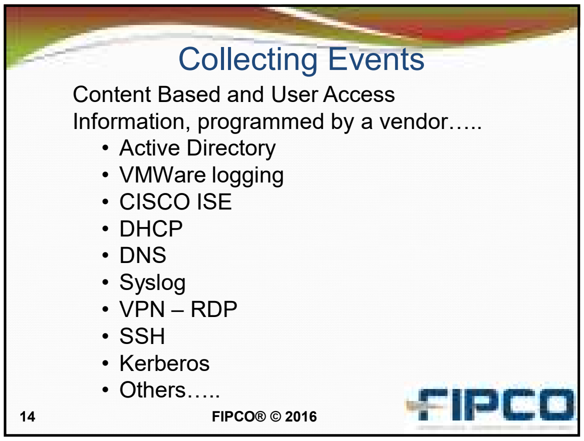
FIPCO® © 2016



Detecting Threats and Using Intelligence

- User activity and other assets
  - managed and unmanaged endpoints,
  - networks,
  - applications (including cloud, mobile and other on-premises applications),
  - Printing, storage devices, access,
  - as well as external threats.

13 FIPCO® © 2016

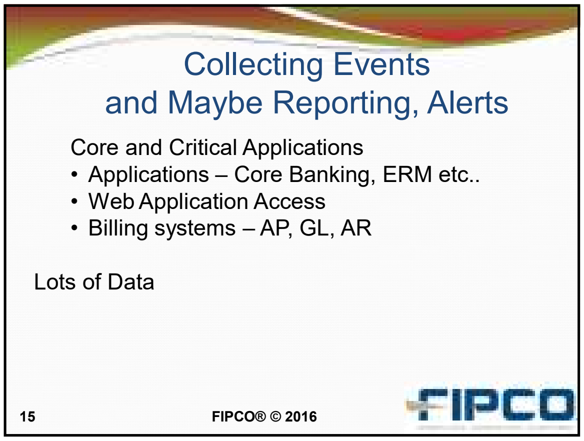


Collecting Events

Content Based and User Access
Information, programmed by a vendor…..

- Active Directory
- VMWare logging
- CISCO ISE
- DHCP
- DNS
- Syslog
- VPN – RDP
- SSH
- Kerberos
- Others…..

14 FIPCO® © 2016



Collecting Events and Maybe Reporting, Alerts

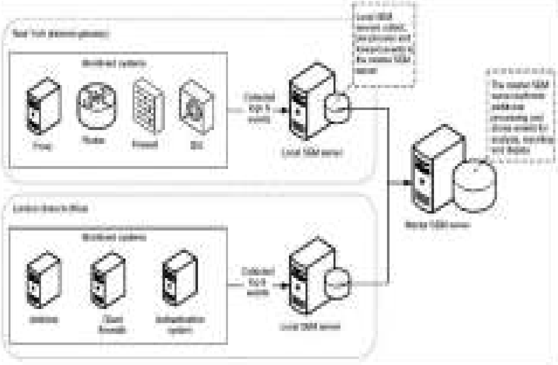
Core and Critical Applications

- Applications – Core Banking, ERM etc..
- Web Application Access
- Billing systems – AP, GL, AR

Lots of Data

15 FIPCO® © 2016

Traditional - Collecting Events



SIEM (Security Information and Event Management)

- Good at aggregating logs and alerts from other tools for reporting and compliance purposes,

does not provide accurate and efficient detection of *attacks in progress*

  - SIEM combines SIM (security information management) and SEM (security event management) functions into one security management system.
- collects logs and other security related documentation for analysis

17 FIPCO® © 2016

What are other Experts Saying

- SEM or EM Primarily aggregating events from operating systems and infrastructure devices (e.g. firewall) - provide centralized logging….
- SIEM began monitoring the security of applications
- Next generation:
  - needs to detect and predict threats based on the behavior across systems
  - Anomaly - changes from normal versus just what was logged….

Article: The hunt for data analytics: Is your SIEM on the endangered list? searchsecurity.techtarget.com

18 FIPCO® © 2016

SIEM (Security Information and Event Management)

- Correlation may offer some detection….
  - Organizations have spent years trying to write correlation rules to leverage this data into attack detection, but it hasn't worked.
- Doesn't have the best source of data for advanced attacks – have logs from servers and other tools
- No granular network traffic or current state of an endpoint being attacked
- SIEM's suggest adding Netflow, but that is still limiting

19 FIPCO® © 2016

What are other Experts Saying?

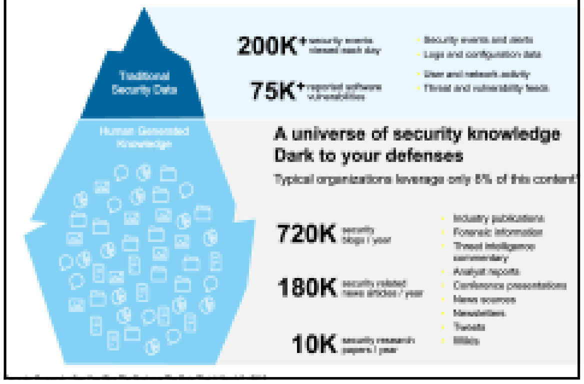
SIEM systems regularly saw as many as 15,000 events per second.
Now, 80,000 events per second is not uncommon

> "As an analyst starts to get swamped, that precognitive bias kicks in, and they say, 'I've seen this alert before,' and they will ignore it."

Article: The hunt for data analytics: Is your SIEM on the endangered list? searchsecurity.techtarget.com

20 FIPCO® © 2016

Most security knowledge is for humans and is untapped



200K+ security events viewed each day

75K+ reported software vulnerabilities

- Security events and alerts
- Logs and configuration data
- User and network activity
- Threat and vulnerability feeds

A universe of security knowledge Dark to your defenses

Typical organizations leverage only 8% of this content!

720K security blogs / year

180K security related news articles / year

10K security research papers / year

- Industry publications
- Forensic information
- Threat intelligence commentary
- Analyst reports
- Conference presentations
- News sources
- Newsletters
- Tweets
- Wikis

Security blindness:

Too many alerts and too few resources

22 FIPCO® © 2016

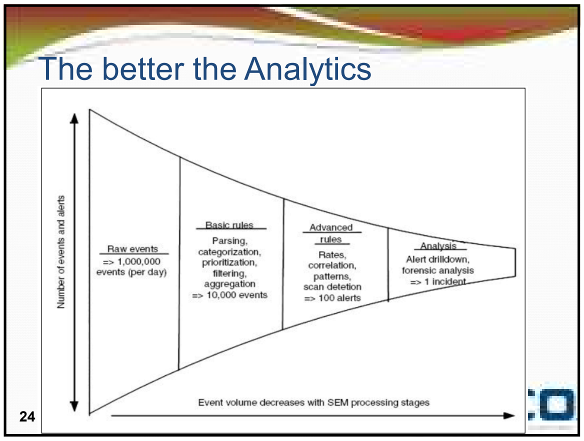
FIPCO

SIEM Blindness

Events only as programmed not all activity

23 FIPCO® © 2016

FIPCO



The better the Analytics

Number of events and alerts

Raw events
=> 1,000,000
events (per day)

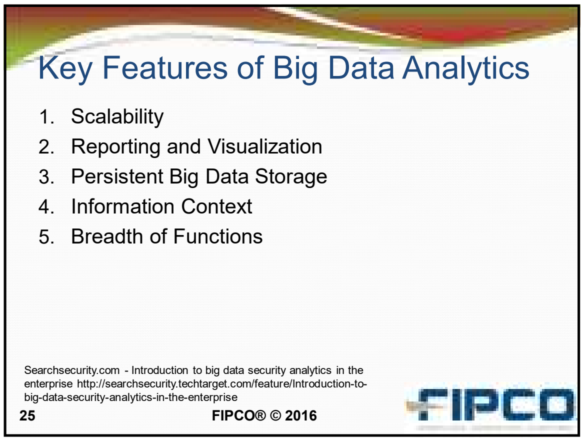
Basic rules
Parsing,
categorization,
prioritization,
filtering,
aggregation
=> 10,000 events

Advanced
rules
Rates,
correlation,
patterns,
scan detetion
=> 100 alerts

Analysis
Alert drilldown,
forensic analysis
=> 1 incident

Event volume decreases with SEM processing stages

24

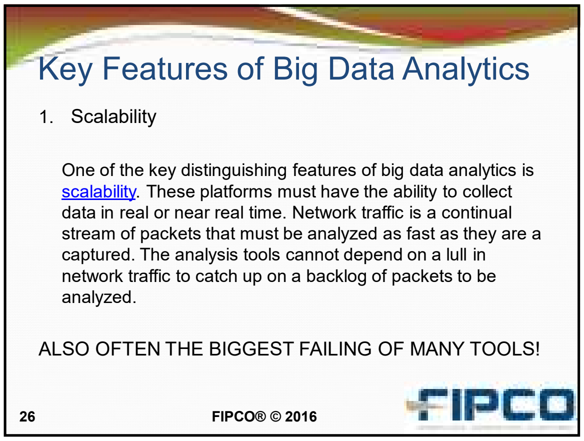


Key Features of Big Data Analytics

1. Scalability
2. Reporting and Visualization
3. Persistent Big Data Storage
4. Information Context
5. Breadth of Functions

Searchsecurity.com - Introduction to big data security analytics in the enterprise http://searchsecurity.techtarget.com/feature/Introduction-to-big-data-security-analytics-in-the-enterprise

25 FIPCO® © 2016



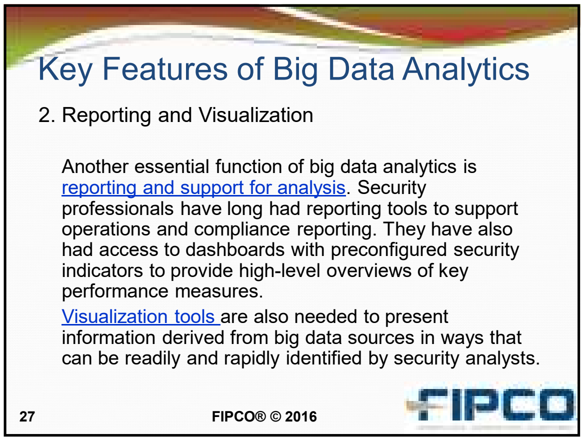
Key Features of Big Data Analytics

1. Scalability

One of the key distinguishing features of big data analytics is scalability. These platforms must have the ability to collect data in real or near real time. Network traffic is a continual stream of packets that must be analyzed as fast as they are a captured. The analysis tools cannot depend on a lull in network traffic to catch up on a backlog of packets to be analyzed.

ALSO OFTEN THE BIGGEST FAILING OF MANY TOOLS!

26 FIPCO® © 2016



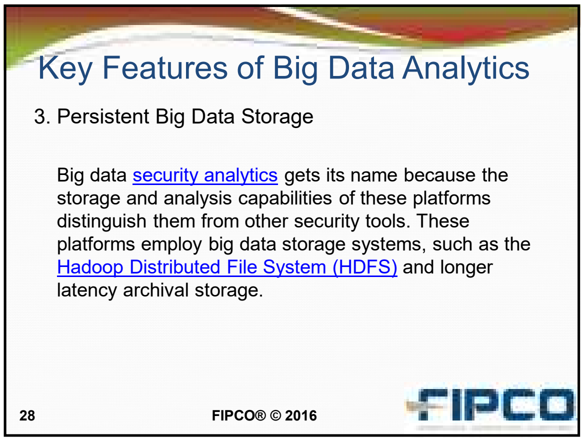
Key Features of Big Data Analytics

2. Reporting and Visualization

Another essential function of big data analytics is reporting and support for analysis. Security professionals have long had reporting tools to support operations and compliance reporting. They have also had access to dashboards with preconfigured security indicators to provide high-level overviews of key performance measures.

Visualization tools are also needed to present information derived from big data sources in ways that can be readily and rapidly identified by security analysts.

27 FIPCO® © 2016

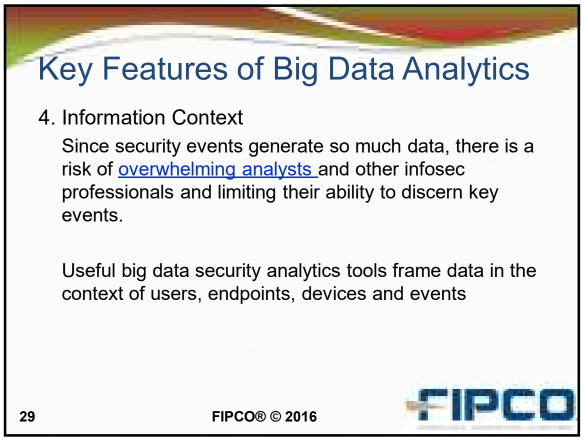


Key Features of Big Data Analytics

3. Persistent Big Data Storage

Big data security analytics gets its name because the storage and analysis capabilities of these platforms distinguish them from other security tools. These platforms employ big data storage systems, such as the Hadoop Distributed File System (HDFS) and longer latency archival storage.

28 FIPCO® © 2016



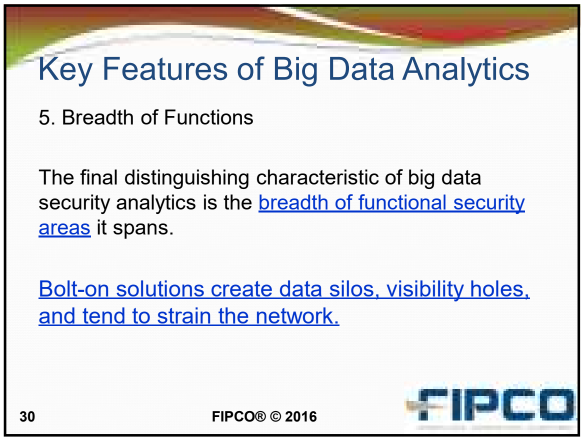
Key Features of Big Data Analytics

4. Information Context

Since security events generate so much data, there is a risk of overwhelming analysts and other infosec professionals and limiting their ability to discern key events.

Useful big data security analytics tools frame data in the context of users, endpoints, devices and events

29 FIPCO® © 2016



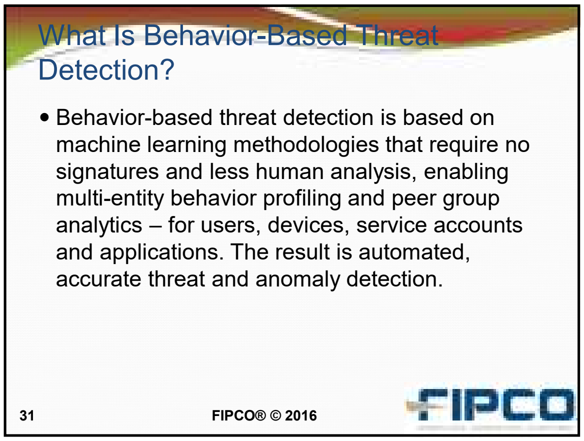
Key Features of Big Data Analytics

5. Breadth of Functions

The final distinguishing characteristic of big data security analytics is the breadth of functional security areas it spans.

Bolt-on solutions create data silos, visibility holes, and tend to strain the network.

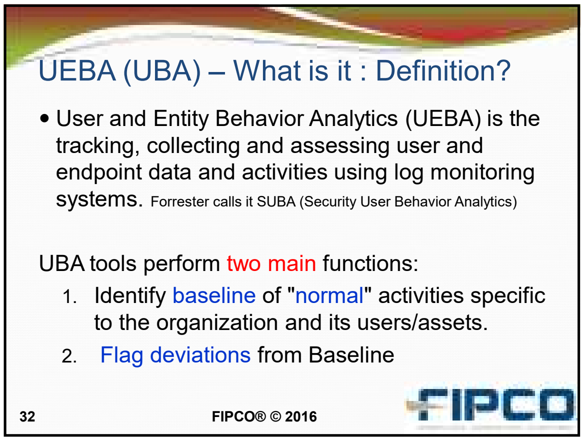
30 FIPCO® © 2016



What Is Behavior-Based Threat Detection?

- Behavior-based threat detection is based on machine learning methodologies that require no signatures and less human analysis, enabling multi-entity behavior profiling and peer group analytics – for users, devices, service accounts and applications. The result is automated, accurate threat and anomaly detection.

31 FIPCO® © 2016



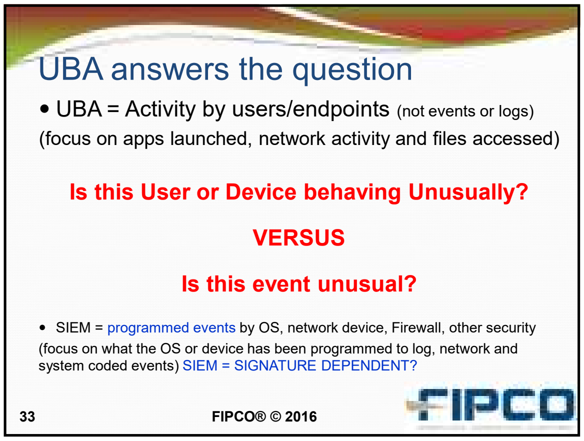
UEBA (UBA) – What is it : Definition?

- User and Entity Behavior Analytics (UEBA) is the tracking, collecting and assessing user and endpoint data and activities using log monitoring systems. Forrester calls it SUBA (Security User Behavior Analytics)

UBA tools perform two main functions:

1. Identify baseline of "normal" activities specific to the organization and its users/assets.
2. Flag deviations from Baseline

32 FIPCO® © 2016



UBA answers the question

- UBA = Activity by users/endpoints (not events or logs)

(focus on apps launched, network activity and files accessed)

Is this User or Device behaving Unusually?

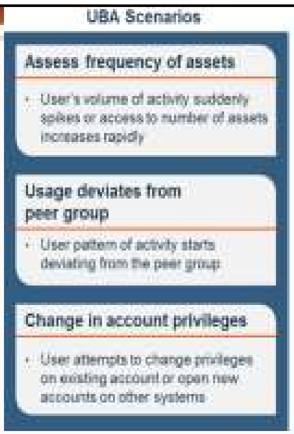
VERSUS

Is this event unusual?

- SIEM = programmed events by OS, network device, Firewall, other security

(focus on what the OS or device has been programmed to log, network and system coded events) SIEM = SIGNATURE DEPENDENT?

33 FIPCO® © 2016



UBA Scenarios

Assess frequency of assets

- User's volume of activity suddenly spikes or access to number of assets increases rapidly

Usage deviates from peer group

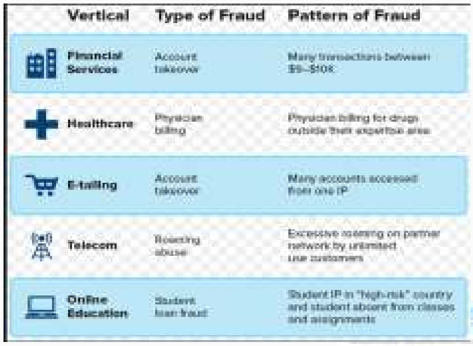
- User pattern of activity starts deviating from the peer group

Change in account privileges

- User attempts to change privileges on existing account or open new accounts on other systems

34

What is a Behavior Anomaly?



Vertical	Type of Fraud	Pattern of Fraud
Financial Services	Account takeover	Many transactions between $5–$10K
Healthcare	Physician billing	Physician billing for drugs outside their expertise area
E-tailing	Account takeover	Many accounts accessed from one IP
Telecom	Roaming abuse	Excessive roaming on partner network by unlimited use customers
Online Education	Student loan fraud	Student IP in "high-risk" country and student absent from classes and assignments

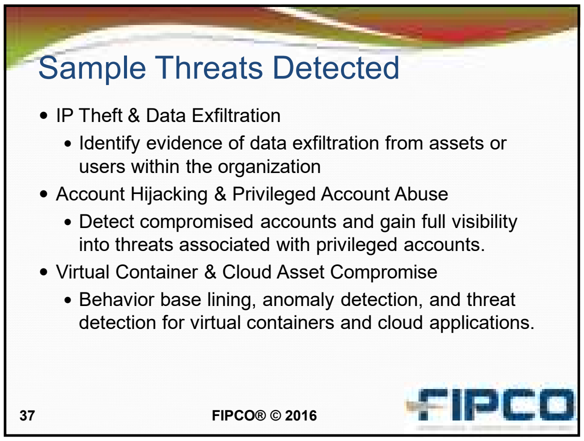
35

Sample Threats Detected

- Privileged Account Abuse – inappropriate usage of access permissions
- Privilege Escalation – transformation of identity and access credentials
- Data Exfiltration – the act of stealing private, confidential and sensitive data within an organization by malware or an attacker
- Unusual Activity – accessing external domains, remotely accessing high privileged assets, and unusual login duration, time or location
- Credential Compromise – stealthy takeover of accounts for malicious purposes

36

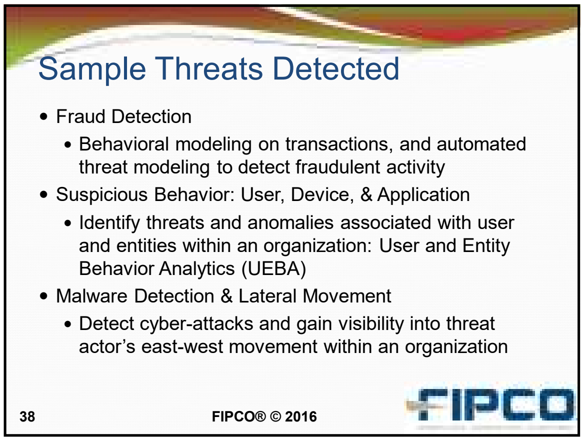
FIPCO® © 2016



Sample Threats Detected

- IP Theft & Data Exfiltration
  - Identify evidence of data exfiltration from assets or users within the organization
- Account Hijacking & Privileged Account Abuse
  - Detect compromised accounts and gain full visibility into threats associated with privileged accounts.
- Virtual Container & Cloud Asset Compromise
  - Behavior base lining, anomaly detection, and threat detection for virtual containers and cloud applications.

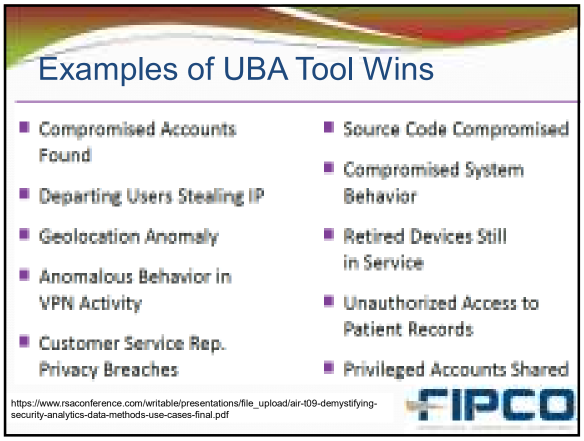
37 FIPCO® © 2016



Sample Threats Detected

- Fraud Detection
  - Behavioral modeling on transactions, and automated threat modeling to detect fraudulent activity
- Suspicious Behavior: User, Device, & Application
  - Identify threats and anomalies associated with user and entities within an organization: User and Entity Behavior Analytics (UEBA)
- Malware Detection & Lateral Movement
  - Detect cyber-attacks and gain visibility into threat actor's east-west movement within an organization

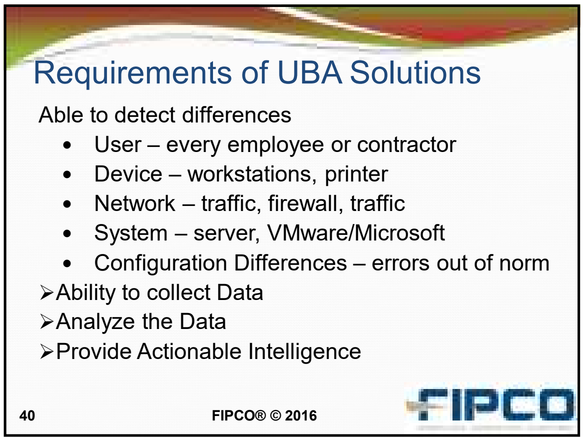
38 FIPCO® © 2016



Examples of UBA Tool Wins

- Compromised Accounts Found
- Departing Users Stealing IP
- Geolocation Anomaly
- Anomalous Behavior in VPN Activity
- Customer Service Rep. Privacy Breaches
- Source Code Compromised
- Compromised System Behavior
- Retired Devices Still in Service
- Unauthorized Access to Patient Records
- Privileged Accounts Shared

https://www.rsaconference.com/writable/presentations/file_upload/air-t09-demystifying-security-analytics-data-methods-use-cases-final.pdf



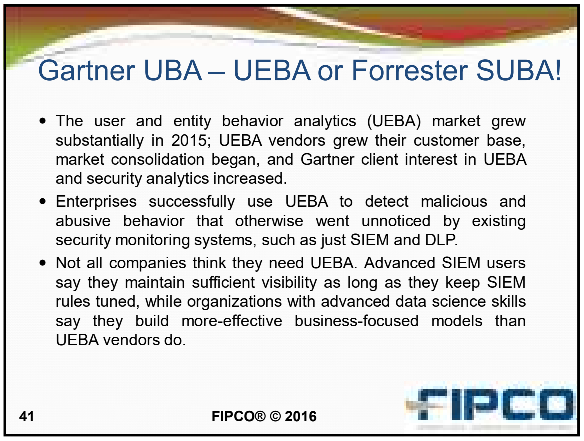
Requirements of UBA Solutions

Able to detect differences

- User – every employee or contractor
- Device – workstations, printer
- Network – traffic, firewall, traffic
- System – server, VMware/Microsoft
- Configuration Differences – errors out of norm

➢Ability to collect Data
➢Analyze the Data
➢Provide Actionable Intelligence

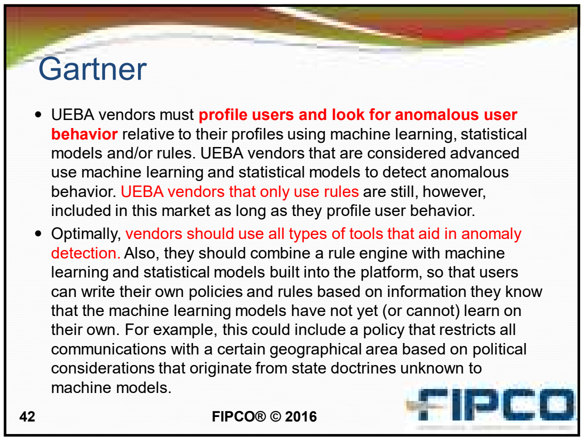
40 FIPCO® © 2016



Gartner UBA – UEBA or Forrester SUBA!

- The user and entity behavior analytics (UEBA) market grew substantially in 2015; UEBA vendors grew their customer base, market consolidation began, and Gartner client interest in UEBA and security analytics increased.
- Enterprises successfully use UEBA to detect malicious and abusive behavior that otherwise went unnoticed by existing security monitoring systems, such as just SIEM and DLP.
- Not all companies think they need UEBA. Advanced SIEM users say they maintain sufficient visibility as long as they keep SIEM rules tuned, while organizations with advanced data science skills say they build more-effective business-focused models than UEBA vendors do.

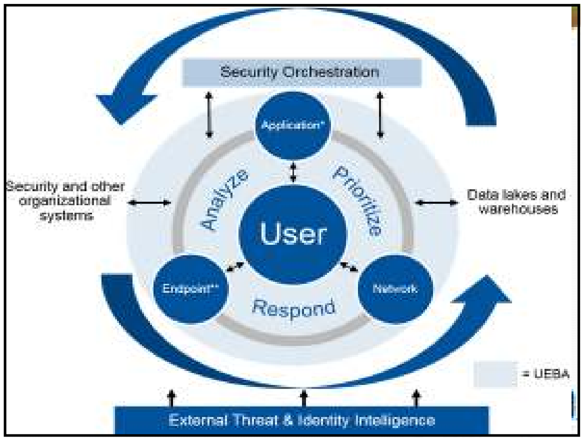
41 FIPCO® © 2016



Gartner

- UEBA vendors must **profile users and look for anomalous user behavior** relative to their profiles using machine learning, statistical models and/or rules. UEBA vendors that are considered advanced use machine learning and statistical models to detect anomalous behavior. UEBA vendors that only use rules are still, however, included in this market as long as they profile user behavior.
- Optimally, vendors should use all types of tools that aid in anomaly detection. Also, they should combine a rule engine with machine learning and statistical models built into the platform, so that users can write their own policies and rules based on information they know that the machine learning models have not yet (or cannot) learn on their own. For example, this could include a policy that restricts all communications with a certain geographical area based on political considerations that originate from state doctrines unknown to machine models.

42 FIPCO® © 2016



Security Orchestration

Application*

Security and other organizational systems

Analyze

User

Prioritize

Data lakes and warehouses

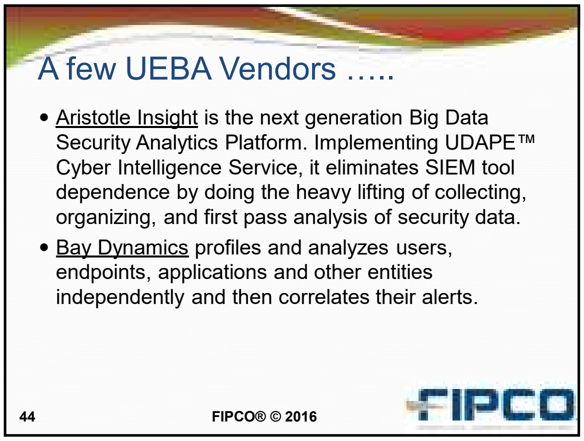
Endpoint**

Respond

Network

= UEBA

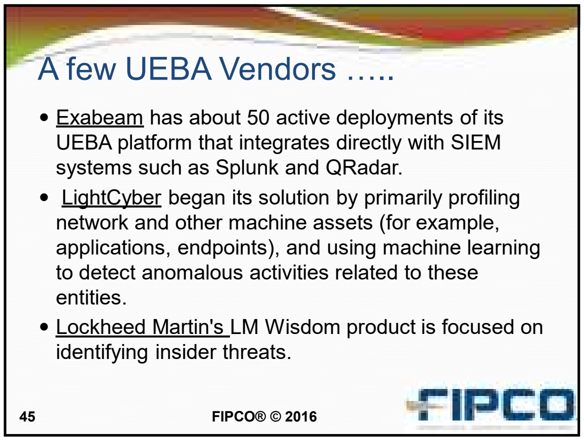
External Threat & Identity Intelligence



A few UEBA Vendors …..

- Aristotle Insight is the next generation Big Data Security Analytics Platform. Implementing UDAPE™ Cyber Intelligence Service, it eliminates SIEM tool dependence by doing the heavy lifting of collecting, organizing, and first pass analysis of security data.
- Bay Dynamics profiles and analyzes users, endpoints, applications and other entities independently and then correlates their alerts.

44 FIPCO® © 2016



A few UEBA Vendors …..

- Exabeam has about 50 active deployments of its UEBA platform that integrates directly with SIEM systems such as Splunk and QRadar.
- LightCyber began its solution by primarily profiling network and other machine assets (for example, applications, endpoints), and using machine learning to detect anomalous activities related to these entities.
- Lockheed Martin's LM Wisdom product is focused on identifying insider threats.

45 FIPCO® © 2016

A few UEBA Vendors …..

- Microsoft's Advanced Threat Analytics (ATA) platform is based on the Aorato software it acquired in November 2014. It provides deep packet inspection of Active Directory traffic, which is captured through port mirroring and data from SIEM tools
- ObserveIT uses an agent-based desktop collection method to monitor desktop and user activity, and it aligns its solutions to the domains of employee monitoring (including privilege users), audit and compliance, insider threat, vendor risk management, and gateway and windows monitoring.

46 FIPCO® © 2016

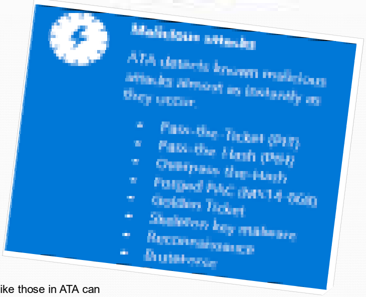
A few UEBA Vendors …..

- Securonix, founded in 2008 and one of the first UEBA vendors, supports behavioral analytics for multiple use cases, such as detecting insider or external threats, for more than 50 enterprises.
- Splunk moved into the UEBA market with its July 2015 acquisition of Caspida, which profiles users, peer groups, endpoints, IP addresses and other entities, and detects anomalies using machine learning and by correlating entity behavior. Most UEBA vendors listed have relatively tight integrations with Splunk, but now Splunk has its own UEBA engine that supplements its existing Enterprise security module
- Varonis uses a rule-based engine and some statistical analysis functions that focus on insider threats and data exfiltration by analyzing users' access to files and their use of email

47 FIPCO® © 2016

Splunk User Behavior Analytics

Microsoft ATA



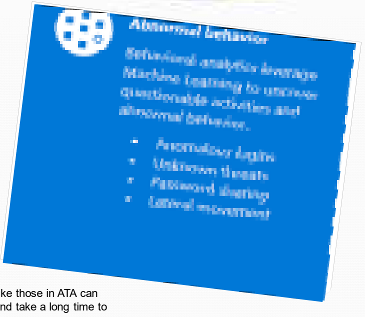
Malicious attacks

ATA detects known malicious attacks almost as instantly as they occur.

- Pass-the-Ticket (PtT)
- Pass-the-Hash (PtH)
- Overpass-the-Hash
- Forged PAC (MS14-068)
- Golden Ticket
- Skeleton key malware
- Reconnaissance
- Brute Force

Behavioral analysis technologies like those in ATA can be extremely tricky to implement and take a long time to deliver impactful information.
https://www.clearswift.com/blog/2015/08/27/microsoft-advanced-threat-analytics-is-it-enough

Microsoft ATA



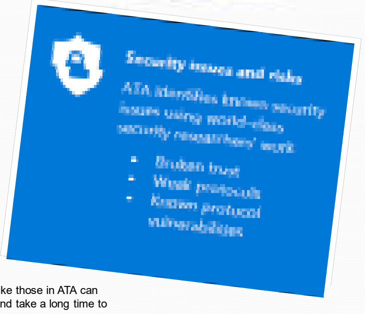
Abnormal behavior

Behavioral analytics leverage Machine Learning to uncover questionable activities and abnormal behavior.

- Anomalous logins
- Unknown threats
- Password sharing
- Lateral movement

Behavioral analysis technologies like those in ATA can be extremely tricky to implement and take a long time to deliver impactful information.
https://www.clearswift.com/blog/2015/08/27/microsoft-advanced-threat-analytics-is-it-enough

Microsoft ATA

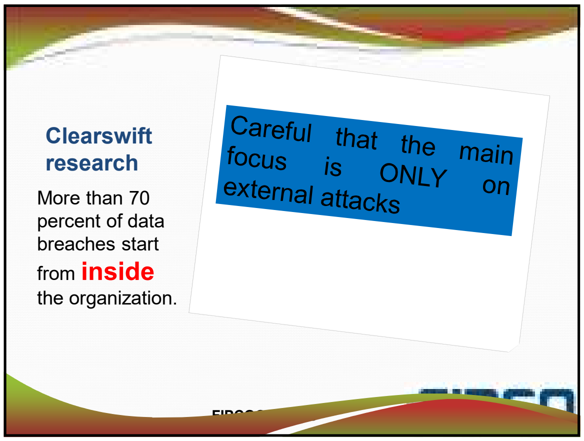


Security issues and risks

ATA identifies known security issues using world-class security researchers' work.

- Broken trust
- Weak protocols
- Known protocol vulnerabilities

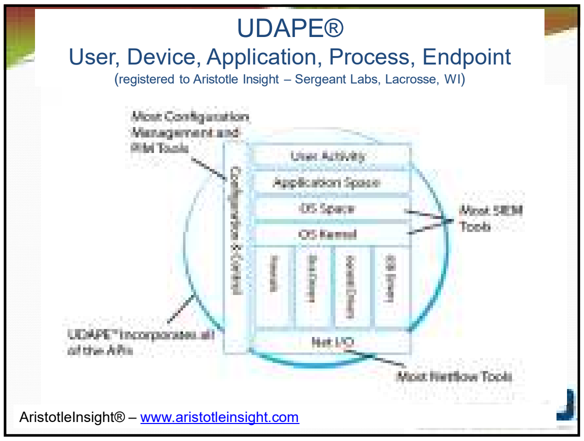
Behavioral analysis technologies like those in ATA can be extremely tricky to implement and take a long time to deliver impactful information.
https://www.clearswift.com/blog/2015/08/27/microsoft-advanced-threat-analytics-is-it-enough



Clearswift research

More than 70 percent of data breaches start from **inside** the organization.

Careful that the main focus is ONLY on external attacks

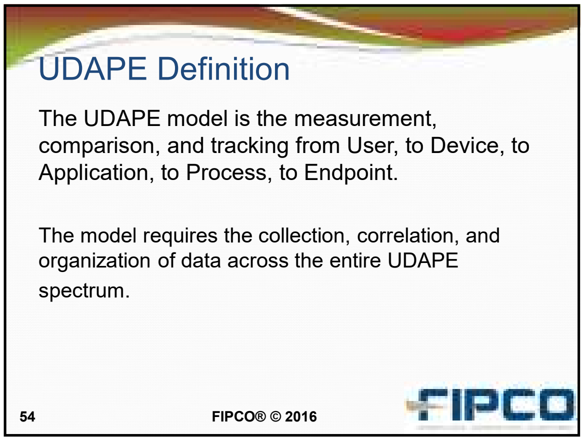


UDAPE®

User, Device, Application, Process, Endpoint

(registered to Aristotle Insight – Sergeant Labs, Lacrosse, WI)

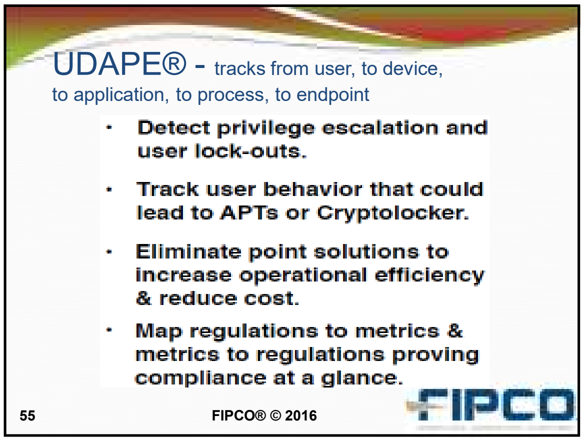
AristotleInsight® – www.aristotleinsight.com



UDAPE Definition

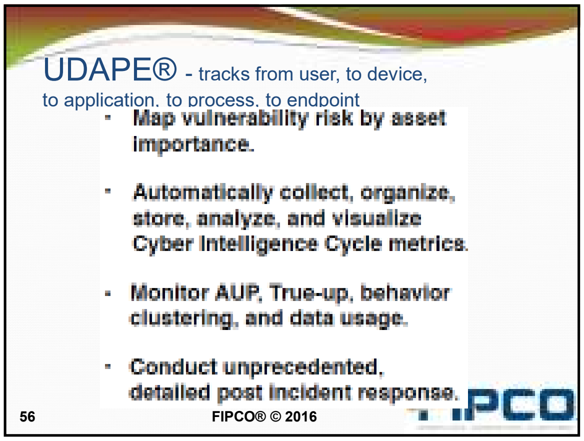
The UDAPE model is the measurement, comparison, and tracking from User, to Device, to Application, to Process, to Endpoint.

The model requires the collection, correlation, and organization of data across the entire UDAPE spectrum.



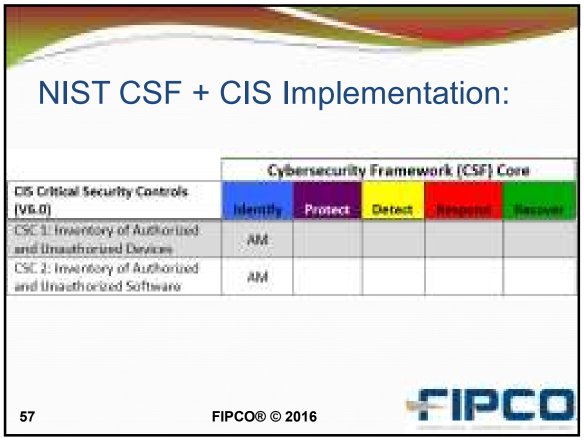
UDAPE® - tracks from user, to device, to application, to process, to endpoint

- Detect privilege escalation and user lock-outs.
- Track user behavior that could lead to APTs or Cryptolocker.
- Eliminate point solutions to increase operational efficiency & reduce cost.
- Map regulations to metrics & metrics to regulations proving compliance at a glance.



UDAPE® - tracks from user, to device, to application, to process, to endpoint

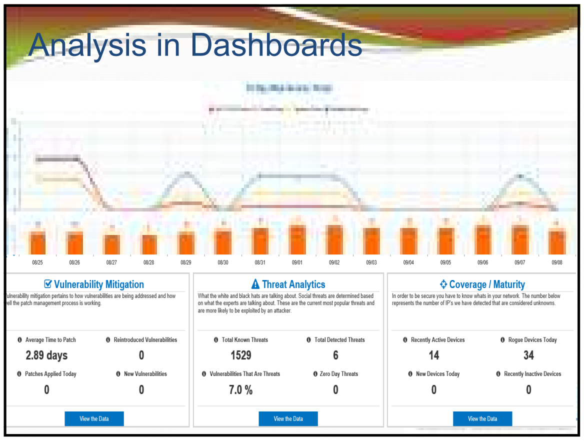
- Map vulnerability risk by asset importance.
- Automatically collect, organize, store, analyze, and visualize Cyber Intelligence Cycle metrics.
- Monitor AUP, True-up, behavior clustering, and data usage.
- Conduct unprecedented, detailed post incident response.



NIST CSF + CIS Implementation:

	Cybersecurity Framework (CSF) Core				
CIS Critical Security Controls (V6.0)	Identify	Protect	Detect	Respond	Recover
CSC 1: Inventory of Authorized and Unauthorized Devices	AM				
CSC 2: Inventory of Authorized and Unauthorized Software	AM				

Asset Inventory



Analysis in Dashboards

☑ Vulnerability Mitigation

ulnerability mitigation pertains to how vulnerabilities are being addressed and how ell the patch management process is working.

Average Time to Patch	Reintroduced Vulnerabilities
2.89 days	0
Patches Applied Today	New Vulnerabilities
0	0

View the Data

Threat Analytics

What the white and black hats are talking about. Social threats are determined based on what the experts are talking about. These are the current most popular threats and are more likely to be exploited by an attacker.

Total Known Threats	Total Detected Threats
1529	6
Vulnerabilities That Are Threats	Zero Day Threats
7.0 %	0

View the Data

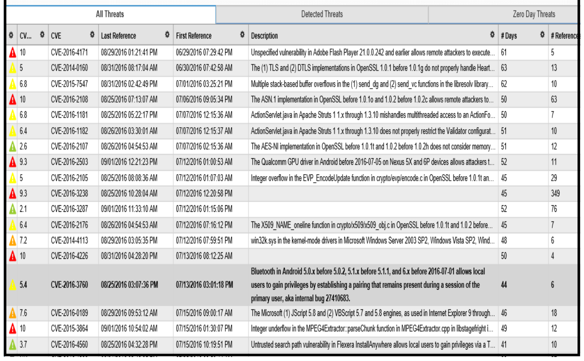
Coverage / Maturity

In order to be secure you have to know whats in your network. The number below represents the number of IP's we have detected that are considered unknowns.

Recently Active Devices	Rogue Devices Today
14	34
New Devices Today	Recently Inactive Devices
0	0

View the Data

Threat Detail



	CV...	CVE	Last Reference	First Reference	Description	# Days	# Reference
▲	10	CVE-2016-4171	08/29/2016 01:21:41 PM	06/29/2016 07:29:42 PM	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier allows remote attackers to execute...	61	5
▲	5	CVE-2014-0160	08/31/2016 08:17:04 AM	06/30/2016 07:42:58 AM	The (1) TLS and (2) DTLS implementations in OpenSSL 1.0.1 before 1.0.1g do not properly handle Heart...	63	13
▲	6.8	CVE-2015-7547	08/31/2016 02:42:49 PM	07/01/2016 03:25:21 PM	Multiple stack-based buffer overflows in the (1) send_dg and (2) send_vc functions in the libresolv library...	62	10
▲	10	CVE-2016-2108	08/25/2016 07:13:07 AM	07/06/2016 09:05:34 PM	The ASN.1 implementation in OpenSSL before 1.0.1o and 1.0.2 before 1.0.2c allows remote attackers to...	50	63
▲	6.8	CVE-2016-1181	08/25/2016 05:22:17 PM	07/07/2016 12:15:36 AM	ActionServlet.java in Apache Struts 1 1.x through 1.3.10 mishandles multithreaded access to an ActionFo...	50	7
▲	6.4	CVE-2016-1182	08/26/2016 03:30:01 AM	07/07/2016 12:15:37 AM	ActionServlet.java in Apache Struts 1 1.x through 1.3.10 does not properly restrict the Validator configurat...	51	10
▲	2.6	CVE-2016-2107	08/26/2016 04:54:53 AM	07/07/2016 02:15:36 AM	The AES-NI implementation in OpenSSL before 1.0.1t and 1.0.2 before 1.0.2h does not consider memory...	51	12
▲	9.3	CVE-2016-2503	09/01/2016 12:21:23 PM	07/12/2016 01:00:53 AM	The Qualcomm GPU driver in Android before 2016-07-05 on Nexus 5X and 6P devices allows attackers t...	52	11
▲	5	CVE-2016-2105	08/25/2016 08:08:36 AM	07/12/2016 01:07:03 AM	Integer overflow in the EVP_EncodeUpdate function in crypto/evp/encode.c in OpenSSL before 1.0.1t an...	45	29
▲	9.3	CVE-2016-3238	08/25/2016 10:28:04 AM	07/12/2016 12:20:58 PM		45	349
▲	2.1	CVE-2016-3287	09/01/2016 11:33:10 AM	07/12/2016 01:15:06 PM		52	76
▲	6.4	CVE-2016-2176	08/26/2016 04:54:53 AM	07/12/2016 07:16:12 PM	The X509_NAME_oneline function in crypto/x509/x509_obj.c in OpenSSL before 1.0.1t and 1.0.2 before...	45	7
▲	7.2	CVE-2014-4113	08/29/2016 03:05:35 PM	07/12/2016 07:59:51 PM	win32k.sys in the kernel-mode drivers in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Wind...	48	6
▲	10	CVE-2016-4226	08/31/2016 04:28:20 PM	07/13/2016 08:12:25 AM		50	4
▲	5.4	CVE-2016-3760	08/25/2016 03:07:36 PM	07/13/2016 03:01:18 PM	Bluetooth in Android 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-07-01 allows local users to gain privileges by establishing a pairing that remains present during a session of the primary user, aka internal bug 27410683.	44	6
▲	7.6	CVE-2016-0189	08/29/2016 09:53:12 AM	07/15/2016 09:00:17 AM	The Microsoft (1) JScript 5.8 and (2) VBScript 5.7 and 5.8 engines, as used in Internet Explorer 9 through...	46	18
▲	10	CVE-2015-3864	09/01/2016 10:54:02 AM	07/15/2016 01:30:07 PM	Integer underflow in the MPEG4Extractor::parseChunk function in MPEG4Extractor.cpp in libstagefright i...	49	12
▲	3.7	CVE-2016-4560	08/25/2016 04:32:28 PM	07/15/2016 10:19:51 PM	Untrusted search path vulnerability in Flexera InstallAnywhere allows local users to gain privileges via a T...	41	10

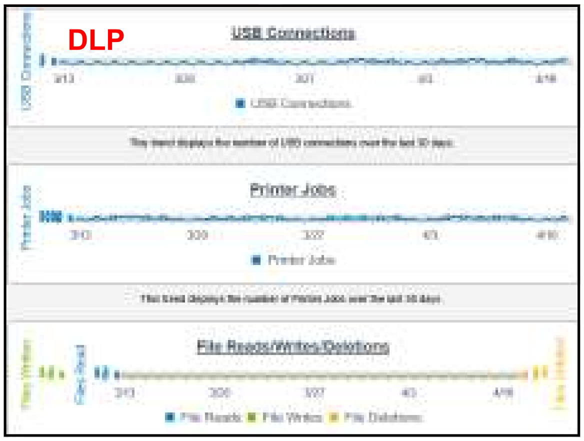
Hunt Teams
Informed security decisions

The FBI’s Cyber Intelligence Cycle:

- Collect,
- Organize,
- Store,
- Analyze, and
- Visualize

Track activity from user, to device, to application, to process, to endpoint.

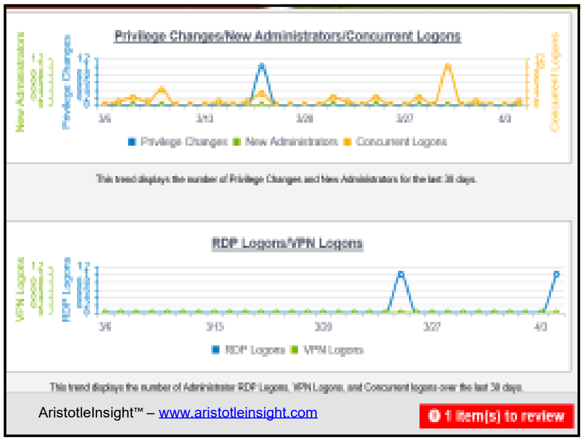
Monitoring the integrity of your assets, specifically configurations, is vital to ensuring your network is secure and operating efficiently. These configurations include monitoring th status of group policy to ensure all devices are in sync with the latest GPOs and keeping an accurate inventory of audit policy settings for all devices, so Windows event logs are properly generated when important events occur.



DLP

This trend displays the number of USB connections over the last 30 days.

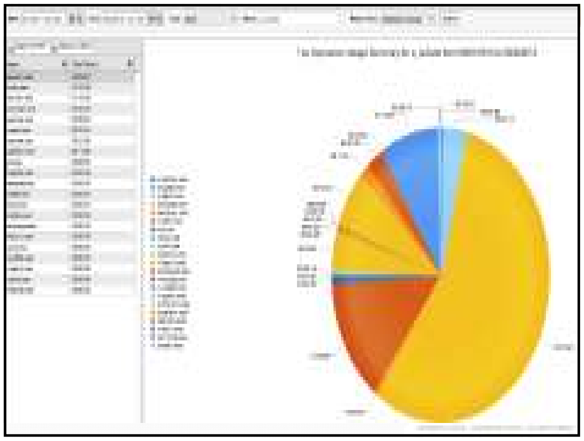
This trend displays the number of Printer Jobs over the last 30 days.

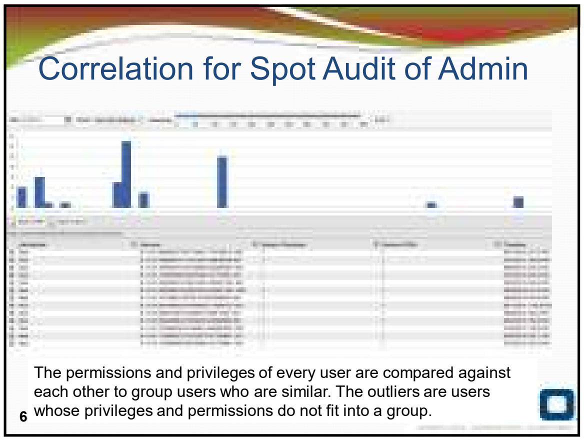


This trend displays the number of Privilege Changes and New Administrators for the last 30 days.

This trend displays the number of Administrator RDP Logons, VPN Logons, and Concurrent logons over the last 30 days.

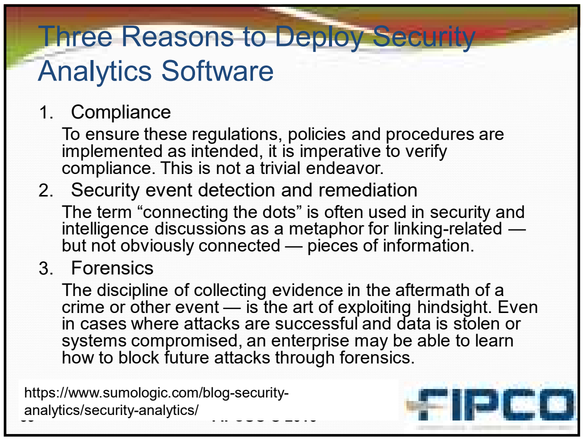
AristotleInsight™ – www.aristotleinsight.com





Correlation for Spot Audit of Admin

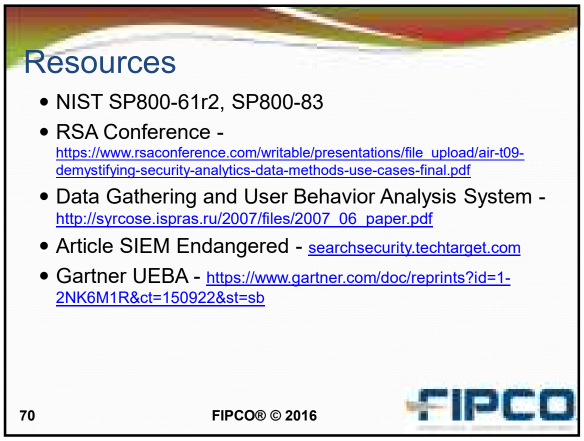
The permissions and privileges of every user are compared against each other to group users who are similar. The outliers are users whose privileges and permissions do not fit into a group.



Three Reasons to Deploy Security Analytics Software

1. Compliance
   To ensure these regulations, policies and procedures are implemented as intended, it is imperative to verify compliance. This is not a trivial endeavor.
2. Security event detection and remediation
   The term “connecting the dots” is often used in security and intelligence discussions as a metaphor for linking-related — but not obviously connected — pieces of information.
3. Forensics
   The discipline of collecting evidence in the aftermath of a crime or other event — is the art of exploiting hindsight. Even in cases where attacks are successful and data is stolen or systems compromised, an enterprise may be able to learn how to block future attacks through forensics.

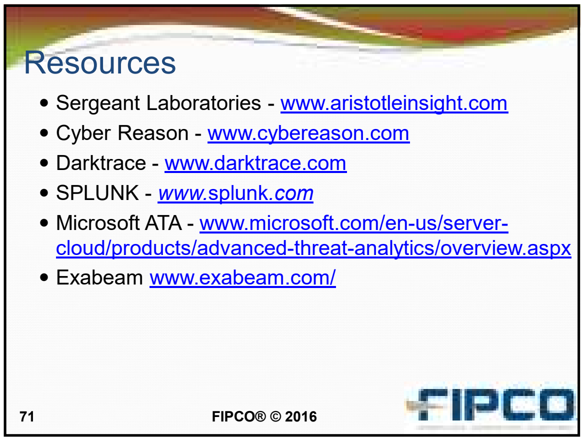
https://www.sumologic.com/blog-security-analytics/security-analytics/



Resources

- NIST SP800-61r2, SP800-83
- RSA Conference - https://www.rsaconference.com/writable/presentations/file_upload/air-t09-demystifying-security-analytics-data-methods-use-cases-final.pdf
- Data Gathering and User Behavior Analysis System - http://syrcose.ispras.ru/2007/files/2007_06_paper.pdf
- Article SIEM Endangered - searchsecurity.techtarget.com
- Gartner UEBA - https://www.gartner.com/doc/reprints?id=1-2NK6M1R&ct=150922&st=sb

70 FIPCO® © 2016



Resources

- Sergeant Laboratories - www.aristotleinsight.com
- Cyber Reason - www.cybereason.com
- Darktrace - www.darktrace.com
- SPLUNK - *www.splunk.com*
- Microsoft ATA - www.microsoft.com/en-us/server-cloud/products/advanced-threat-analytics/overview.aspx
- Exabeam www.exabeam.com/

71 FIPCO® © 2016

Questions & Discussion

CLICK HERE

72 FIPCO® © 2016