UEBA™
User Entity Behavior Analytics
Aristotle Insight
Sergeant Laboratories

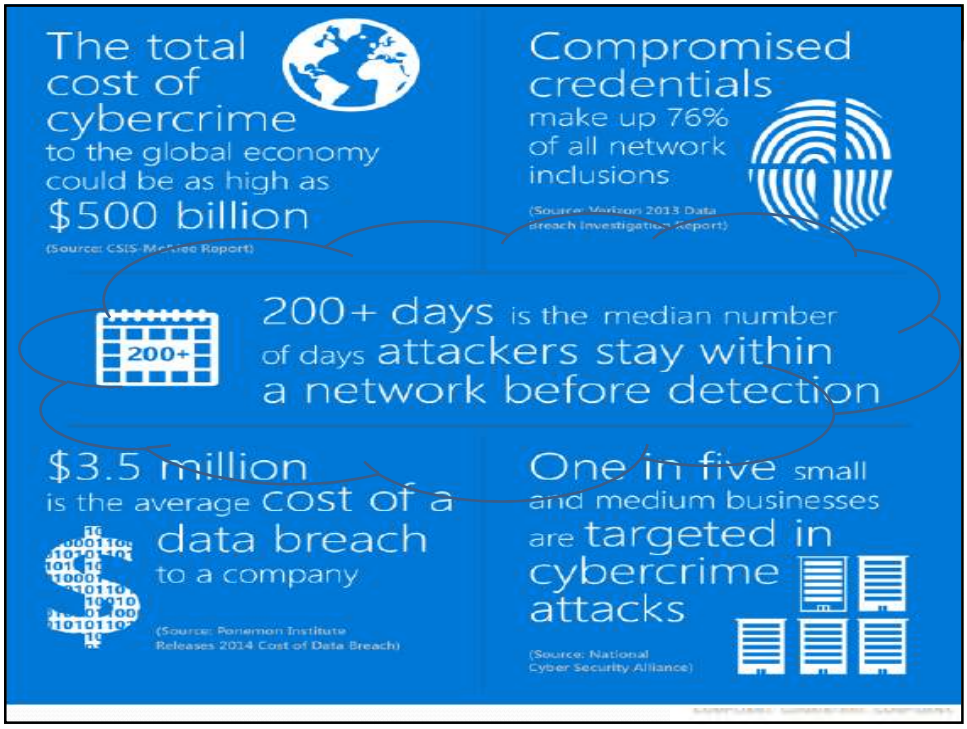
20+ Year Old organically grown company from the Silicon Technology Belt right here in the Midwest – Lacrosse Wisconsin.

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

DISCLAIMER

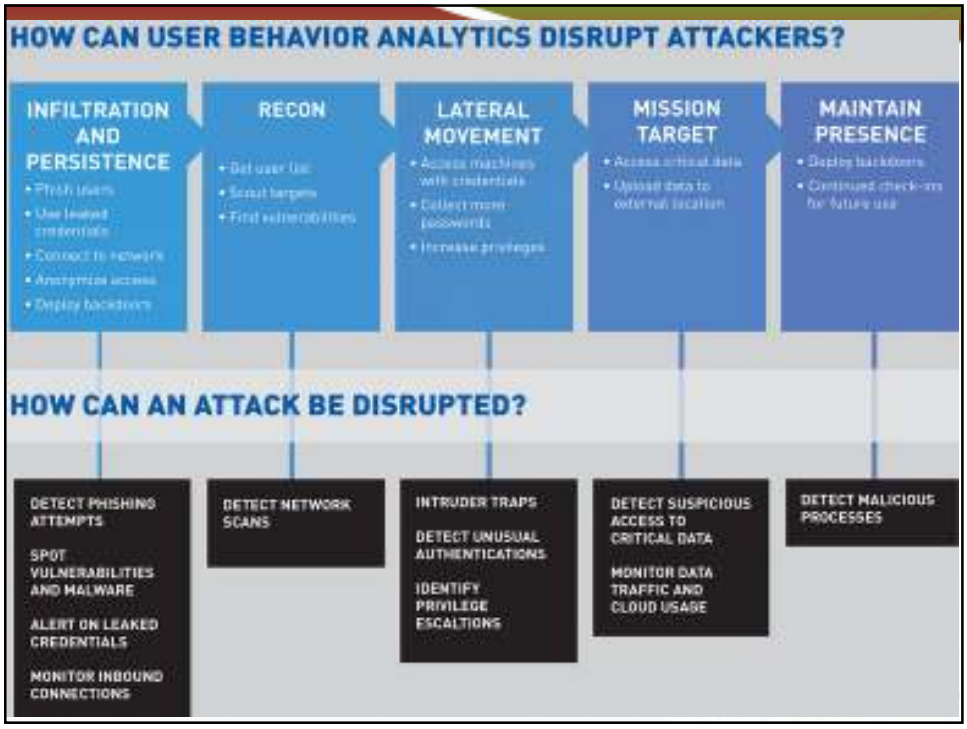
- Statements describing solutions may be made in general terms during this presentation.
- We understand that some products may provide options and cross over between industry segments such as SIEM/SEM/SIM or UEBA.
- Presenter is not an expert on SIEM/UEBA or extremely technical.

Statements made during this presentation are the opinions of the presenter and may not represent any vendor or other industry expertise.



CYBERscape – The Security Sector

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



SANS Top 5 - Why Collect and Analyze?

1. Detection/prevention
2. Ensure and Meet regulatory Compliance
2. Forensic analysis and correlation
3. Track suspicious behavior
4. IT troubleshooting and network operations

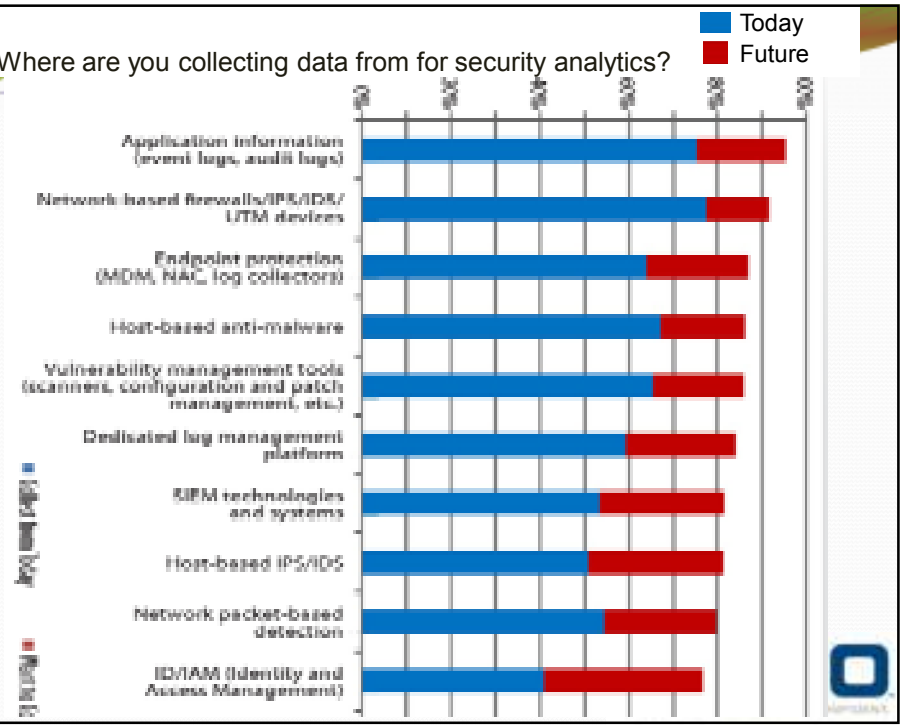
SANS Sixth Annual Log Management Survey Report
Copyright SANS.. https://www.sans.org/reading-room/whitepapers/analyst/sixth-annual-log-management-survey-report-34880

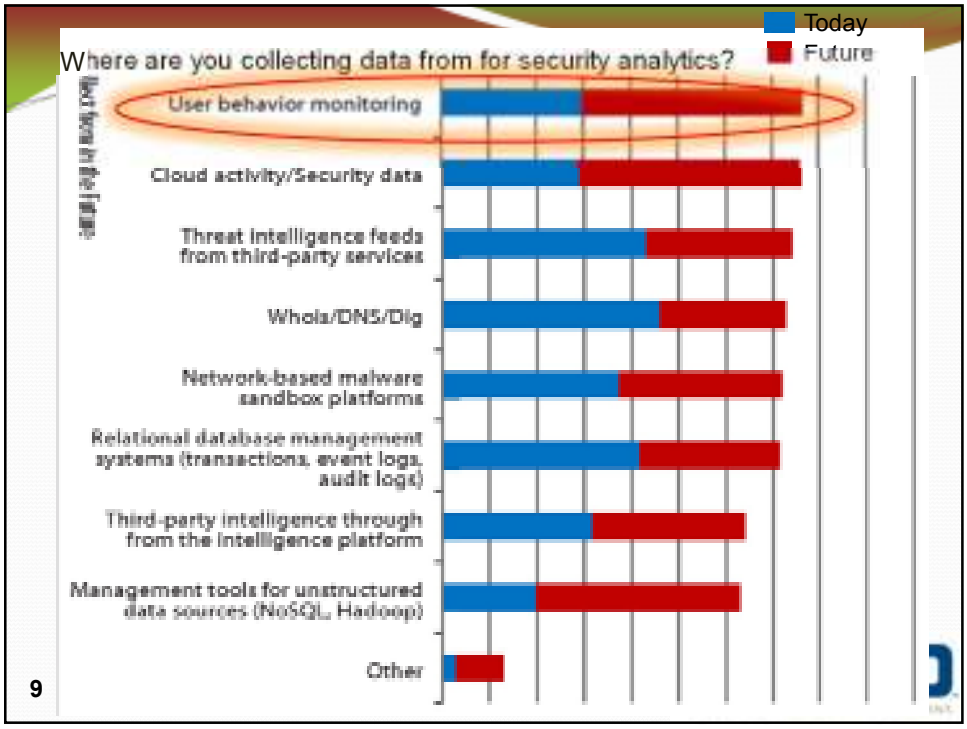
Collecting Events

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

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

Where are you collecting data from for security analytics?





Traditional
Collecting Events and Alerting

Example Event/Log Data Repositories

- SIEM – SEM
  - IBM Qradar
  - HP Arcsight
  - Solarwinds
  - Logrythm
  - Splunk (has added new layers)
  - Numerous others……

Collecting Events and Maybe Reporting

Core and Critical Applications

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

Collecting Events and Maybe Reporting

SIEM systems regularly used to see as many as 15,000 events per second.

Now; 80,000 events per second is not uncommon…..

What Percentage of Event offer Value?

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 management system.
- collects logs and other security related documentation for analysis, some begin to correlate..

What are other Experts Saying?

- SEM or EM was just aggregating events from operating systems and infrastructure devices (e.g. firewall) – provided some centralized logging….
- SIEM began monitoring the security of applications and correlation
- Next generation analysis needs to detect and predict threats based on the behavior across systems – identify based on changes from normal versus depend just on what was logged….
- Threat Intelligence inputs….

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

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 – 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

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

Gartner UBA – UEBA!

- 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.

UEBA – 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.

UEBA tools perform two main functions:

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

Address Behavior, Not Rules

- 200+ days = the average amount of time attackers reside inside a network before detection

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

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

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.

UEBA answers the question

- 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?

Requirements of UEBA Solutions

Able to detect differences

- User – every employee or contractor
- Device – workstations, printer
- Network – traffic, firewall, traffic
- System – server, VMware/Microsoft

➢Ability to collect Data

➢Analyze the Data

➢Provide Actionable Intelligence

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

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 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!

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.

AristotleInsight provides the information derived from big data sources in ways that can be readily and rapidly identified by security analysts.

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.

AristotleInsight provides a DataVault™ appliance that stores years worth of history.

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 Infosecurity professionals and limiting their ability to discern key events.

   A framework like AristotleInsight provides the data in the context of users, devices and events.

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.

AristotleInsight spans the silos, leaves no holes in visibility and puts no discernable strain on the network.

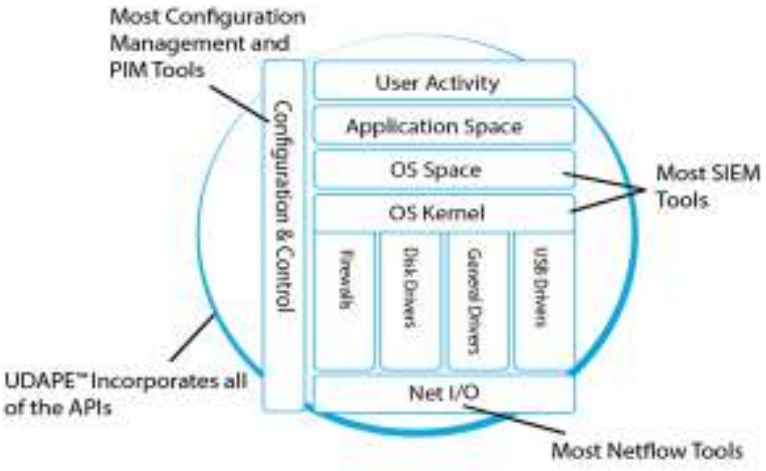
Clearswift research

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
(AristotleInsight – Sergeant Labs)



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.
- Collection, correlation, and organization of data across the entire UDAPE spectrum.
- Concentrated on the collection of data, no negative affect.
- Work across desktop, mobile, embedded devices and cloud. In the FOG!!
- **Use the Kernel not the application, system, DB, infrastructure device programmed events ONLY.**

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				

Vulnerability History to Standards

Vulnerability Monthly Statistics

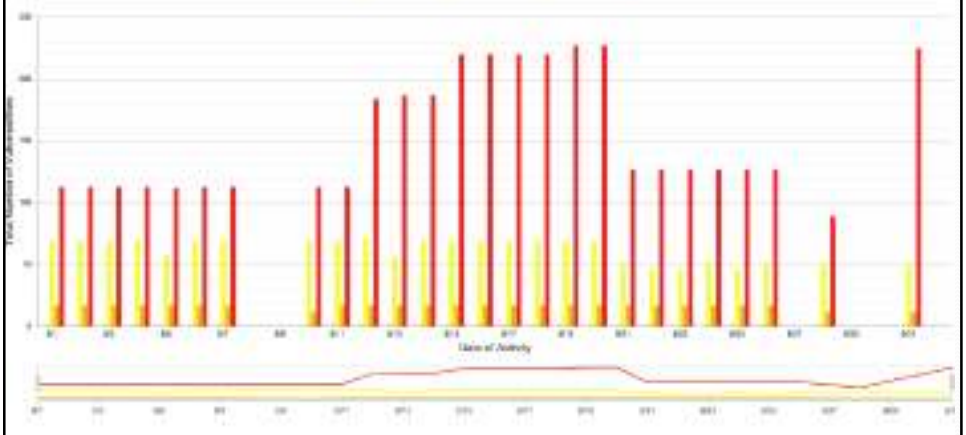


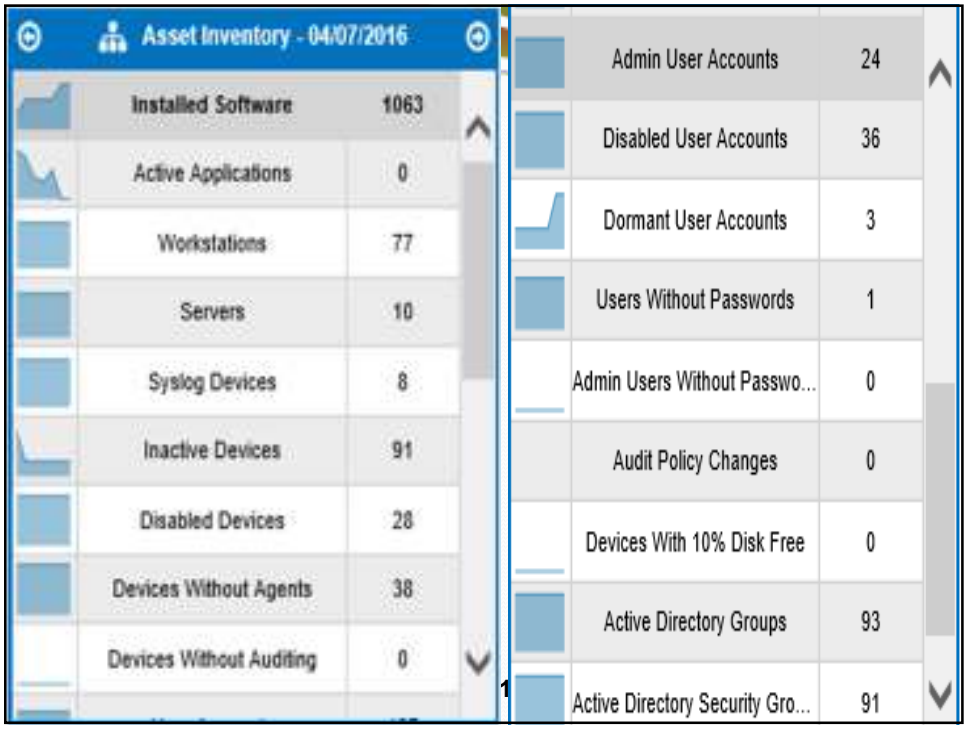
Figure 4: *A trend graph for the month of August showing total vulnerabilities installed within the IT environment*

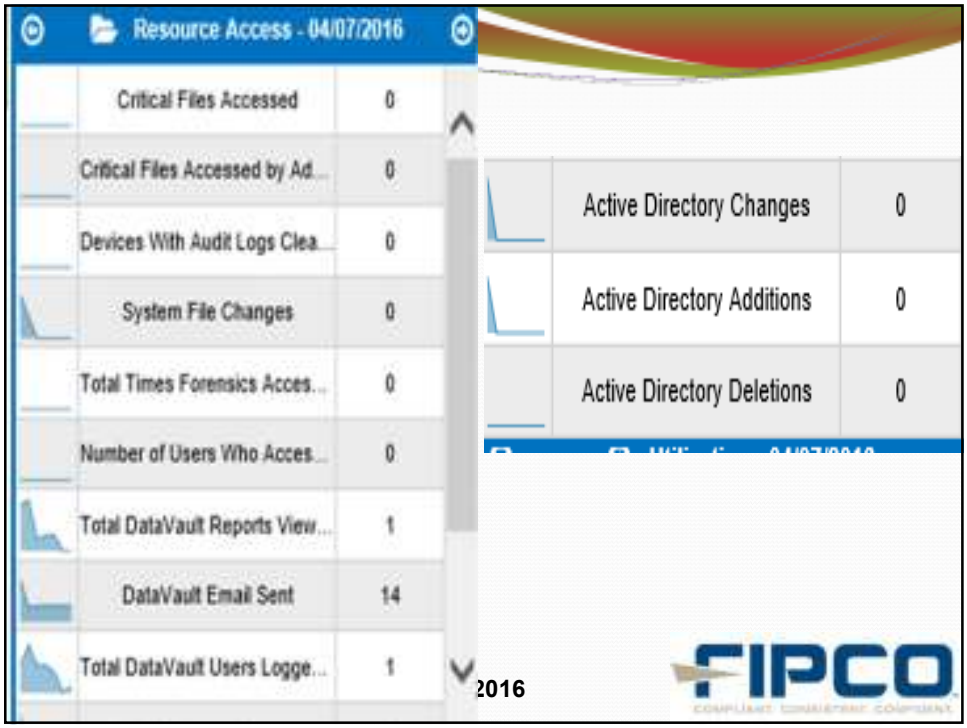
Hunt Teams
Informed security decisions

The FBI's Cyber Intelligence Cycle:

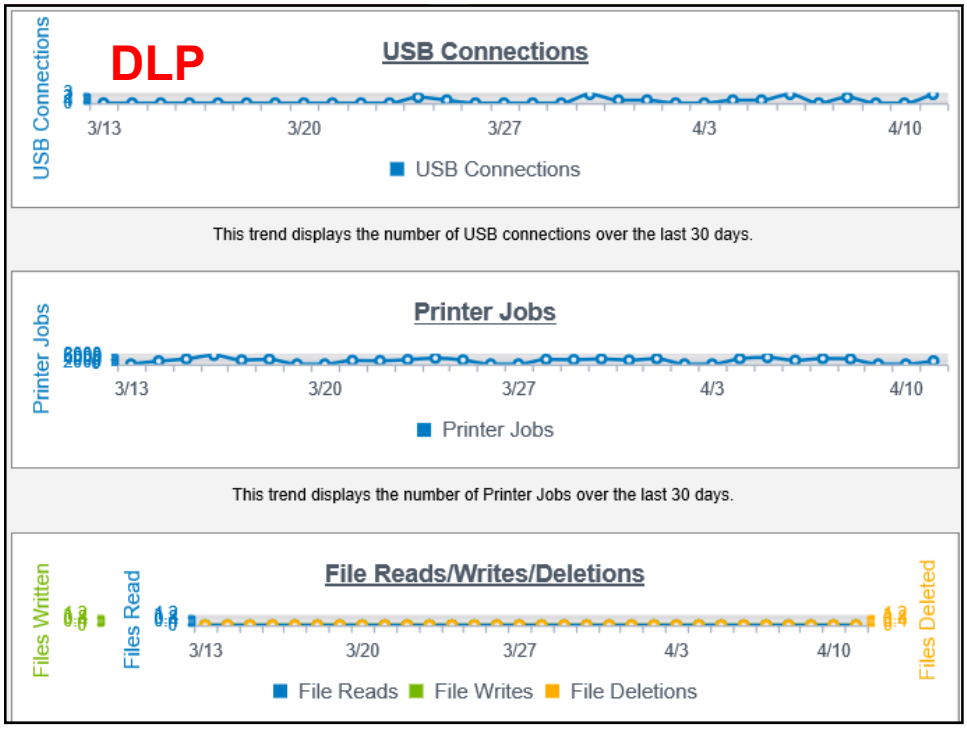
- Collect,
- Organize,
- Store,
- Analyze, and
- Visualize

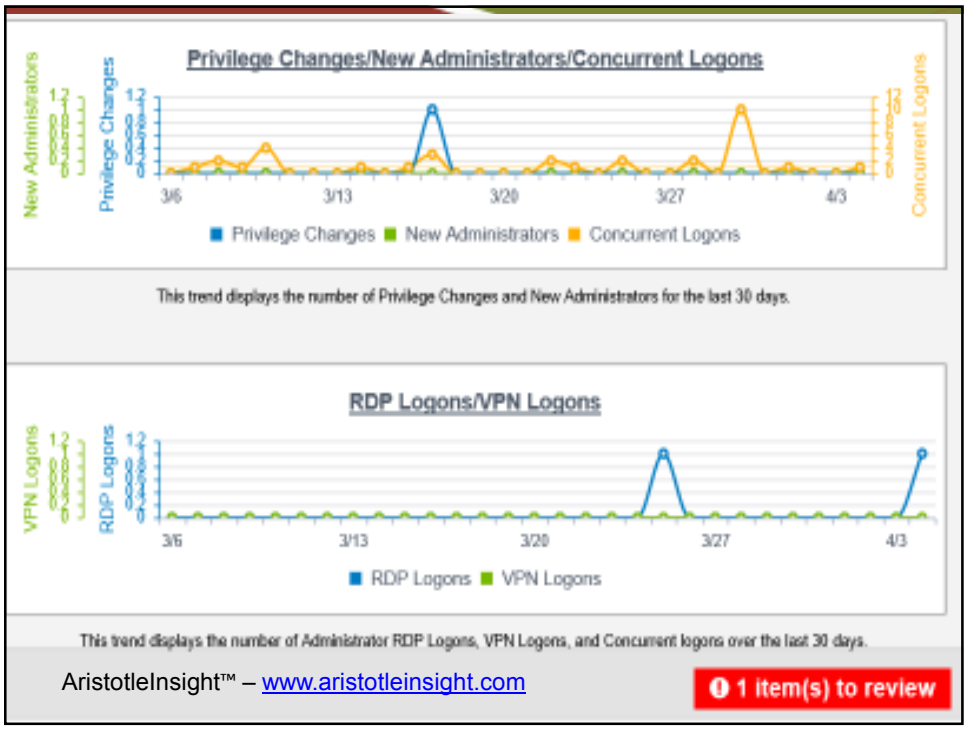
Track activity from user, to device, to application, to process, to endpoint.

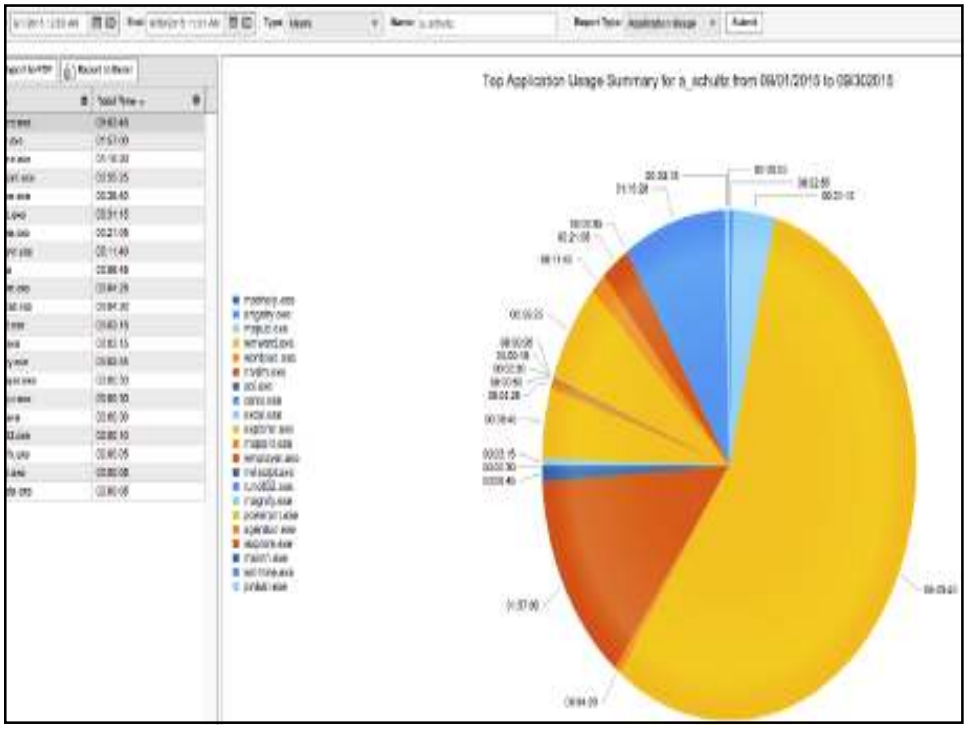



Resource Access - 04/07/2016
Critical Files Accessed 0
Critical Files Accessed by Ad... 0
Devices With Audit Logs Clea... 0
System File Changes 0
Total Times Forensics Acces... 0
Number of Users Who Acces... 0
Total DataVault Reports View... 1
DataVault Email Sent 14
Total DataVault Users Logge... 1
Active Directory Changes 0
Active Directory Additions 0
Active Directory Deletions 0
2016
FIPCO

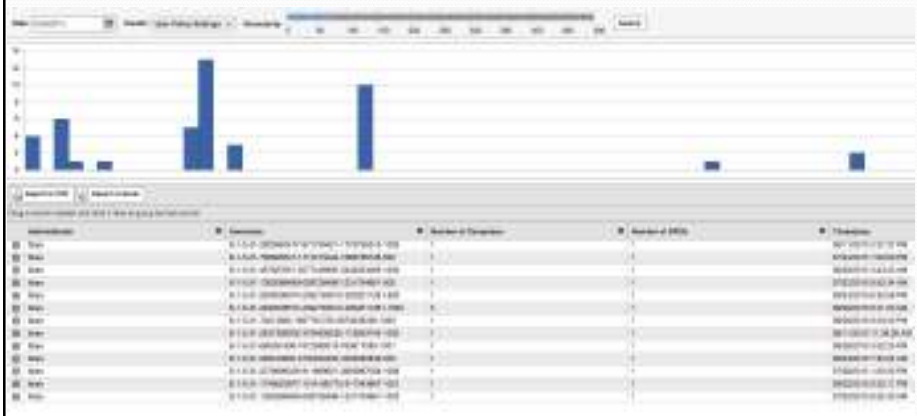

Integrity Drift
3 item(s) to review
Monitoring the integrity of your assets, specifically configurations, is vital to ensuring your network is secure and operating efficiently. These configurations include monitoring th
status of group policy to ensure all devices are in sync with the latest GPOs and keeping an accurate inventory of audit policy settings for all devices, so Windows event logs are
properly generated when important events occur.
Group Policy Changes: 1335
Group Policy Errors: 1
Group Policy Conflicts: 3
Audit Policies: 0
Group Policy Changes
Group Policy Changes
Group Policy Errors/Conflicts
Group Policy Errors
Group Policy Conflicts
Audit Policies


DLP
USB Connections
USB Connections
3/13
3/20
3/27
4/3
4/10
USB Connections
This trend displays the number of USB connections over the last 30 days.
Printer Jobs
Printer Jobs
3/13
3/20
3/27
4/3
4/10
Printer Jobs
This trend displays the number of Printer Jobs over the last 30 days.
File Reads/Writes/Deletions
Files Written
Files Read
Files Deleted
3/13
3/20
3/27
4/3
4/10
File Reads
File Writes
File Deletions


Privilege Changes/New Administrators/Concurrent Logons
New Administrators
Privilege Changes
Concurrent Logons
3/6
3/13
3/20
3/27
4/3
Privilege Changes
New Administrators
Concurrent Logons
This trend displays the number of Privilege Changes and New Administrators for the last 30 days.
RDP Logons/VPN Logons
VPN Logons
RDP Logons
3/6
3/13
3/20
3/27
4/3
RDP Logons
VPN Logons
This trend displays the number of Administrator RDP Logons, VPN Logons, and Concurrent logons over the last 30 days.
AristotleInsight™ – www.aristotleinsight.com
1 item(s) to review



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.

4

Technical Compatibility

- PUPPET Development Compatible - configuration of Unix-like and Microsoft Windows systems, user describes system resources and their state, either using Puppet's declarative language or a Ruby DSL (domain-specific language). information is stored in files called "Puppet manifests". Puppet discovers the system information via a utility called Facter, and compiles the Puppet manifests into a system-specific catalog containing resources and resource dependency, which are applied against the target systems. Any actions taken by Puppet are then reported.

Technical Compatibility

- Chef Development Kit Compatible - Chef is a configuration management tool written in Ruby and Erlang. It uses a pure-Ruby, domain-specific language (DSL) for writing system configuration "recipes". Chef is used to streamline the task of configuring and maintaining a company's servers, and can integrate with cloud-based platforms such as Rackspace, Internap, Amazon EC2, Google Cloud Platform, OpenStack, SoftLayer, and Microsoft Azure to automatically provision and configure new machines. Chef contains solutions for both small and large scale systems, with features and pricing for the respective ranges.

Resources

- NIST SP800-61r2,
- NIST SP800-83
- Sergeant Laboratories - www.aristotleinsight.com
- Article SIEM Endangered - searchsecurity.techtarget.com
- Chef DK - downloads.chef.io/chef-dk/
- PUPPET - puppet.com/blog/test-driven-development-puppet

Consider a Local Behavior Analysis Reporting Tool – Aristotle Insight, www.aristotleinsight.com

CLICK HERE