ManageEngine

Webinar

The art of real-time incident detection and preemption

Siddharth Sharath Kumar

Recap - Part 1

- Cyberattacks 2018 & 2019—Malware, Ransomware, DDoS, Zero day exploits, Man-in-the-middle attacks
- Cybersecurity challenges—Complex devices and applications, cloud security challenges, evolving users
- How can UEM make a difference in tackling data breaches
- UEM best practices for 2019
- Overview of an insider attack—Insider threat kill chain, scope, categories and security risks
- Key findings on insider threats, predictions for 2019, and how privileged access plays a crucial role
- Capabilities that a perfect PIM solution should contain

Webinar agenda

- An overview of today's IT security landscape
- The importance of SIEM in IT security
- Security auditing best practices
- SIEM use cases
- Tracking insider threats
- Streamlining incident response
- Latest trends in SIEM

Challenges faced by security teams today

- Cloud adoption
- Cutting-edge cyber attacks such as ransomware
- Internal threats
- IoT (Internet of things)
- New data protection regulations

How do we approach the problem?

- Measures to reduce the chance of being breached (patching, identity management etc.)
- **Measures to detect and respond to security threats - SIEM (security information and event management)**
- Steps to recover from an attack

Consider this scenario

- John is a regular end user from your sales team

  John is added to the **Domain Admins** group in Active Directory

  Problem?

Track important security events

- 4728 – Member added to security enabled global group
- 4732 – Member added to security enabled local group
- 4756 – Member added to security enabled universal group

Why do you need the audit trail?

- To know exactly what is going on in your network
- Who is accessing and modifying your files and folders?
- Which user accounts have been locked out and why?
- Were any critical changes made to my Domain Controller/network devices?
- Is there unusual activity on my database/web server? Privilege abuse? Or an attack like SQL injection?

What are my log sources?

- Workstations
- Servers
- Domain Controllers
- Network devices - firewalls, routers and switches
- IDS/IPS
- Endpoint security solutions
- Databases
- Web servers
- Public cloud platforms

Three crucial aspects of SIEM

- **Audit reports** to periodically review security events and demonstrate compliance
- Set up **alerts** to investigate events of interest
- Leverage **event correlation and analytics** to detect and mitigate advanced attacks

ManageEngine

Log360

ManageEngine

EventLog Analyzer

ManageEngine

ADAudit Plus

Scheduling daily reports

- Track events based on severity
- Audit privileged user activities
- Monitor firewall traffic
- Review login activity
- Review file/folder/database activity (accesses, modifications)
- Check web server usage
- Configuration changes

All File or Folder Changes

(From May 22,2017 11:12:08 AM to May 23,2017 11:12:08 AM)

Domain: fap.adap.internal.com

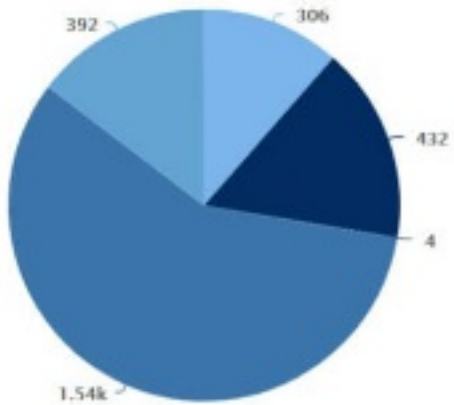
Period: Last 24 Hours

Hours: All

Export As | Add to | More

All File or Folder Changes

All File Changes



Advanced Search

1-25 of 2675

25

Add/Remove Columns

SERVER	FILE / FOLDER NAME	LOCATION	TIME ACCESSED	ACCESSED BY	MESSAGE	CLIENT MACHINE NAME
FAP-DC1	AlertProfile_7.conf	C:\Program Files\ManageEngine\FileAudit Plus Agent\AlertProfiles\	May 23,2017 10:29:54 AM	ranjith	User 'ranjith' Modified file/folder '\\fap-dc1\f\fileaudit plus agent\alertprofiles\alertprofile_7.conf'.	-

Critical alerts for detecting security threats

- Unauthorized accesses/modifications to sensitive data
- Repeated server shutdowns/restarts
- Multiple login failures/account lockouts
- Security group membership changes
- Firewall rule changes
- Malicious URL interactions
- XSS, SQL injection, and other known attacks

Event correlation

- Correlation rules can detect complex attack patterns by associating events from different log sources
- Leverage the correlation engine to detect logon attacks, installation of suspicious software/services, worm activity, and many other attacks

Latest trends in SIEM

- Threat intelligence
- Public cloud auditing (Office 365, Azure, AWS)
- Advanced correlation rules
- Distributed architecture and SOC
- UBA (user behavior analytics)
- Security orchestration and integrations

UBA (user behavior analytics)

- Instantly detect malicious insiders trying to access/steal sensitive data
- Unsupervised machine learning to profile user behaviors and detect anomalies
- A must have feature to thwart data theft

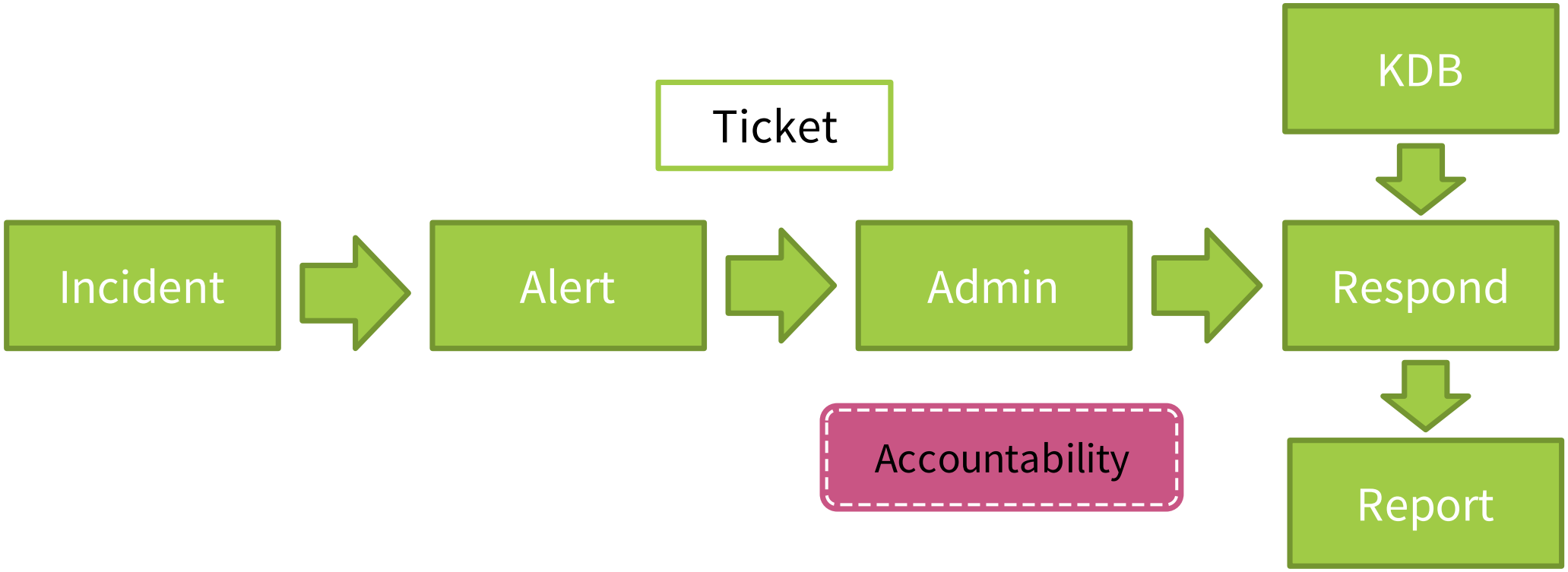
USER NAME	DOMAIN NAME	UNUSUAL HOST ACCESSED	RESOURCE ACCESSED TIME ▼	ACTIVITY TYPE	MESSAGE
surya	adap.internal.com	ADAP-ms1.adap.internal.com	Apr 12,2018 01:26:38 AM	First Time - Host accessed by User	host:ADAP-MS1.adap.internal.com was accessed by user:surya for the first time. Anomaly category:First Time -Host accessed by User

USER NAME	SID	DOMAIN NAME	UNUSUAL ACTIVITY HOUR	TIME GENERATED ▼	GENERAL START TIME	GENERAL END TIME	ACTIVITY TYPE	MESSAGE	ACTIVITY ANALYZER
surya	S-1-5-21-992173265-572275416-1555582462-203614	adap.internal.com	1-2 AM	Apr 12,2018 01:26:38 AM	10 AM	7 PM	Unusual Activity - Logon Time (Based on User)	Logon activity was done by surya within 1-2 AM which deviates from user's normal Logon activity hours:10 AM-7 PM. Anomaly category:Unusual Activity -Logon Time (Based on User)	Details

USER NAME	SID	DOMAIN NAME	UNUSUAL ACTIVITY HOUR	TIME GENERATED ▼	GENERAL START TIME	GENERAL END TIME	ACTIVITY TYPE	MESSAGE	ACTIVITY ANALYZER
surya	S-1-5-21-992173265-572275416-1555582462-203614	adap.internal.com	1-2 AM	Apr 12,2018 01:26:38 AM	1 PM	6 PM	Unusual Activity - File Activity Time	File activity was done by surya within 1-2 AM which deviates from user's normal File activity hours:1 PM-6 PM. Anomaly category:Unusual Activity -File Activity Time	Details

USER NAME	SID	DOMAIN NAME	HOUR OF ACTIVITY	TIME GENERATED ▲	MEAN COUNT	THRESHOLD COUNT	ACTIVITY TYPE	MESSAGE	ACTIVITY ANALYZER
surya	S-1-5-21-992173265-572275416-1555582462-203614	adap.internal.com	1-2 AM	Apr 12,2018 01:32:38 AM	0	10	Unusual Activity - File Activity Count (Based on User)	10+ number of File Activity was done by surya within 1-2 AM. Usual average is 0, Threshold calculated is 10. Anomaly category:Unusual Activity -File Activity Count (Based on User)	Details

Streamlining incident response



Questions?

ManageEngine

www.manageengine.com