ManageEngine
ADSolutions

9th Infocom Security – Athens

Abishek | Technical Evangelist

ManageEngine
ADSolutions

IT Security and Risk: recommendations to safe guard one's IT landscape with SIEM

Abishek | Technical Evangelist

State of IT in Greece

Greece's ICT market is to be around $6.7bn in 2018, the information technology sector accounts for 31% of the ICT market total

HELLENIC REPUBLIC
Ministry of Digital Policy, Telecommunications and Media

How would you feel if you walked into office and

no one remembers you?

Attacks of 2018 and 2017

- Equifax Data Breach – 145.5 Million Accounts
- Uber Data Breach – 57 Million Records
- WannaCry Cyber Attack – 300,000 Systems
- Yahoo Data Breach – 3 *Billion* Accounts
- Deep Root Analytics Data Breach – 198 Million U.S. Voters

The idea of log management is to ~~prevent~~ minimize the impact of new attacks!

What do you see?

1, 1, 2, 3, 5, 8,…. Behavior Patterns

Security holes

Puzzles

What an attacker sees?

What attackers want to be successful?

- Network Access
  - Internet
  - VPN
  - Local network
- Privileged Access
  - Standard user access limits attacks
  - More privileges = more capabilities: Admin priv., permissions, rights
- Weak Security
  - Unpatched systems
  - Password authentication

Don’t be a blind man describing an Elephant

Tools can help us in transforming data

Log management solutions / SIEM (MSSPs)

SIEM Functions

- Log Management
- Correlation and Threat mitigation
- Compliance and Forensic Analysis
- User Behaviour and it’s criticality.

Importance of logs

- Logs
  - Documentation of events
  - All software applications and systems produce log files
- Log management
  - Important for security intelligence
  - Compliance

Correlation

- Pipelining a sequence of Events
- Identify patterns of invisible behavior for a complex threat matrix
- Matching against information specific to your Business

Beauty of Correlation

Correlation is the Difference Between:

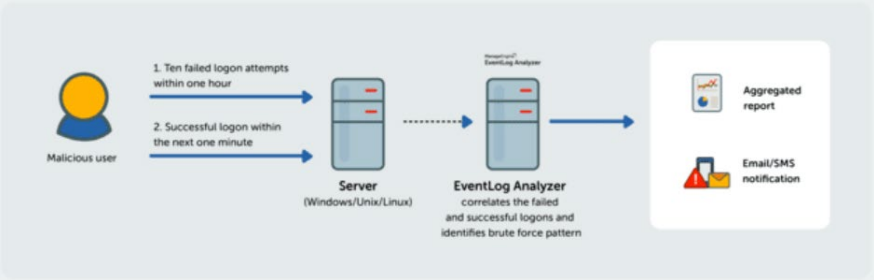
"12:35 11/06/2018 User Jsmith Successful Auth to 10.100.53.125 from 10.10.100.52"

and

"An account belonging to Marketing connected to a System in Finance department from an office desktop, on a day when nobody should be in the office"

Correlation Examples

Brute force attack




User
Behavior
Analytics

Why SIEM and UBA is needed: Lessons learned

- Current processes are failing to catch changes
- Current processes are failing to detect an intrusion
- Example: Marriott breach
  - 500,000,000 accounts affected
  - Initial breach: 2014
  - Discovery of breach: September 2018
  - Determination of breach: Late November 2018
  - 4 years from breach to determination!!!!!!!!

What is AI and UBA?

- User Behavior Analytics (UBA) uses machine learning to create a baseline of activity and also detect anomalies
  - Statistical modelling and unsupervised ML (mainly clustering)
- UBA focuses on what the user is doing: apps launched, logons, and, most critically files accessed
  - UBA creates a baseline of activity
  - Analyzes patterns of usage - indicate unusual or anomalous behavior
  - Activity is analyzed, regardless of who or what initiated it
  - UBA can't prevent hackers or insiders from getting into your system, however it can detect potential attacks to minimize damage

U

user1

All Anomalies

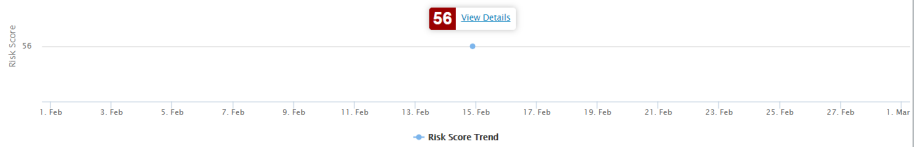
Domain or Host 192.168.2.1

Average Risk Score 56

Peak Risk Score 56

Cards Based Peak Risk Score

Compromised Accounts	15/02/2019 06:59 PM	70
Insider Threats	15/02/2019 06:59 PM	69
Data Exfiltration	16/02/2019 06:59 PM	22



Anomalies contributing to Risk Score

1 - 10 of 44

Date and Time	Anomaly Message	Risk Score
15/02/2019 04:29 PM	Multiple Host Shut Down By User **User :** 192.168.2.1\user1 **Obtained :** 103 events **Threshold :** 14 events	100
15/02/2019 04:29 PM	Multiple Services Installed By User **User :** 192.168.2.1\user1 **Obtained :** 103 events	100

UBA for attack detection

- Create baseline of normal behavior for all users and hosts
  - Logon time
  - Thresholds for logon failure
  - Usual host access
  - Remote access
  - Resource access volume
  - Processes running on host
- UBA then measures real-time events against baseline, checking for anomalies

Questions to your vendor

Questions to your vendor

- Support for agent-based and agentless log collection
- Faster processing rate of logs from heterogeneous log sources
- Are you looking at log data on a daily basis?
- Can you perform fast, targeted searches for specific data?
- Can you set alerts on anything in the logs?
- Are the logs stored securely?
  - For Forensic analysis and internal audit
  - Is it tamper proof? (Encrypted, hashed, and time-stamped)

Resources that might be useful for you

- ADManager Plus
  - List of workstations, user accounts, groups, etc.
- Service Account Management Tool
  - List of service accounts on all windows servers and workstations

Note: Visit manageengine.com (*Active Directory section*) to download the tools.

ManageEngine

Log360

www.manageengine.com/log-management

Summary

- Tracking key security events: Insider and External attacks.
- What attackers want to be successful?
- Ingredients of good SIEM deployment
- Understanding User Behavior Analytics (UBA)
  - *Leveraging machine learning and AI.*

ManageEngine

Thank you!

abishek@manageengine.com