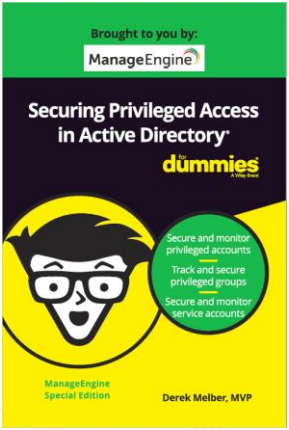
ManageEngine
ADSolutions

Leveraging SIEM Advanced Technologies

hary@manageengine.com

Resources

- hary@manageengine.com
- derek@manageengine.com
- Online Resources
  - ManageEngine Active Directory Blog
  - Security Hardening Site
  - Download free Dummies book
- 2018 World Tour
  - Amsterdam, London
  - Johannesburg, Cape Town, Milan, Rome
  - Madrid, Tel Aviv, Istanbul, Ankara
  - ...



Agenda

- The limitations that Microsoft Event Viewer possesses
- Powerful use cases that can help you manage security and access better
- Customization concepts that will allow you to tailor your SIEM solution for your environment
- How to leverage correlation to detect anomalies and attacks better

The limitations that Microsoft Event Viewer possesses

Microsoft Event Viewer Limitations

- Audited events are stored in Event Viewer – Security Log
- Tracked changes are stored in Security Log on DC where event occurred
- Each DC has a unique Security Log
- Log size is limited
- Log can be retained, but access is time consuming
- Consolidation of logs is possible, but must be setup and is slow to converge
- Alerting is possible, but not granular
- No correlation possibilities

Powerful use cases that can help you manage security and access better

Powerful Use Cases

- Windows
  - Changes to “Admin” groups
  - Changes to service accounts
  - Changes to Active Directory permissions
  - Changes to Group Policy
  - Failed logons/account locked by a specific group (Admins, C-level, etc)
- Files
  - Changes to file extensions
  - File deletions
  - Changes to file/folder ACLs
- Firewall
  - Changes to firewall rules
  - Deletion of firewall rules

Customization concepts that will allow you to tailor your SIEM solution for your environment

Why Customize?

- No off the shelf tool knows about your exact environment
- User, computer, and group names differ for each environment
- Every organization has distinct needs and requirements
- Not every organization has the same devices and operating systems

Customizing Core concepts

- Each device and operating system has a unique set of events and event IDs
- Knowing what each device is responsible for can help narrow key events for each device
- Understand authentication, communication, access, routing, etc.
- Leverage past experience to develop what to monitor
- Leverage requests for information to develop what and how to monitor

Customization Use Cases

- Privileged users
  - Users typically gain privileges through membership in Active Directory groups
  - (Note: User Rights also grant privileges, but per computer and don't change often)
  - Typically privileged groups don't change membership often
  - Monitoring the membership of these groups gives insight into immediate privileges
  - Organize privileged groups for better reporting and alerting
    - AD privileges (administration, delegated users, etc.)
    - GDPR (admin of AD and resources, access to resources)
    - PCI (admin of AD and resources, access to resources)
    - HIPAA, SOX, ITIL, etc.
    - Financials
    - Human Resources

Customization Use Cases

- Ransomware attacks
  - Specify resources to be monitored
  - Associate file types to attacks
  - Set thresholds to eliminate false positives
  - Setup alerts
    - Who will be alerted
    - If there will be any post alert actions

How to leverage correlation to detect anomalies and attacks better

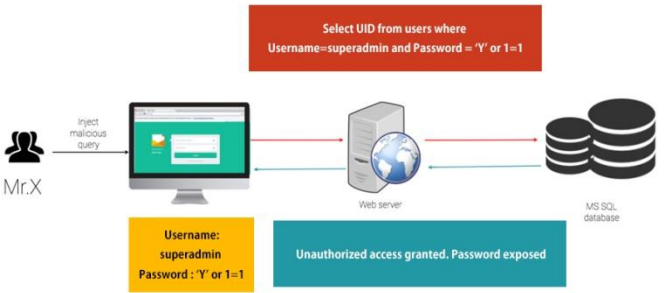
What is SIEM Correlation?

Event correlation is a technique for making sense of a large number of events and pinpointing the few events that are really important in that mass of information. This is accomplished by looking for and analyzing relationships between events.

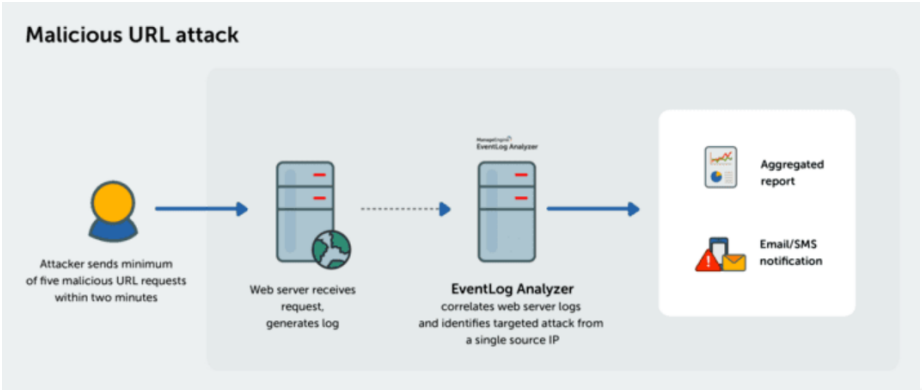
Key Correlation Concepts to Consider

- Collect data from **disparate devices** on network
- **Predefined Rules** for efficient configurations
- **Overview dashboard** for quick view of network activity
- **Rule builder** that is intuitive, yet powerful
- **Filters** for forensic and analysis of attacks
- **Real-time alerting**
- **Scheduling** of reports

Containing SQL injection attacks

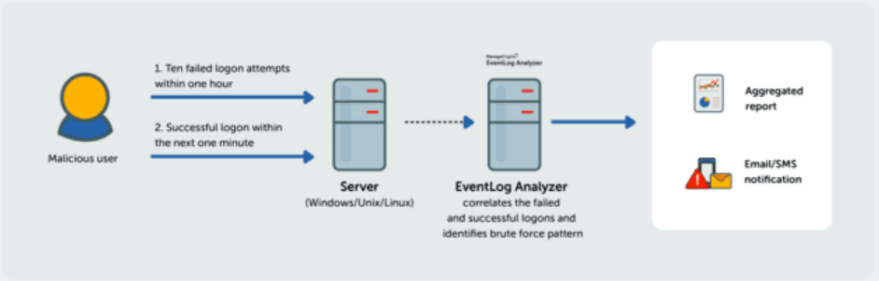


Correlation Examples

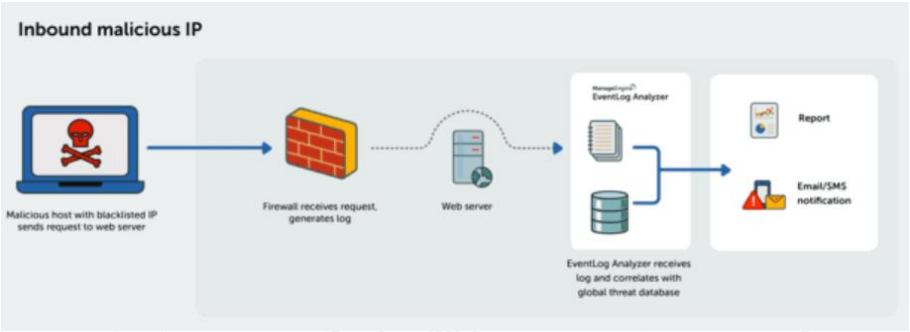


Correlation Examples

Brute force attack



Correlation Examples



Correlation Examples

- Failed logon – successful logon – install services
- Failed logon – successful logon – disabled service(s)
- Failed logon – successful logon – installed software
- Locked user accounts across domain

Summary

- The limitations that Microsoft Event Viewer possesses
- Powerful use cases that can help you manage security and access better
- Customization concepts that will allow you to tailor your SIEM solution for your environment
- How to leverage correlation to detect anomalies and attacks better

ManageEngine

Thank you!

hary@manageengine.com