Quick and Easy Forensic Timelines via Sysmon, WEF, and ELK

Presented by
Aaron Jewitt
@acjewitt

whoami

- "Threat" Hunter
- Working for Booz Allen Hamilton
  - But soon I start a new job with Elastic
- Former NSA ROC operator
- Father of 3 boys
- American living in Frankfurt
- Collector of SANS certifications
- All opinions in this talk are my own

what this talk is about

- Using Kibana or Splunk dashboards to make it faster and easier to Respond to alerts and investigate hosts, users, and processes in your network

- What the talk is **not** about (but it could be if I had more time)
  - Anomaly detection and alerting using this data
  - Threat Hunting with this data
  - Step-by-step walkthrough of setting up the event data pipeline

  - Absolutely zero Blockchain or AI in this talk.

scenario

- Brian Krebs just called your CISO on a Saturday and gave her two computer and user names he saw in a compromise. She wants forensic timeline of events from those systems and all user activity ASAP. One is in Singapore, the other is in New York, and you are in Frankfurt.
- How long does it take to collect and analyze the data?
- How many people are capable of completing this task?

problem

- During an attack you have to be able to move as fast as the attacker
- Getting data for forensics investigations can take a long time
  - Get the data, parse the data, analyze the data…
  - Evidence will be spread through multiple locations
  - Time zones are a pain
  - Permissions on the remote systems may stop you
- You need to have DFIR specialists on the team to collect information
  - Or you need hire Incident Response consultants $$$ €€€ £££

problem++

- Traditional SIEMs only contain alerts
  - Alerts tell you that something happened, but not the whole story
- Attackers will delete host logs to hide their tracks
- Attackers will compromise user accounts to spread and persist
- Evading antivirus is super easy to do – then there aren’t any alerts
  - When the AV does find something the alerts don't tell you much

Solution – What?

- Create Kibana or Splunk dashboards to make forensic timelines easy
  - Timeline of all activity on a host
  - Timeline of all activity of a User
  - Timeline of all activity of a process
- Elastic & Splunk are good for Forensic Science, not just Data Science
  - **(Don’t let the Data Scientists take all the cool toys!)**

solution – How?

1. Enable verbose logging on hosts
   - Deploy Sysmon to all windows hosts in your enterprise
   - Deploy Elastic's Auditbeat System Module to all *nix/MacOS systems
2. Centralized collection of Logs and Windows Events
3. Create dashboards and alerts in Kibana or Splunk

STEP 1:
Getting the right logs

Sysmon overview

- If you have a windows domain you need Sysmon!
- Sysmon is a **free** utility from Microsoft that turns on lots of great logging
- Config file allows very granular control of what gets logged and what doesn't

- https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon
- https://www.rsaconference.com/writable/presentations/file_upload/hta-t09-how-to-go-from-responding-to-hunting-with-sysinternals-sysmon.pdf

sysmon logging

- Process start and stop
- File Timestamp changes
- File Creation
- Network connections
- Registry changes
- File Downloads
- Named Pipes
- Driver Loading
- WMI Subscriptions
- Modules & dlls loaded in memory
- Process Memory Access

sysmon config tips

- Start with Taylor Swift's config and work from there
  - https://github.com/SwiftOnSecurity/sysmon-config
- Start with a small test group while building your config!!!
- Every Domain is unique, take the time to tune the config
- Constant testing and changing – it never ends
  - New software deployments will break your config

sysmon config tips

- Exclude known good, include everything else
- You must whitelist events or you will flood the system
- Whitelist with caution – be as specific as possible
  - If you whitelist an event you will have no evidence of it
  - If you whitelist a folder the attacker can operate from there
- Whitelist the full command line of a process, not the process name

sysmon management tips

- Keep multiple read only configs on the NETLOGON share
- At a minimum you should have 3 production and 3 test group configs
  - Workstations
  - Domain controllers
  - Servers
- Use Group Policy and PowerShell to deploy and regularly update
- Test before deploying to production!
  - And don’t make changes on a Friday…

Elastic auditbeat system module

- It’s like sysmon for Linux and Mac (also works on Windows)
- Experimental module released by Elastic on Jan 29th
  - host information – Unique host GUID, uptime, changes to IP, hostname, etc.
  - process info – command line, hash, path, user
  - socket creation – src, dst, calling process, user
  - user logons – UID, GUID, Shell, CWD
- Because linux logging is a mess.
- https://www.elastic.co/blog/introducing-auditbeat-system-module

Additional data for forensics

- Enable auditing of changes to active directory objects on your DC
- Autoruns – collect daily
  - https://github.com/palantir/windows-event-forwarding/tree/master/AutorunsToWinEventLog
- Other Windows Event logs

STEP 2
Collecting the logs

agent based or agentless forwarding

- Either use an agent to forward logs
  - Logstash, Splunk forwarder, ArcSight Connector, etc
- Or use the built in capabilities of the operating system
  - Windows Event Forwarding (WEF), syslog, etc

windows event forwarding

- Any Windows server can be a Windows Event Collector (WEC) server
- The WEC server has a subscription file that tells the workstations what to send
- Use GPO to tell workstations who their WEF collector is
- Workstations must have winrm configured

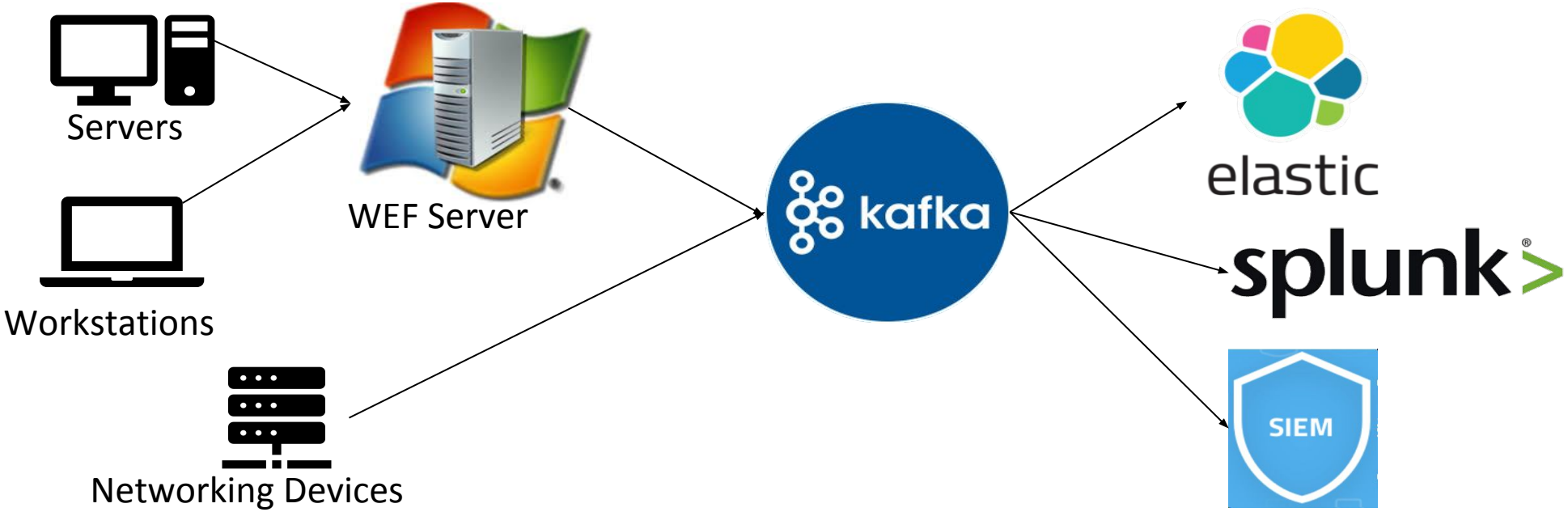
- @jepayneMSFT has some great blogs and videos about WEF for Hunting
- https://docs.microsoft.com/en-us/windows/security/threat-protection/use-windows-event-forwarding-to-assist-in-intrusion-detection

WEF subscription

- Recommended events to collect in your WEF subscription
  - All sysmon events – you've already filtered them
  - Logon events – success (4624), failure (4625), special login (4672)
  - Services – change (7040), new services (7045)
  - USB events - Microsoft-Windows-Kernel-PnP (410 and 420)
  - Kerberos events from the DC – TGT requested (4768), TGT failed (4771)
  - AD Object changes from the DC – See Microsoft recommendations

send it from the WEF to your analytic system

- Use Beats, Splunk forwarder, or other agent to push the events from the WEF to the analytic system
- Kafka is useful for collecting the data and sending it to multiple SIEMs



Step 3: Build things with the logs

alerts – not the point of the talk but still important

- Sigma - By Florian Roth @cyb3rops
  - https://github.com/Neo23x0/sigma
  - Open source project for generic SIEM rules
  - Comes with a script to format all of the rules for your SIEM
  - Many of the rules require Sysmon
- ElastAlert – https://github.com/Yelp/elastalert
  - Framework for custom alerting in Elastic
- HELK has scripts that download newest Sigma rules to create Alerts

Dashboards

- Make the data easy to use and understand
- Don’t make your security people become data scientists
- Focus on making repeatable tasks easy
- Don’t just focus on alerts, tell a story

Host Investigation Dashboard

- Answer the Who, What, When, Why, & How for a single host
- Enter a Hostname or IP address and select a timeframe
- Split the dashboard into easy to understand panels
  - Each panel should answer a question
- Whitelist known noise out of the panels
  - Nessus scans, SCCM, Regular Scheduled Tasks

Host Investigation Panels – User events

- All active users
  - Display all Distinct values of the User field in Sysmon
  - Timechart with count of events by user
- Successful and failed local authentication
  - Security event_id 4624,4625
- Successful and failed authentication at the DC
  - Authentication events from the DCs containing the hostname
  - Kerberos and NTLM

Host Investigation Panels – Special logins

- Elevated Privileges assigned to a login – event_id 4672
  - Pay close attention to SeDebugPrivilege
- Commands Executed by the SYSTEM user
  - event_id:1 user_account:SYSTEM
  - SYSTEM shouldn’t run whoami.exe, or ping.exe, or ipconfig.exe, etc…
- Network Connections by SYSTEM privilege processes
  - event_id:3 user_account:SYSTEM

Host Investigation Panels– Downloaded files

- Sysmon event_id 15 – creation of Alternate Data Streams (ADS)
- Files downloaded from the internet are given an ADS for tracking
- Each event contains the filename, User and Process that downloaded the file
  - event_id:15

Host Investigation Panels– Process execution

- Processes executed by cmd, powershell, wscript, or cscript
  - Good for quickly finding strange activity or administrative actions
  - event_id:1 AND (process_parent_name:*\\cmd.exe OR process_parent_name:*\\powershell* OR process_parent_name:*\\wscript.exe OR process_parent_name:*\\cscript.exe)
- All Distinct Process Command Line, grouped by User
  - This panel will quickly show you suspicious processes without duplicates

Host Investigation Panels– Network Connections

- Strange Network Connections – exclude Chrome, Outlook, etc.
  - This panel must be customized for each domain, whitelist known scripts
  - event_id:3 AND process_path!:*\\chrome.exe AND process_path!:*\\outlook.exe AND etc.
- Network Connections sorted by time - event_id:3
  - This panel will be very noisy, but is good for deep analysis
- Additional Panels with IP information from Proxy, Firewall, Bro, etc.

Host Investigation Panels– Changes to the host

- Registry modifications – Sysmon has 3 events for Registry changes
  - event_id:12 OR event_id:13 OR event_id:14
- Any new files created – Sysmon Event has User and Process that created file
  - event_id:11
- New Services installed or changed
  - event_id:7040 OR event_id:7045
- Drivers Loaded – Pay attention to the Signature and Signed values
  - event_id:6

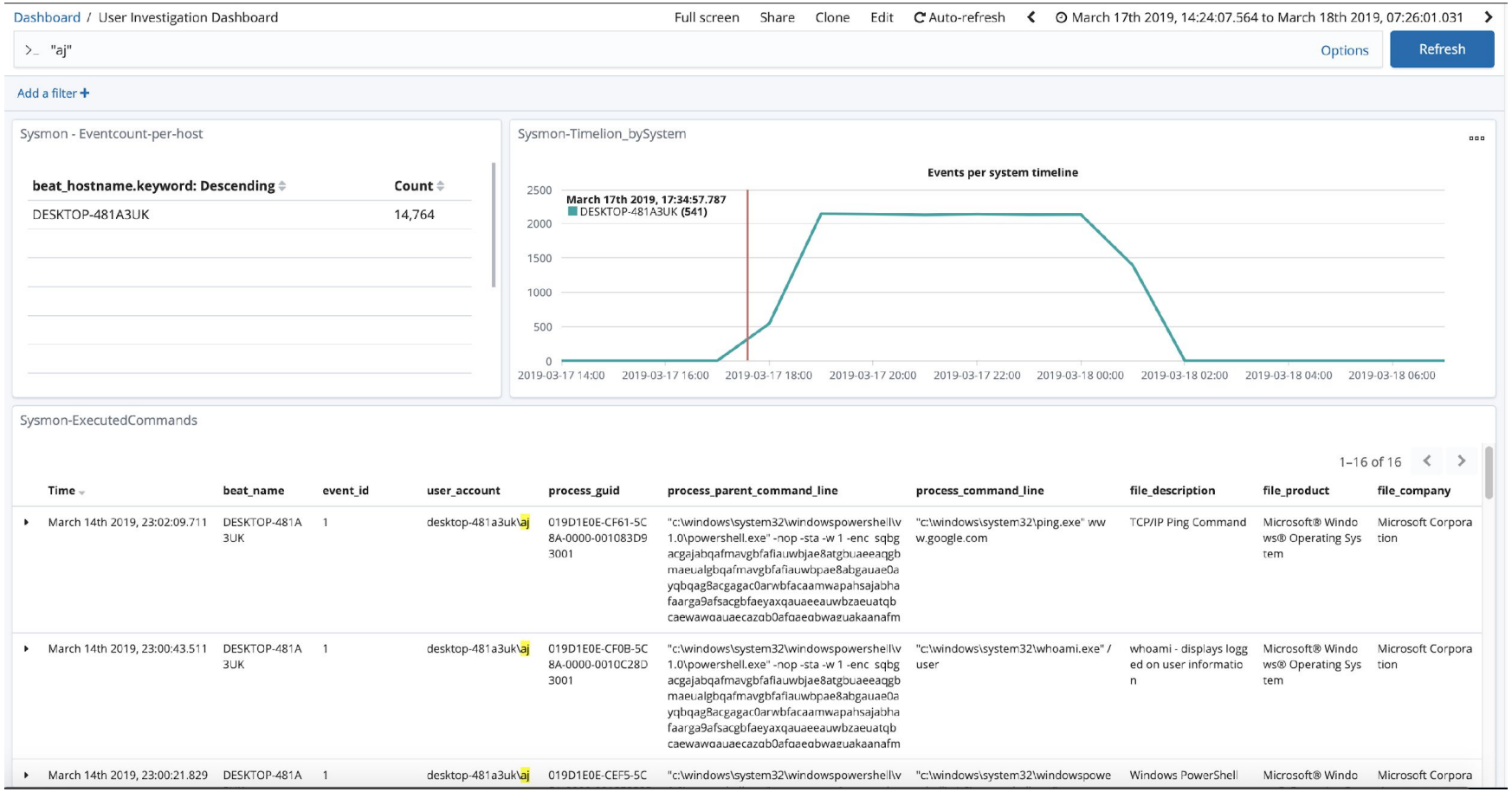
Host Investigation Panels – Changes to the host

- USB device changes – insertion and removal
  - event_id:410 OR event_id:420
- WMI Subscription changes – Used for ‘file-less’ persistence
  - event_id:19 OR event_id:20 OR event_id:21

User Investigation Dashboard

- Display all activity by a compromised user account
- Attackers will compromise an account to move laterally and spread
- Very Similar to the Host Investigation Panel
- If you have AD User information you can enrich the dashboard
  - Get-ADUser

User Investigation Dashboard



User Investigation Dashboard

- List of all Computers the user executed processes on
- Timeline of activity on each system
  - Using sysmon events instead of authentication events shows you how active the user was on each system

- Successful and failed login attempts
  - (event_id:4624 OR event_id:4625 OR event_id:4648)

User Investigation Dashboard

- All Processes and commands executed, on every computer
- All Network Connections, on every computer
- All Files Downloaded, on every computer
- All Files Created, on every computer
- All registry modifications, on every computer

- Totally not creepy...

Process Investigation Dashboard

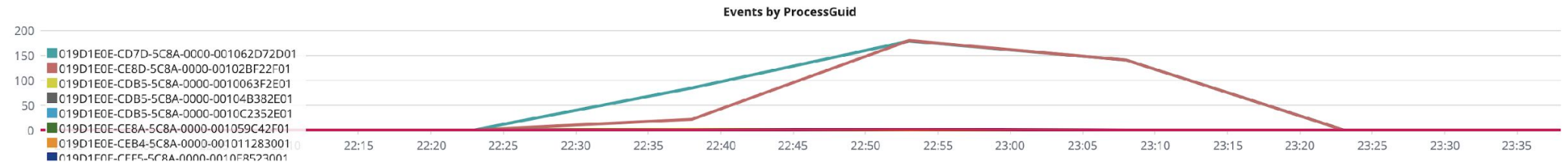
- In Sysmon every process execution has a Unique ProcessGuid
- Process Execution events have the ProcessGuid and ParentProcessGuid
- Searching for a ProcessGuid will return every event about that process
  - Network Connections, Files Created, Registry Changes, Child Processes, etc.
- Make a dashboard to sort and display all activity by a process
- Add multiple Guids with OR statements to get a better view of events

Dashboard / Sysmon-ProcessInvestigation Full screen Share Clone Edit Auto-refresh March 14th 2019, 21:53:56.935 to March 14th 2019, 23:45:00.000

>_ "019D1E0E-CE8D-5C8A-0000-00102BF22F01" OR "019D1E0E-CD7D-5C8A-0000-001062D72D01" Options Refresh

Add a filter +

Sysmon-Timelion-ProcessEvents_byProcessGuid



Sysmon-Process Creation - EventId1

1–10 of 10

Time	beat_name	user_account	process_parent_guid	process_guid	process_parent_command_line	process_command_line	file_description	file_product	file_company
March 14th 2019, 22:54:05.808	DESKTOP-481A3UK	desktop-481a3uk\aj	019D1E0E-CD79-5C8A-0000-0010DEFC2C01	019D1E0E-CD7D-5C8A-0000-001062D72D01	"c:\windows\system32\windowspowershell\v1.0\powershell.exe"	"c:\windows\system32\windowspowershell\v1.0\powershell.exe" -nop -sta -w 1 -enc sqbgacgajabqafmavgblafiauwbjae8atgbuageaygbsaeualgbqafmavgblafiauwbjag8abgauae0aqqbqae8augagac0arwbfacaamwapahsajabhafaarga9afsaug	Windows PowerShell	Microsoft® Windows® Operating System	Microsoft Corporation
March 14th 2019, 22:55:01.394	DESKTOP-481A3UK	desktop-481a3uk\aj	019D1E0E-CD7D-5C8A-0000-001062D72D01	019D1E0E-CDB5-5C8A-0000-0010C2352E01	"c:\windows\system32\windowspowershell\v1.0\powershell.exe" -nop -sta -w 1 -enc sqbgacgajabqafmavgblafiauwbjae8atgbuageaygbsaeualgbqafmavgblafiauwbjag8abgauae0aqqbqae8augagac0arwbfacaamwapahsajabhafaarga9afsaugbfaevaxqauaeeacwbtaeuatqbiaewawqa	"c:\windows\system32\whoami.exe" /groups	whoami - displays logged on user information	Microsoft® Windows® Operating System	Microsoft Corporation
March 14th 2019, 22:55:01.479	DESKTOP-481A3UK	desktop-481a3uk\aj	019D1E0E-CD7D-5C8A-0000-001062D72D01	019D1E0E-CDB5-5C8A-0000-00104B382E01	"c:\windows\system32\windowspowershell\v1.0\powershell.exe" -nop -sta -w 1 -enc sqbgacgajabqafmavgblafiauwbjae8atgbuageaygbsaeualgbqafmavgblafiauwbjag8abgauae0aqqbqae8augagac0arwbfacaamwapahsajabhafaarga9afsaugbfaevaxqauaeeacwbtaeuatqbiaewawqa	"c:\windows\system32\whoami.exe" /groups	whoami - displays logged on user information	Microsoft® Windows® Operating System	Microsoft Corporation

Conclusion

- Any org can build these dashboards and alerts for very little $$$
- These Dashboards aren’t just for the security team
  - DevOps, Active Directory, Help Desk, and other admins love them!
- With these Dashboards your Security team can find the problem quickly instead of spending hours or days collecting all of the data

Questions?

- Slides and Kibana Dashboards are on Github
- https://github.com/aarju/Kibana_ForensicDashboards

- These Dashboards were developed to work with Hunting ELK (HELK)
  - You may need to adjust the field names in your ELK stack
  - https://github.com/Cyb3rWard0g/HELK