Make Your Sandbox Useful

Accelerate Your End-to-End Response Capabilities

Zach Sivertson

Sr. Director, Product Management – Symantec

October 2018

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

Make Your Sandbox Useful

The Problem

splunk> .conf18

The Problem

Sandboxing Systems are Slow

- Most Sandbox Systems are Slow
- Average Sandbox Response Time
  - Over 6 minutes (7 vendors tested)
  - Test done with system not under load
  - New/unknown malware
  - Sandbox vendors will tell you they are much faster
    - Only for known malware IoC (URLs, file hashes, signatures etc.)

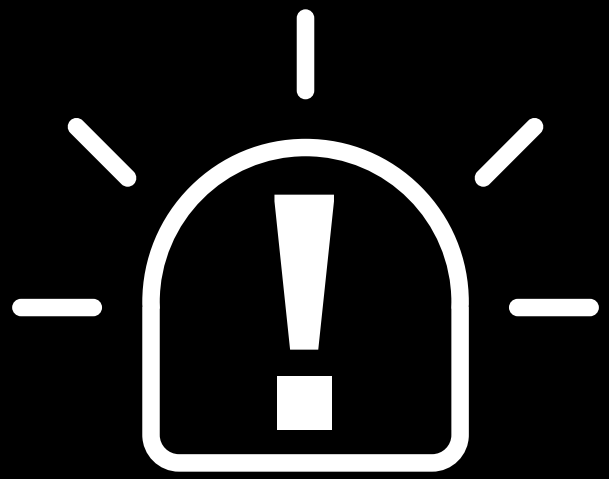
Average Sandbox Response Time (Unkn. Malware):

> 6 min

The Problem

Most Sandbox Systems are Not Real-Time

- Most sandbox systems don’t block unknown malware in real-time
  - Many vendors will claim real-time blocking by:
    - Claiming victory by blocking known samples
    - Making end user wait or trickling file (w/ Proxy) to end user
  - Many are deployed off TAP port where only option is TCP reset
- Patient Zero (First client getting infected)
  - Creates a security response need
    - Clean up- initial infection
    - Prevent lateral spread



The Problem

Too Many Alerts; SoC Teams are Overwhelmed

- Sandbox systems can create lots of alerts that aren't prioritized or automated
  - Many vendors want systems deployed in-front Proxy or Firewall to "see everything"
- Don't know right away if you need to take action
  - Did the file reach the endpoint?
  - How do I prioritize thousands or alerts?

"Two-thirds of the time spent by security staff responding to malware alerts is wasted because of faulty intelligence."

The Cost of Malware Containment
- Ponemon Institute

The Problem

Too Many Alerts; SoC Teams are Overwhelmed

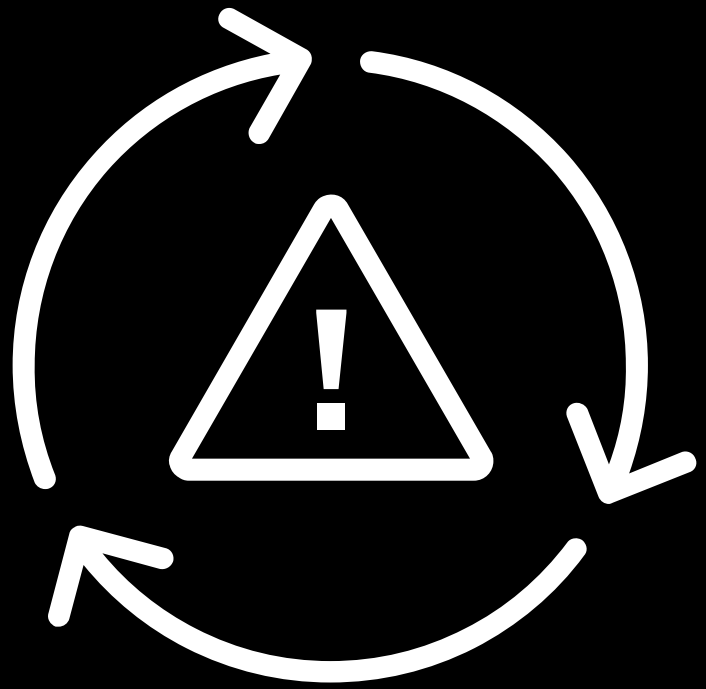
Overwhelming Incident Response (IR) Queue

- Systems create alarms for all types of malware, even common
- IR teams can't reach majority of alarms
- Doesn't "**prevent**" enough – "**detect & respond**" is much more expensive process

The Problem

Sandbox Responses are Not Automated

- SoC Teams get thousands of sandbox alerts that require manual verification:
  - Did this file get blocked by some downstream security device?
  - How risky is this incident?
  - Is it more important than other items in my queue?
  - Should I act now?
  - How should I remediate this issue?



splunk> .conf18

The Problem

This is where the subtitle goes

1. Most Sandboxing Systems are Slow
2. Most Sandboxing Systems are not Real-Time
3. Patient Zero Occurs
4. Too Many Alerts
5. Response in Not Automated

Make Your Sandbox Useful

Tips & Recommendations

splunk> .conf18

- Deploy Sand
  - Allows
    - Trickl
    - Displ
  - E.g. Re
- Find Sc
  - Use bo
  - Some e

Viru

Det
Con
Det
App

For

Task 52927

Task Summary | Dynamic Event List | Static Event List | Event Timeline

Emulation Detonation

Task Details

Risk Level:	10
Analyzed:	2018-09-04 13:53:59
Processing Time:	.97s
Task Status:	Task Complete
Environment:	SandBox
Execution Arguments:	
"c:\windows\temp\sample.exe"	
Properties:	Drop FS Events: Drop Reg Events: Keep FS Events: 1 Keep Reg Events: 1 Keep Raw API: 1 Keep All SandBox Events: 1 Keep Text API: 1 Capture All: 1 Get dropped files: 1 SandBox PE Dump: 1

Recreate Task

Pattern Matching Results

10	File reputation: Malware (10)
6	Dumps and runs batch script
5	Resource section contains an executable
4	Checks whether debugger is present
4	Imports library functions that can be associated with process injection
2	64 bit executable
2	PE: Nonstandard section

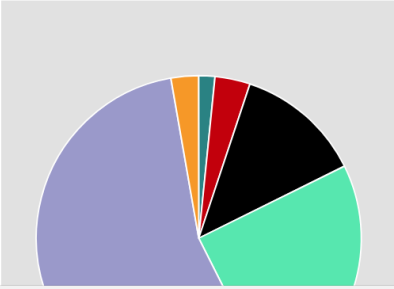
Sample Details

ID:	29381
Source:	www
File Exists:	Yes
Download:	Download Resource
Received:	2018-09-03 03:03:37
Label: edit	poc.exe
MD5:	324a004ae53046087b246b55a03b0...
SHA256:	75cb514f9c6e3c503759f5478cd2ce8...
Filetype:	PE32:win32:gui
Filesize:	237500 bytes
Sample Comments:	edit
VirusTotal:	No result found at VirusTotal

Other Resources

29182-324a004ae53046087b246...	system...
52927-0-00RUNME.BAT.dmp	txt:pow...
52927-3-PROCES~1.PS1.dmp	txt:pow...
52927-1-ALPC-T~1.DLL.dmp	PE32:...
52927-2-INJECT~1.EXE.dmp	PE32:...

Event Distribution Chart



Activity Report

Download PDF Report | View STIX Report

Static Events (4 events)

Anomaly:	PE: Contains one or more non-standard sections
Anomaly:	PE: Resource section contains an executable
File Reputation:	[dropped] c:\WINDOWS\TEMP\ALPC-T~1.DLL [Malware]
File Reputation:	[dropped] c:\WINDOWS\TEMP\INJECT~1.EXE [Malware]

Process/Thread Events (1 events)

File System Events (12 events)

Creates:	__tmp_rar_sfx_access_check_55378704
Creates:	00runme.bat
Creates:	ALPC-TaskSched-LPE.dll
Creates:	InjectDll.exe
Creates:	process-tree.ps1
Opens:	c:\windows\temp\sample.exe
Writes to:	00runme.bat
Writes to:	ALPC-TaskSched-LPE.dll
Writes to:	InjectDll.exe
Writes to:	process-tree.ps1
Reads from:	c:\windows\temp\sample.exe
:es:	C:\WINDOWS\TEMP__tmp_rar_sfx_access_check_55378704

https://research02.osl.bluecoat.com/ma/analysis_center/view_task/52927

- Filter

Web
URL C
& Ris
63
Web re

Activ
Redu
Incre
SMG
adva

- your

Task 53013

Task Summary | Dynamic Event List | Static Event List | Event Timeline

Task Details

Risk Level:	10
Analyzed:	2018-09-05 01:51:33
Profile:	Windows 7 64-bit Office 2013
Processing Time:	62.1s
Task Status:	Task Complete
Environment:	IntelliVM
Execution Arguments:	"c:\windows\tem...B54835653721B0C.exe
Properties:	ANALYTICS.NSE.DUMP_YARA_STRINGS: 1 Create HTTP Archive: 1 Plugin: ghost_user.py Task Logging: 1 IS.enable: 1 IS.event.quit.mem: 1 IS.event.quit.nse_scan: 1 IS.event.quit.strings: 1 IS.event.terminate_process.mem: 1 IS.event.terminate_process.nse_scan: 1 IS.event.terminate_process.strings: 1 IVM.enable_ddna: 1 Get dropped files: 1 Timeout: 60

Recreate Task

Recreate Task with Detailed Capture

Pattern Matching Results

10	File reputation: Malware (10)
7	Generates suspicious network traffic
6	Modifies registry autorun entries
5	Adds autostart object
5	Packer: UPX
4	Checks whether debugger is present
4	Connects to local IP
4	Contains compressed or encrypted data or code
4	Imports library functions that can be associated with process injection
3	Long sleep detected
3	Sleeps skipped
2	PE: Nonstandard section
1	HTTP connection - response code 404 (file not found)

Screenshots

Activity Report

Static Events (7 events)

Anomaly:	PE: Contains a virtual section
Anomaly:	PE: Contains one or more non-standard sections
Packer:	UPX
Web Reputation:	http://bluecrab-soft.com/info_cn.pad [Suspicious]
Web Reputation:	bluecrab-soft.com [Suspicious]
File Reputation:	[sample] c:\windows\temp\64F8B1CE87FDC2BA99E0085FF384B1546B761755139C2F601B54835653721B0C.e
File Reputation:	[create_process] C:\windows\temp\64F8B1CE87FDC2BA99E0085FF384B1546B761755139C2F601B54835653

Process/Thread Events (1 events)

Named Object Events (13 events)

File System Events (6 events)

splunk> .conf18

Tip # 3 Automate and Orchestrate

Automate Your Sandbox Response/Remediation

- Top Reasons to Automate and Orchestrate Sandbox Response with PC:

1. **Save Time:** Confirm attack (that entered through the web, email or other) actually occurred on the endpoint
2. **Prevent the Spread of an Attack:** Blacklist attack via endpoint manager
3. **Automate Remediation:** Perform automated/1-click remediation of endpoints to save on SoC/I.T. resources

User Story – Network to Endpoint IoC Verification

As a security administrator…

When I receive an alert from the sandbox I want to know **what endpoints across my entire network have seen these same IoC's.** This will shorten my indecent response time by preventing my team from performing unnecessary work to confirm if the malicious sample detonated on the endpoint.

Workflow:

1. Sandbox discovers a malicious sample & sends data to Phantom
2. Phantom queries endpoint to verify IoC across entire endpoint deployment (File Hash, Registry changes, URL, process name, registry changes etc.)
3. The list of infected endpoints are then added to the sandbox report showing the admin not only what happened in the sandbox but what endpoints are infected

Makes alerts more relevant

More easily prioritize alerts

Know what endpoints are affected

User Story – Endpoint Automated Blacklist

As a security administrator…

I want attacks that are discovered via the sandbox to be stopped from spreading to other endpoint devices.

Workflow:

1. Sandbox discovers a malicious sample with high certainty and send data to Phantom
2. Phantom reaches out to endpoint and blacklists that hash on all endpoints
3. This prevents the spread of this file to other endpoint devices

Automates basic security response

Saves time and resources

Increase security posture by decreasing lateral spread

splunk> .conf18

User Story – Endpoint Remediation

As a security administrator…

If a malicious sample (originally detected in the sandbox) has been detonated on an endpoint I want some level of automated remediation to take place until possible further action can be taken

Workflow:

1. Sandbox discovers a malicious sample and sends data to Phantom
2. Phantom queried endpoint to verify IoC on endpoints (File Hash, Registry changes, URL, process name, registry changes etc.)
3. The list of infected endpoints are then added to the sandbox report showing the admin not only what happened in the sandbox, but what endpoints are infected
4. **Malicious samples are deleted, processes stopped, call back traffic blocked, registry keys changed in order to help mitigate the damage until the device can be re-imaged**
5. Automate contacting of employee to notify them that their machine needs to be re-imaged and to stop by the I.T. Help Desk (Email, Slack, SMS etc.)

Automates more advanced response

Saves time and resources

Increase security posture by limiting exposure to patient zero

Tip #3 Demo

Tip # 3 Automate and Orchestrate

QuickTime Player File Edit View Window Help 37% Fri Sep 28 6:33:06 PM

Phantom | Analyst Queue | Phantom Playbook Editor | Phantom Playbook Editor | Phantom Playbook Editor | Content Analysis System

Not Secure | https://ec2-54-245-145-163.us-west-2.compute.amazonaws.com/browse/?

splunk>phantom

Non-production use license. version 4.0.1068 admin

Sources

Events Indicators Cases

Search event names

Show Select a filter + EVENT IMPORT

Top Events			Severity			Status			Top Owners
139	12	6	0	142	15	29	3	125	5
splunk nota...	suspicious b...	events	Low	Medium	High	New	Open	Resolved	admin

Dynamic Updates Show Stats

ID	NAME	LABEL	STATUS	SEVERITY	SENSITIVITY	ARTIFACTS	CREATED	OPENED	UPDATED
157	ESCU Account Monitoring and Controls	splunk notable event	New	MEDIUM	TLP: AMBER	1	0 minutes ago		0 minutes ago
156	Email Spear Phishing Campaign	splunk notable event	New	MEDIUM	TLP: AMBER	1	0 minutes ago		0 minutes ago
155	ESCU Suspicious Process	splunk notable event	New	MEDIUM	TLP: AMBER	1	0 minutes ago		0 minutes ago
154	ESCU Account Monitoring and Controls	splunk notable event	Resolved	MEDIUM	TLP: AMBER	1	0 minutes ago		0 minutes ago
153	ESCU Account Monitoring and Controls	splunk notable event	Resolved	MEDIUM	TLP: AMBER	1	0 minutes ago		0 minutes ago
152	Unroutable Activity Detected	splunk notable event	Resolved	MEDIUM	TLP: AMBER	1	0 minutes ago		0 minutes ago
151	ESCU Suspicious Process	splunk notable event	Resolved	MEDIUM	TLP: AMBER	1	0 minutes ago		0 minutes ago
150	Brute Force Behavior From PROD-MFS-003	splunk notable event	Resolved	MEDIUM	TLP: AMBER	1	0 minutes ago		0 minutes ago
149	Email Spear Phishing Campaign	splunk notable event	Resolved	MEDIUM	TLP: AMBER	1	0 minutes ago		0 minutes ago

Key Takeaways

This is where the subtitle goes

1. **Deploy Sandbox Behind Proxy**
   - Enable real-time sandboxing
   - Better user experience w/ trickling

2. **Pre-filter Sandbox**
   - Reduce alert noise
   - Save on deployment cost

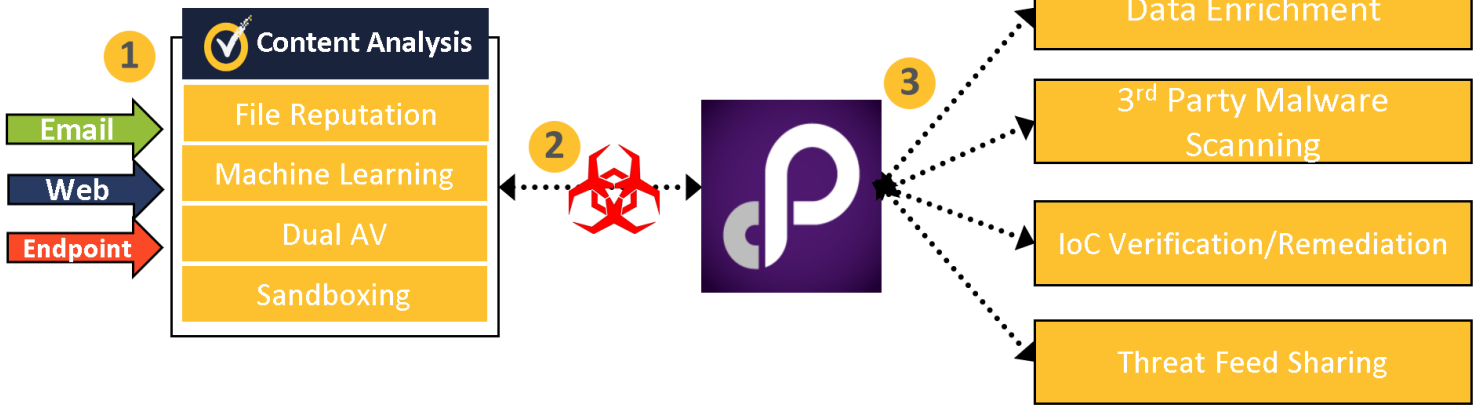
3. **Use Sandbox with Emulation & Full VM**
   - Decrease time to verdict
   - Faster verdicts for real-time blocking

4. **Use Sandbox w/ Custom Image Capabilities**
   - Understand if malware would detonate on your gold image

5. **Automate and Orchestrate Sandbox Response**
   - Save Time: Confirm attack actually occurred on the endpoint
   - Prevent the Spread of an Attack: Blacklist attack via SEP Manager (SEPM)
   - Automate Remediation: Perform automated/1-click remediation of endpoints to save on SoC/I.T. resources

Symantec Phantom Integration

Data Flow – PC Integration



Symantec

virustotal — VirusTotal

OPSWAT Metadefender — Metadefender

FireEye — FireEye

cuckoo — Cuckoo

Carbon Black. — Carbon Black Response

Symantec — Symantec Endpoint Protection

CROWDSTRIKE — Streaming API

Hewlett Packard Enterprise — ArcSight ESM

200 + Integrations

1. Malicious file is discovered via CA
2. Malicious file/meta is sent to Orchestration Vendor
3. Orchestration Vendor executes on the Symantec Playbook
4. If needed, threat intel shared with Symantec for blacklisting purposes

Thank You

Don't forget to rate this session in the .conf18 mobile app

.conf18

splunk>