Hey there!

Top SIEM Use Cases

Ryan Voloch and Peter Giannoutsos

9/23/2016

Why don't you have a seat?

What was your plan here today?

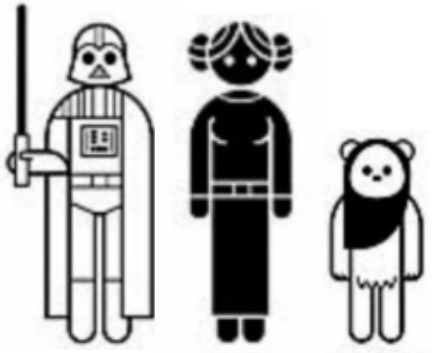
- About Us / Intro
- Methodology and Criteria
- Review Top 10 SIEM Use Cases
- Recommendations

THEME HINT:

Chris Hansen = BLUE TEAM

Pervert = PENETRATION TESTER

Ryan Voloch



- Christian
- Husband
- Father
- Information Security Manager
  - Graduate of Rochester Institute of Technology
  - 13 years InfoSec experience, 9 years with 2 different SIEMs
  - Implemented over 12 different enterprise security systems from the ground up
  - Developed 2 security operations programs
- Spoke last year on "Simplified SIEM Use Case Management"

ROCHESTER INSTITUTE OF TECHNOLOGY
R·I·T
1829

CISSP
GCIH

Download http://voloch.com/usecases.zip

Peter Giannoutsos

- About me:
  - Greek Orthodox Christian
  - Golfer, Husband, Father
  - Bourbon enthusiast/consumer

- Information Security Career
  - 15+ years in InfoSec
  - Built 2 Security Programs / 3rd in process
  - Blue team mostly
  - Devoted to learning red team skills
  - Got InfoSec certs (CISSP, GCIH)
- Attended DerbyCon every year but one
  - First time speaker – slacker

Download http://voloch.com/usecases.zip

Tell me why you are here?

- Being **BLUE** we come to derbycon to understand **RED**.
- One of our primary goals for attending is to come home with ideas for our employers.
- Typical con talk :
  - Technology > Hack it > Defend it > Detect it
- Focusing on sharing a collection of the detection ideas ("Use Cases") in mass quantities by attending one talk.
- Hope to address the question: "What can **most** blue teams do to **most likely** catch red/attacker?"

Download http://voloch.com/usecases.zip

Why?

SIEM deployments are broken today

- Question:
  - Who has a SIEM?
  - Are you detecting the right things?

Average time-to-detection is 165 days

Not detecting the most common indicators

Download http://voloch.com/usecases.zip

What you might be thinking…

- Assumptions:
  - Prevention is first and foremost.
  - Organization has already done or in process of doing as much as possible and has a monitoring program such as SIEM or an MSSP
  - Sometimes risk due to a vulnerability must be accepted or mitigated via detection.
  - Audience knows the attacks

Download http://voloch.com/usecases.zip

Methodology

- Surveyed multiple industry professionals specializing in security and penetration testing.
- Analyzed data, research, selected and cleaned up use cases for presentation.

Download http://voloch.com/usecases.zip

The Basics

- What is a SIEM use case?
  - Documented actionable output for your SIEM or monitoring program
  - In simplistic terms…it's what you want your SIEM to do.
  - Defines who, what, where, when & why.
  - An alert, report, or dashboard.

Download http://voloch.com/usecases.zip

Use Case Criteria

- Alerts of the presence of a typical penetration tester (or external attacker)
- Typical intrusion/pentest scenario:
  - Phish > Compromise Workstation > Steal credentials > Lateral Movement within network > login > exfil data.
- Objective: Mass data breach
- Broad range of cyber kill chain

Download http://voloch.com/usecases.zip

Use Case Criteria

- Doable in 90%+ of all organizations. Assumptions:
  - Basic security technology exists (AV,IPS,Etc..)
  - Common Infrastructures (AD, unix, databases, etc…)
  - Most log feeds already exist in typical SIEM deployment
- Low effort to develop in SIEM
- Can be considered the "basics" or "must-do's" for detection
- Common themes of submissions

Download http://voloch.com/usecases.zip

Use Case: **Authentication with Corporate Credentials to Untrusted Site**
The Phish

Submitted by: Nick Antil

Data Sources	Proxy Logs
Correlated Data Source	User ID List and a List of Sites your employees should authenticated to (Whitelist)
Goal	Detect compromised accounts as a result of a phish
Description	Your employees shouldn't be authentication to random domains! If they are, they were probably phished and you should force a password reset on detection!
Pseduo Code/Logic	logsource= proxylogs IF proxylog URL OR PostBody CONTAINS ListofUserIDs && hostname NOT IN hostname whitelist THEN alert("Potential Credentials Compromise - Authentication to Untrusted Internet Site Detected")
Responsible Group (Typically)	Security or End User
Responsible Group Procedure (Typical)	Reset the password and send a user an email explaining to them how they screwed up.
References	https://www.sans.org/reading-room/whitepapers/email/phishing-detecton-remediation-34082

Use Case: **Server to Internet Communication (Beyond Baseline or Request Made)** C&C

Submitted by: Nick Antill, Ryan Voloch

Data Sources	Edge proxy, edge or local firewall logs
Correlated Data Source	Server Networks
Goal	Detects both C&C and Exfil.
Description	Your servers should never talk to the Internet... and when they do, there should be a documented exception in place. An attacker who has compromised an internal host on the organizations network can establish a permanent remote access channel to exfil data. . Another way to do this is to use edge firewall logs to baseline server traffic. Once baseline is set, review and document the exceptions. When a new connection is established outside of the baselined authorized communications, an alert should be investigated. If firewalls block egress data, use failed/blocked traffic logs.
Pseduo Code/Logic	logsource= IF src_ip IN "server_list" && tcp_port = "80" OR "443") ("border firewall" NOT NULL || "proxy data" NOT NULL" THEN alert("Potentially Compromised System - Direct to External IP Request Detected")
Responsible Group (Typically)	Security Operations Center
Responsible Group Procedure (Typical)	Rule out false positives and validate communications were authorized.
References	http://security.stackexchange.com/questions/24310/why-block-outgoing-network-traffic-with-a-firewall http://securityskeptic.typepad.com/the-security-skeptic/firewall-best-practices-egress-traffic-filtering.html https://technet.microsoft.com/en-us/library/ee215186%28v=ws.10%29.aspx

Use Case: **User Password Spraying**

Lateral Movement 1of 6

Submitted by: Pete & Ryan

Data Sources	Windows Domain Controller Security Event Logs
Correlated Data Source	Password Spray User List
Goal	Detect external attacker performing password spraying to achieve lateral movement.
Description	Password spraying involves attempting to login with only one (very strategically chosen) password across all of the domain accounts. This allows an attacker to attempt many more authentication attempts without locking out users.
Pseduo Code/Logic	count of unique target accounts >= 10 from same source IP or host IF (windows_event_id = 4625 or windows_event_id = 529 or windows_event_id = 675) within 1 hour alert ("User Password Spraying ")
Responsible Group (Typically)	Security
Responsible Group Procedure (Typical)	Validate activity was authorized. If not, escalate to incident handling team.
References	http://www.blackhillsinfosec.com/?p=4694 http://securityweekly.com/2011/10/19/domain-user-spraying-and-brute/ http://gosplunk.com/repeated-unsuccessful-logon-attempts-in-linux/ http://gosplunk.com/failed-logins-windows/

Use Case: **Virus Detected on Server**

Installation

Submitted by: Ryan Voloch

Data Sources	Antivirus
Correlated Data Source	Server Host List or Host Naming Scheme
Goal	Detect stupidity.
Description	Yes, it may sound stupidly obvious to watch your AV output, but this use case should be easy to do and important. We all make mistakes! Attacker forgets to test their payload on virustotal. Yes, AV does not detect attackers 100% of time…but it can detect when attackers make mistakes. Additionally, AV alerts may fire off all day and the logs may suggest they blocked the attack. However, the malware detected and blocked may have only been one piece of the payload/infection. Additional events may have taken place and been successful. This AV event data can be automatically correlated with other events that in isolation may occur semi-frequently, such as new user accounts, new user logins, new applications or services, etc. When combined, they suggest a higher likelihood that something bad happened.
Pseduo Code/Logic	Virus detected from (a list, subnet or hostnaming scheme) of critical servers from your AV system
Responsible Group (Typically)	Security Operations Center
Responsible Group Procedure (Typical)	Identify the reason why the virus appeared on a server. It does not matter if it was cleaned or not, this is a very suspicious IOC. If unknown or not validated by application owner and/or server administrator, escalate to incident handling team.
References	http://gosplunk.com/?s=virus&cat=0

Use Case: **Windows Workstation to Workstation Communication**

Lateral Movement 2 of 6

Submitted by: Nick Antil / Brett Creasy from Bit-X-Bit

Data Sources	Windows firewall logs, EndPoint Security logs
Correlated Data Source	Workstation List
Goal	Detect external attacker executing offsec tools to achieve lateral movement an own more targets.
Description	In an enterprise environment there is no good reason workstation to workstation communication to occur.
Pseduo Code/Logic	IF src_IP IN ""Workstation_List"" && dst_IP IN ""Workstation_List"" THEN alert(""Potential Lateral Movement - Workstation to Workstation Communication Detected"")
Responsible Group (Typically)	Information Security Analysts
Responsible Group Procedure (Typical)	Review Source System Event Logs for Suspicious Behavior or remove host from network.
References	https://scadahacker.com/library/Documents/Best_Practices/NSA%20-%20IA%20-%20Limited%20Workstation-to-Workstation%20Communications.pdf

Use Case: **User Added to Windows Local or Domain Administrator Group**

Lateral Movement 3 of 6

Submitted by: Ryan Voloch

Data Sources	Windows Security Event Log
Correlated Data Source	None
Goal	One popular goal of an attacker is to make himself a local or domain administrator.
Description	Attacker will add a user to Administrator group to obtain or maintain access to a compromised system. Detects privilege escalation and perstistance techniques. This activity should be rare and only occur during system administrators staff changes.
Pseduo Code/Logic	eventId=(4732|4728|4756|632|636) and groupname=(Domain Admins|Administrators|Enterprise Admins|Schema Admins) from domain controller and member server security event logs
Responsible Group (Typically)	System Monitoring
Responsible Group Procedure (Typical)	Compare against user access management request system or ask System Administrators to validate the activity was authorized. If not, escalate to incident handling team.
References	https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=4732 https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=4728 http://blogs.splunk.com/2013/08/05/monitoring-local-administrators-on-remote-windows-systems/ http://gosplunk.com/?s=4732&cat=0 http://social.technet.microsoft.com/wiki/contents/articles/17049.event-id-when-a-user-is-added-or-removed-from-security-enabled-global-group-such-as-domain-admins-or-group-policy-creator-owners.aspx

Use Case: Unauthorized Service Account Successful Login to Server
Lateral Movement 4 of 6

Submitted by: Travis Abrams from Cyberpeak

Data Sources	Windows Domain Controller Security Event Logs
Correlated Data Source	Service account list & hostname baseline
Goal	Detect external attacker executing offsec tools to achieve lateral movement an own more targets.
Description	Detects possible lateral movement using compromised credentials. Alert when a service account is used to interactivate logon to a system it should not be used on.
Pseduo Code/Logic	IF NOT in Allowed Service Account-Host List (service account & hostname baseline table) && (windows_event_id="4624“ or “540” or “672”) && (logon_type ="2“ or “10”) THEN alert ("Potential lateral movement - Server to Server with unauthorized service account")
Responsible Group (Typically)	Security
Responsible Group Procedure (Typical)	Review Source System Event Logs for Suspicious Behavior
References	NA

Use Case: **Windows New Service Creation/Registration**

Lateral Movement 5 of 6

Submitted by: Bret Creasy

Data Sources	Windows Security Event Log
Correlated Data Source	Service Account Listing
Goal	Service creation is most likely a due to an installation or persistence technique.
Description	How often should new services appear on your workstation? Almost never! What about your servers? Even closer to never! If you see new services appearing on your systems and no changes were planned - it's worth investigating.
Pseduo Code/Logic	logsource=WinEventLogs IF win_event_id= "4697" THEN alert (Suspicious activity - new service installed)
Responsible Group (Typically)	Security Operations Center
Responsible Group Procedure (Typical)	Validate any new services with change control documentation. Consider user account in event. If not an authorized change, escalate and investigate for potential attacker webshell.
References	https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=4697

Use Case: **Service Accounts Performing Non-service Account Actions**

Lateral Movement 6 of 6

Submitted by: Bret Creasy from Bit-x-Bit

Data Sources	Windows events
Correlated Data Source	Server Account List & Event ID
Goal	Detect external attacker utilizing compromised service account executing actions outside of the baseline to achieve lateral movement an own.
Description	Application service accounts are often utilized for convenience and manageability of applications. However they also often include passwords that don't expire and over provisioning of access to resources that they do not need access to. By monitoring where and what the accounts access, alerts can be generated to identify compromised service accounts. Example: a service account meant to perform backups on the servers would not likely need to access a different server through UNC paths or mapped drives. Windows auditing needs enabled (event IDs).
Pseduo Code/Logic	"logsource = windows events 5140|5145 IF account_name in service_account_list && event_id NOT IN critical_server1_allowed_eventid_list THEN alert ("Potential lateral movement - Service Accounts performing non-service account actions")
Responsible Group (Typically)	Security
Responsible Group Procedure (Typical)	Documented actions to be taken by the recipients/responsible group.
References	N/A

Use Case: **Netflow/Data Upload Threshold Exceeded Traffic to Internet Exfil**

Submitted by: Kevin Gennuso, Ryan Voloch

Data Sources	Edge Netflow, Firewall or Proxy Logs
Correlated Data Source	Server Networks
Goal	Detects mass amount of data leaving organization.
Description	Attacker uses a compromised system to exfil data to an external network. Detecting the data leaving the server out to the internet using Netflow or firewall log data (like bytesout).
Pseduo Code/Logic	Internal host sends > 10MB to an untrusted/unknown/uncommon destination (workstations) or beyond a defined baseline (servers). Netfow: sum(dOctets) >=10 MB within 1 minute)
Responsible Group (Typically)	Security Operations Center
Responsible Group Procedure (Typical)	Review for false detections due to communications to legitimate systems. Work with system owners to validate data transfer. If not authorized, escalate and investigate for potential attacker data exfil.
References	https://www.cpni.gov.uk/Documents/Publications/2014/2014-04-11-de_lancaster_technical_report.pdf https://www.sans.org/reading-room/whitepapers/networkdevs/shedding-light-security-incidents-network-flows-33935z

Honorable Mentions

- Authentication with Corporate Credentials to Untrusted Site (Phish Detection)
- New Port Listening on Server Possible Shell
- Windows Technical Command Issued by Non-Technical Windows User
- New Virtual Machine being spawned
- Encrypted container file (zip/rar,etc) sent outbound from the network (exfil)
- Remote connection from a known TOR exit node
- Man-in-the-middle attack
- Rogue device on network
- Rogue WiFi access point
- Unauthorized Powershell script or command detection

Download http://voloch.com/usecases.zip

Recommendations

- Blue
  - Learn some red: run some offsec tools against servers and see what logs are generated (in DEV of course)

Recommendations

- Blue
  - Doing 3rd party pentest, evaluate IR/SIEM use cases

Download http://voloch.com/usecases.zip

Recommendations

- Blue
  - Make 3rd party pen testers correlate SIEM use to each findings

Download http://voloch.com/usecases.zip


Recommendations

- Blue
  - Read the news: Learn from major attacks to identify new SIEM use cases

Download http://voloch.com/usecases.zip

Recommendations

- Red
  - Offer SIEM use case detection recommendations with your findings (if applicable)

Recommendations

- Red
  - Review the anatomy of the attack with customer and identify key points of detection

Go ahead and download this…

You can download all of the use cases collected
and this slide deck. URL is below.

- http://voloch.com/usecases.zip
  - Includes this presentation and all collected submissions
  - *Submit your use case!*
  - *Watch Hansen vs Predator!*

Thank you!

Ryan Voloch

ryan@voloch.com

Peter Giannoutsos

panoyio@gmail.com