Deploying Security Onion for Monitoring HIDS

AmherstSec Meetup July 2019

Agenda

- Who am I?
- What is Security Onion?
- What problem was I facing?
- Does it work?

What is Security Onion?

"Security Onion is a **free and open source** Linux distribution for **intrusion detection**, enterprise security monitoring, and log management. It includes **Elasticsearch**, **Logstash**, **Kibana**, **Snort**, **Suricata**, **Bro**, **Wazuh**, **Sguil**, **Squert**, **CyberChef**, **NetworkMiner**, and many other security tools."

https://securityonion.net/

What is Security Onion?

"Security Onion is a **free and open source** Linux distribution for **intrusion detection**, enterprise security monitoring, and log management. It includes Elasticsearch, **Logstash**, **Kibana**, Snort, Suricata, Bro, **Wazuh**, Sguil, Squert, CyberChef, NetworkMiner, and many other security tools."

https://securityonion.net/

Logstash

"Logstash is an open source, server-side data processing pipeline that ingests data from a multitude of sources simultaneously, transforms it, and then sends it to your favorite 'stash.'"

https://www.elastic.co/products/logstash

Wazuh

"Wazuh is a free, open source and enterprise-ready security monitoring solution for threat detection, integrity monitoring, incident response and compliance."

https://wazuh.com/

Kibana

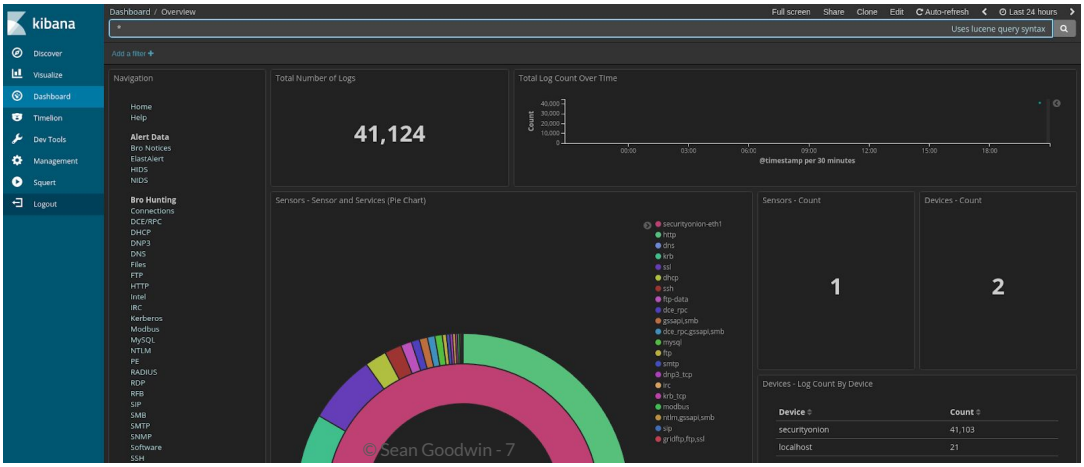


Image courtesy of securityonion.net

The Problem

- Identify a toolset that SMBs can implement to reduce resources needed to detect malicious activity on hosts
- Minimize cost and time spent analyzing event logs
- Minimize time spent vetting alerts for false-positive events

According to the 2018 Verizon Data Breach Investigations Report,

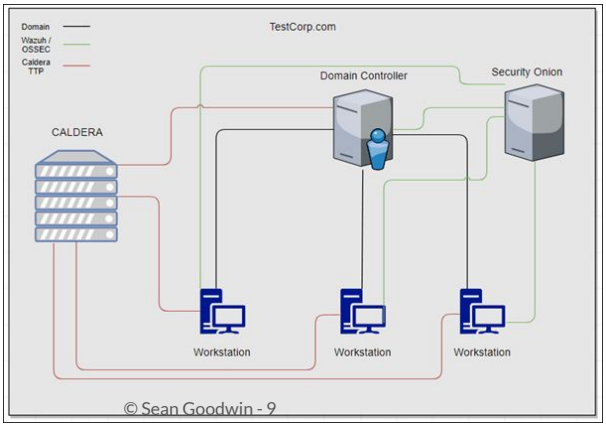
- 50% of breach victims were categorized as small businesses
- 68% of breaches took “months or longer to discover”

To make matters worse, a large percentage of small and medium-sized businesses (SMBs) identify restricted budgets as the greatest challenge to security (Untangle, n.d.). Another significant concern identified in the survey was not having enough staff to “monitor and manage security”.

Identifying a toolset that minimizes cost and complexity while providing actionable alerts will enable an SMB to reduce the time required to identify a breach.

2018 Data Breach Investigations Report (Rep.). (n.d.). Verizon.
Untangle. (n.d.). 2018 SMB It Security Report. Retrieved from https://www.untangle.com/2018-smb-it-security-report/

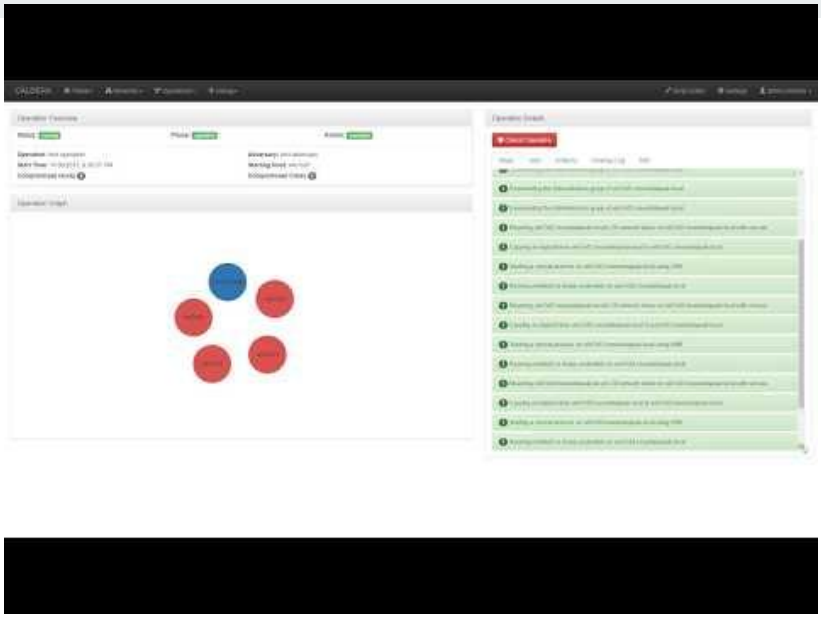
Testing in the Lab



Red Team: Caldera

“CALDERA can be used to test endpoint security solutions and assess a network's security posture against the common post-compromise adversarial techniques contained in the ATT&CK model. CALDERA leverages the ATT&CK model to identify and replicate adversary behaviors as if a real intrusion is occurring.”

https://www.mitre.org/research/technology-transfer/open-source-software/caldera



6 min overview of Caldera

https://www.youtube.com/watch?v=xjDrWStR68E

Blue Team

- Audit Policy (Malware Archaeology)
- Sysmon (SwiftOnSecurity)
- Wazuh Agent

```
PS C:\Windows\system32> AuditPol /get /category:*
System audit policy
Category/Subcategory                    Setting
System
  Security System Extension             Success and Failure
  System Integrity                      Success and Failure
  IPsec Driver                          Success
  Other System Events                   Failure
  Security State Change                 Success and Failure
Logon/Logoff
  Logon                                 Success and Failure
  Logoff                                Success
  Account Lockout                       Success
  IPsec Main Mode                       No Auditing
  IPsec Quick Mode                      No Auditing
  IPsec Extended Mode                   No Auditing
  Special Logon                         Success and Failure
  Other Logon/Logoff Events             Success and Failure
  Network Policy Server                 Success and Failure
  User / Device Claims                  No Auditing
  Group Membership                      Success
Object Access
  File System                           Success
  Registry                              Success
  Kernel Object                         No Auditing
  SAM                                   Success
  Certification Services                Success and Failure
  Application Generated                 Success and Failure
  Handle Manipulation                   No Auditing
  File Share                            Success and Failure
  Filtering Platform Packet Drop        No Auditing
  Filtering Platform Connection         Success
  Other Object Access Events            No Auditing
  Detailed File Share                   Success
  Removable Storage                     Success and Failure
  Central Policy Staging                No Auditing
Privilege Use
  Non Sensitive Privilege Use           No Auditing
  Other Privilege Use Events            No Auditing
  Sensitive Privilege Use               Success and Failure
Detailed Tracking
  Process Creation                      Success and Failure
  Process Termination                   No Auditing
  DPAPI Activity                        No Auditing
  RPC Events                            Success and Failure
  Plug and Play Events                  Success
  Token Right Adjusted Events           Success
Policy Change
  Audit Policy Change                   Success and Failure
  Authentication Policy Change          Success and Failure
  Authorization Policy Change           Success and Failure
  MPSSVC Rule-Level Policy Change       No Auditing
  Filtering Platform Policy Change      Success
  Other Policy Change Events            No Auditing
Account Management
  Computer Account Management           Success and Failure
  Security Group Management             Success and Failure
  Distribution Group Management         Success and Failure
  Application Group Management          Success and Failure
  Other Account Management Events       Success and Failure
  User Account Management               Success and Failure
DS Access
  Directory Service Access              No Auditing
  Directory Service Changes             Success and Failure
  Directory Service Replication         No Auditing
  Detailed Directory Service Replication  No Auditing
Account Logon
  Kerberos Service Ticket Operations    No Auditing
  Other Account Logon Events            Success and Failure
  Kerberos Authentication Service       No Auditing
  Credential Validation                 Success and Failure
PS C:\Windows\system32>
```

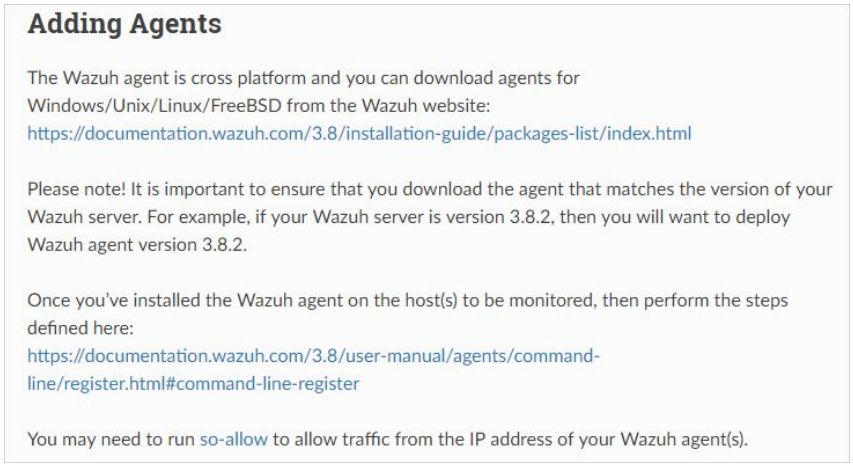

https://static1.squarespace.com/static/552092d5e4b0661088167e5c/t/5c586681f4e1fced3ce1308b/1549297281905/Windows+Logging+Cheat+Sheet_ver_Feb_2019.pdf

Sysmon

https://github.com/SwiftOnSecurity/sysmon-config

```
C:\Windows\system32>sysmon.exe -accepteula -i sysmonconfig-export.xml
```

Wazuh



Adding Agents

The Wazuh agent is cross platform and you can download agents for Windows/Unix/Linux/FreeBSD from the Wazuh website:
https://documentation.wazuh.com/3.8/installation-guide/packages-list/index.html

Please note! It is important to ensure that you download the agent that matches the version of your Wazuh server. For example, if your Wazuh server is version 3.8.2, then you will want to deploy Wazuh agent version 3.8.2.

Once you've installed the Wazuh agent on the host(s) to be monitored, then perform the steps defined here:
https://documentation.wazuh.com/3.8/user-manual/agents/command-line/register.html#command-line-register

You may need to run so-allow to allow traffic from the IP address of your Wazuh agent(s).

https://securityonion.readthedocs.io/en/latest/wazuh.html

The Good

- All the necessary data was captured
- Custom local rules are easily written
- Filtering in the Kibana dashboard is intuitive

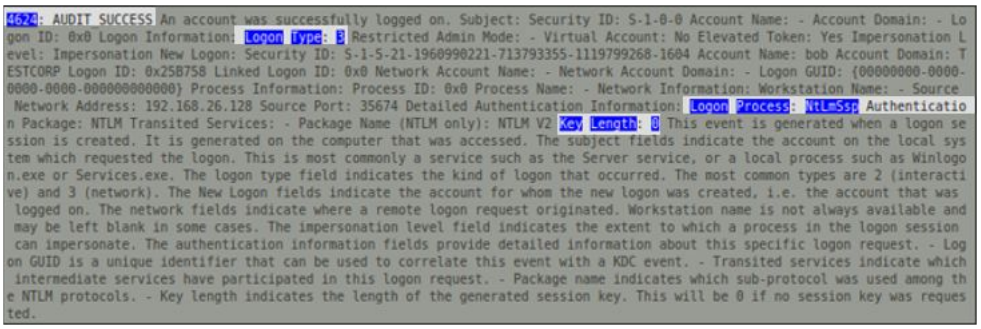
The Bad

- None of the tested attacks generated high priority alerts
- “Living off the Land” attacks only visible after the attack

Hunting PSexec

```
5145: AUDIT SUCCESS A network share object was checked to see whether client can be granted desired access. Subject: Security
 ID: S-1-5-21-1960990221-713793355-1119799268-1109 Account Name: admin02 Account Domain: TESTCORP Logon ID: 0x9D2E5A Network
 Information: Object Type: File Source Address: 192.168.26.20 Source Port: 49782 Share Information: Share Name: \\*\IPC$ Shar
e Path: Relative Target Name: PSEXESVC-5501-WKSTN1-4020-stdout Access Request Information: Access Mask: 0x120089 Accesses: RE
AD CONTROL SYNCHRONIZE ReadData (or ListDirectory) ReadEA ReadAttributes Access Check Results: -
```

Hunting Pass-the-Hash



Hunting File Collection

```
5142: AUDIT_SUCCESS A network share object was added. Subject: Security ID: S-1-5-21-1960990221-713793355-1119799268-1109 Acc
ount Name: admin02 Account Domain: TESTCORP Logon ID: 0x260B9F Share Information: Share Name: \\*\Documents Share Path: C:\Us
ers\admin02\Documents
```

Sample Custom Rule

```
<!-- Built-in rule 1807 is used as our initial trigger. Below each of the search criteria discussed in the paper
are presented in a chain. If all search criteria are met, a level 7 alert is raised for further investigation.

<rule id="18107" level="3">
        <if_sid>18104</if_sid>
         <id>^4528$|^5408$|^4673$|^4624$|^4769$</id>
        <description>Windows Logon Success.</description>
        <group>authentication_success,pci_dss_10.2.5,gpg13_7.1,gpg13_7.2,gdpr_IV_32.2,</group>
</rule>
-->

<!-- This rule searches any entries that match rule 18107 for the string 'S-1-0-0' (Security ID) -->
<rule id="100002" level="1">
        <if_sid>18107</if_sid>
        <match>S-1-0-0</match>
        <description>S-1-0-0 successful Auth</description>
</rule>

<!-- This rule searches any entries that match rule 100002 for the string 'Logon Type:  3' -->
<rule id="100003" level="1">
        <if_sid>100002</if_sid>
        <match>Logon Type:  3</match>
        <description>Logon Type:  3</description>
</rule>

<!-- This rule searches any entries that match rule 100003 for the string 'Logon Process: NtLmSsp' -->
<rule id="100004" level="1">
        <if_sid>100003</if_sid>
        <match>Logon Process: NtLmSsp</match>
        <description>Logon Process: NtLmSsp</description>
</rule>

<!-- This rule searches any entries that match rule 100004 for the string 'Key Length:  0'. If this rule is
triggered, all search criteria have been met, and this event warrants further investigation -->
<rule id="100005" level="7">
        <if_sid>100004</if_sid>
        <match>Key Length:  0</match>
        <description>Potential Pass the Hash!</description>
</rule>
```

Companion Blog Post

https://www.seangoodwin.blog/amherstsec-july-2019

or

https://bit.ly/2xbYh1N

Contact Info

@0xSeanG on Twitter

SeanGoodwin.blog