Contents

[INTRODUCTION 1](#_Toc500514432)

[SYSMON 2](#_Toc500514433)

[LEVEL OF VISIBILITY 4](#_Toc500514434)

[PREVENT THREATS 8](#_Toc500514435)

[RESPONSE CAPABILITIES 9](#_Toc500514436)

[ENDPOINT IMPACT 9](#_Toc500514437)

[SECURITY CONTROLS 10](#_Toc500514438)

[SPLUNK 10](#_Toc500514439)

[LEVEL OF VISIBILITY 12](#_Toc500514440)

[PREVENT THREATS 19](#_Toc500514441)

[RESPONSE CAPABILITIES 24](#_Toc500514442)

[ENDPOINT IMPACT 26](#_Toc500514443)

[SECURITY CONTROLS 27](#_Toc500514444)

[SYSMON AND SPLUNK INTEGRATION 28](#_Toc500514445)

[SPECIAL CONFIG FOR SYSMON 31](#_Toc500514446)

[TESLA 32](#_Toc500514447)

[REFERENCES 32](#_Toc500514448)

# INTRODUCTION

This lab will analyze two EDR (Endpoint Detection and Response) systems:

* Microsoft SYSMON
* SPLUNK

[1] states the 13 essential questions to guide EDR evaluation. For purposes of this lab, the following questions will be considered:

* **What level of visibility does the solution provide?**

An EDR solution has limited value if it cannot record and use a rich set of information collected from protected endpoints.

* **Does the solution prevent threats from executing?**

Many EDR solutions focus on either threat prevention or detection.

* **What response capabilities does the solution offer?**

Look for EDR solutions that includes actionable intelligence about threats and the capabilities to respond so your team can immediately react to the threat and stop it before it does more damage to your organization.

* **What is the impact to your endpoints?**

Most EDR solutions use a complex agent that is tightly integrated into the endpoint’s operating system, meaning it can have serious performance impacts and cause instability if not well designed and tested.

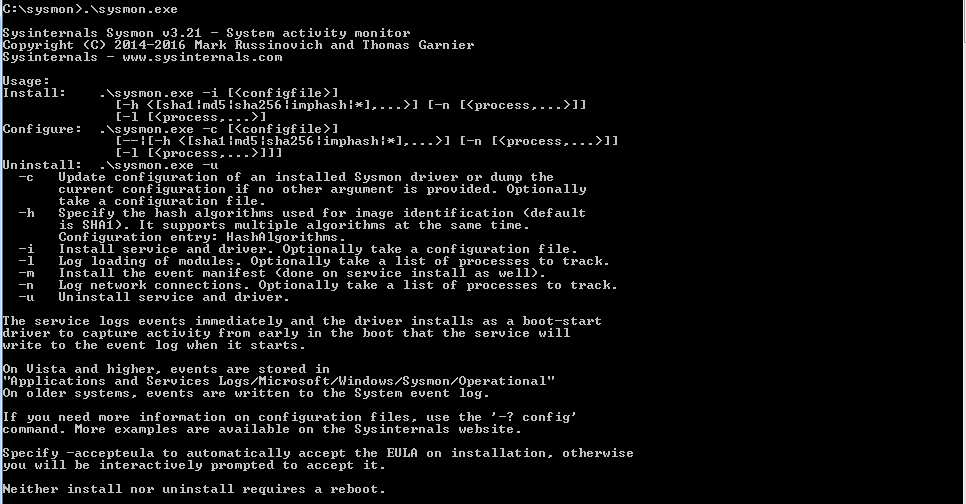
* **What security controls does the solution use to protect itself?**

An EDR solution is a large security risk to your organization if the solution is not designed to detect tampering and secure the data collected from your endpoints.

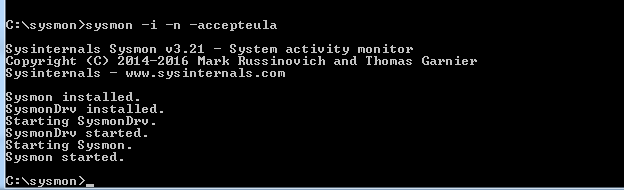
Besides trying to answer these questions for EDR system evaluated, any limitations noticed will be explained. SYSMON is freely available. SPUNK is a commercial EDR and offers general trial versions. SYSMON and SPUNK will be compared to each other as well as compared to other commercial EDRs when appropriate.

# SYSMON

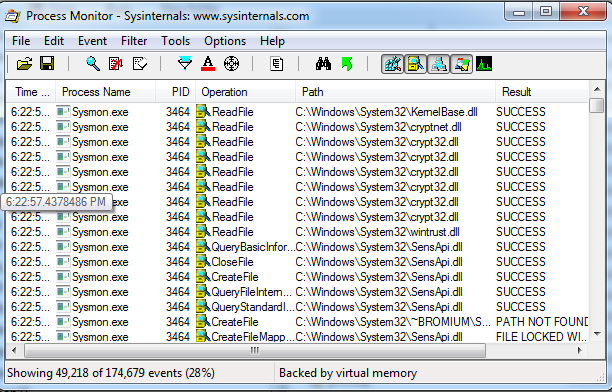
[2] states “System Monitor (Sysmon) is a Windows system service and device driver that, once installed on a system, remains resident across system reboots to monitor and log system activity to the Windows event log. It provides detailed information about process creations, network connections, and changes to file creation time. Note that Sysmon does not provide analysis of the events it generates, nor does it attempt to protect or hide itself from attackers.”



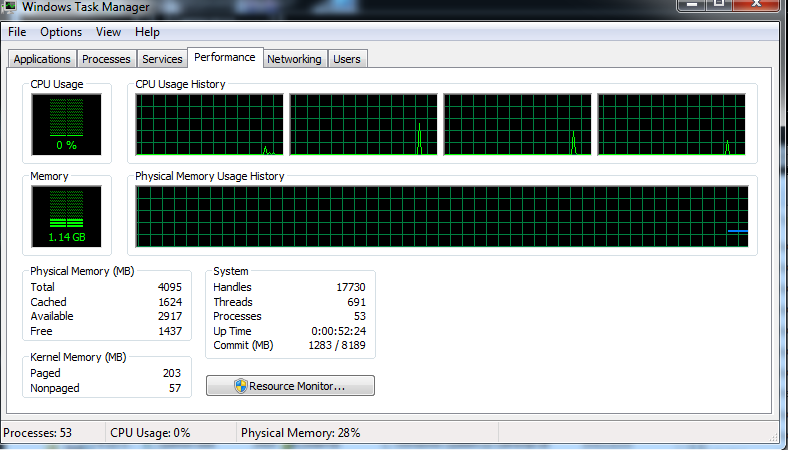
There are three options: Install, Configure, Uninstall.



SYSMON installed



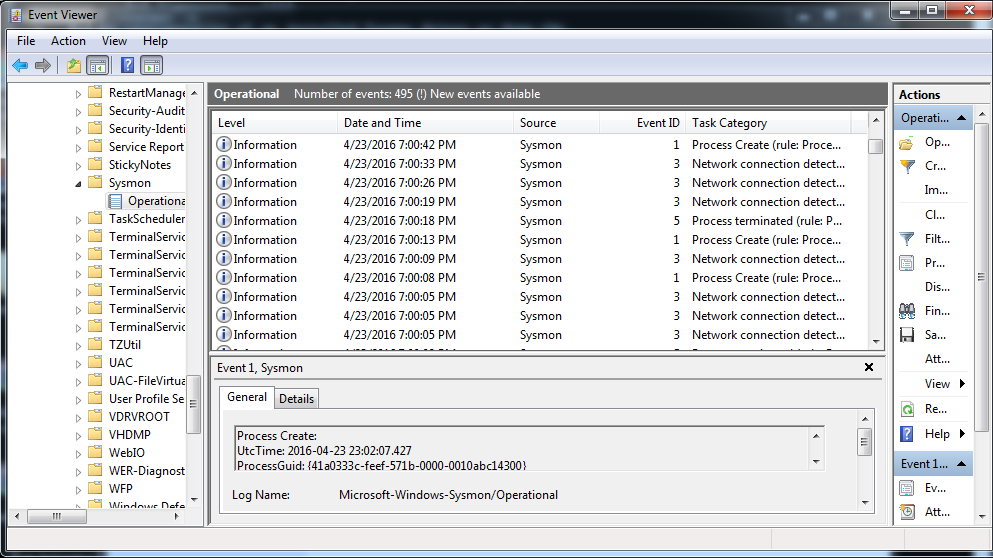
After the installation of SYSMON, I started PROCMON. It shows SYSMON reading lots of files.

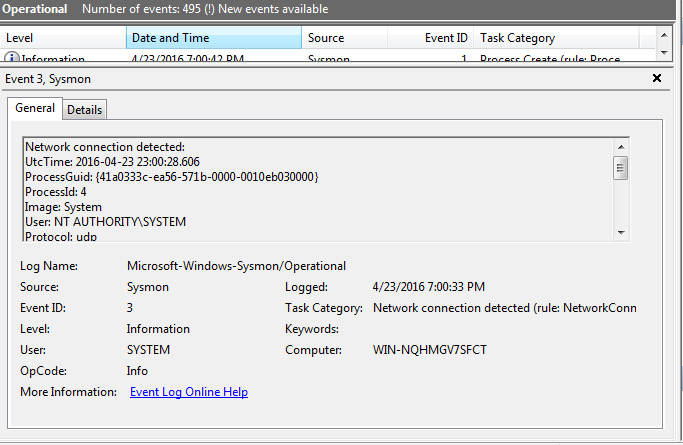


During the installation, there was very little impact to this endpoint, my VM used for testing.

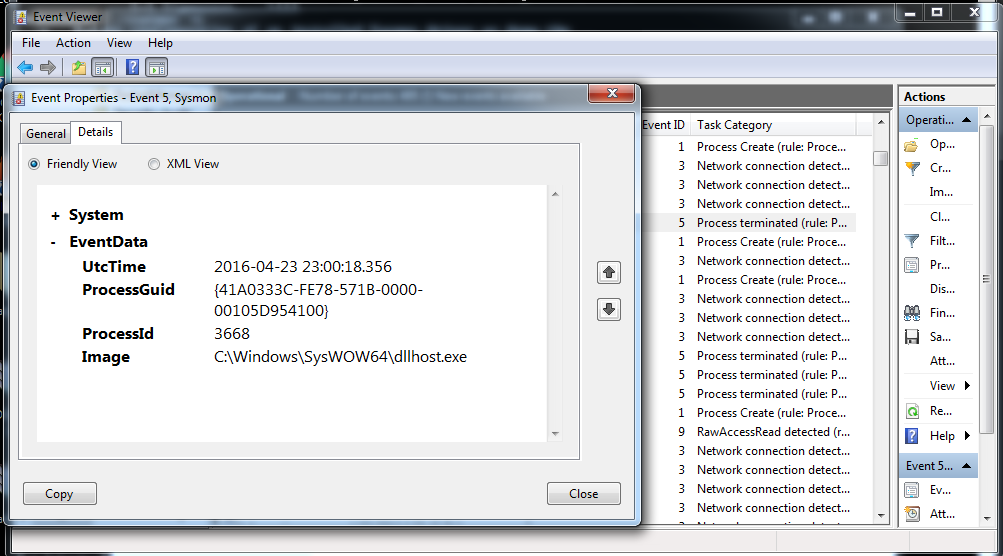
## LEVEL OF VISIBILITY

[2] states “provides detailed information about process creations, network connections, and changes to file creation time… collecting the events it generates using Windows Event Collection or SIEM agents” Therefore, SYSMON appears to be limited in what is analyzed and does not provide a central repository for all endpoints. Other tools are needed to integrate with SYSMON for a central repository for ease of reporting, such as SPLUNK [3].

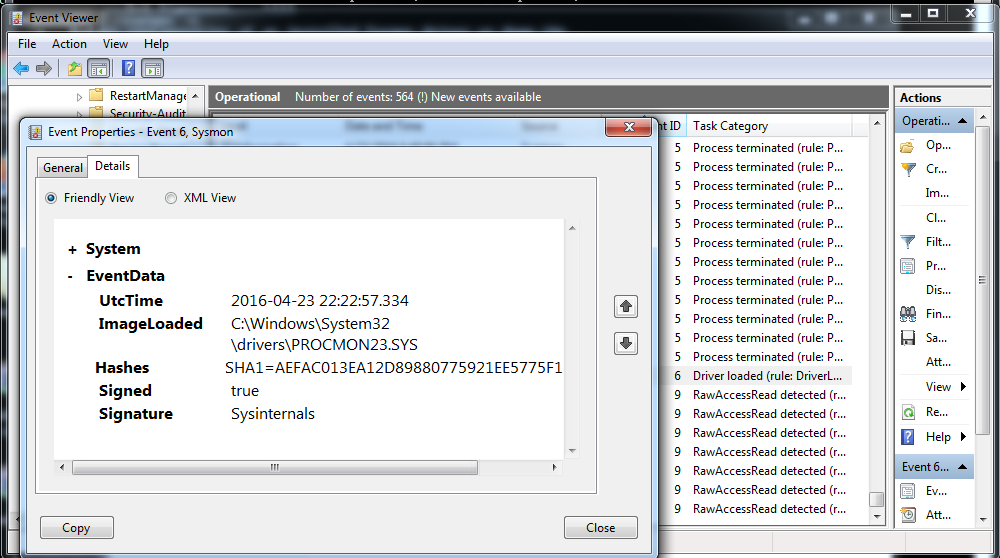


In the Event Viewer [Applications and Services ->Microsoft->Windows->Sysmon->Operations], Network connections, Process Create, RawAceessRead and Process Terminated events were recorded. I performed several actions to generate these events: Internet Browsing, Editing DLL’s, and Reading files. I could have performed other actions to trigger other events, but I feel that these changes have given me enough information for evaluation. 

Event logger provides a General and Details tab. In the General tab, basic information is provided about the process, such as process id, time ……… This example is for a network connection.



Details provide more in-depth information. For example, the Image is provided. This event is for a Process terminated.



Above the Driver Loaded Event is triggered for the PROCMON I used to monitor SYSMON. I have been able to monitor many events, but the only way to view these events, without an additional tool, is thru windows event viewer. Event viewer does not seem to have a search function. If WEF (Windows Event Forward) [8] is not turned on, to view the events for the endpoint, you must log into that endpoint, since SYSMON does not provide any additional reporting tools beyond the standard event viewer.

[7] states “While logging is nice, it provides no value if the log is not reviewed. The purpose of this post is to provide an easy and automated way to present the Sysmon event log for review … To turn the XML event log into an easier to digest file, we can use Microsoft Logparser. Logparser will parse the event log into a CSV file … To pull further information out of the file, we can turn to TekDefense’s TekCollect python script. This script will help us gather all IP Address, MD5 hashes, domain names, and executable names.”.

Several other tools are mentioned to perform various other analysis. The point here, [7] has to use several different tools; seems like a cumbersome and time-consuming process to perform EDR with SYSMON. And, do we have lots of time to perform EDR when under an attack? Do we want to be using different tools or do we want one tool, like an army Swiss knife, that can perform most of the analysis? As for me, I would like to keep it as simple as possible and opt for one tool that performs the EDR, whenever possible.

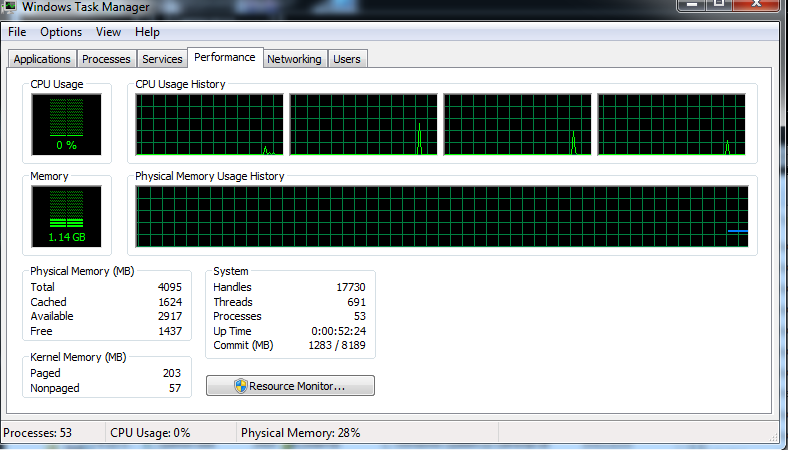
## PREVENT THREATS

SYSMON, alone, does not prevent threats. SYSMON records events into the Windows Event Logging mechanism. Another tool is needed that takes this information and then reacts to and responds the event. The information could be sent to MATA (Microsoft Advanced Threat Analytics) [4] to perform advanced analysis, such as in recognizing abnormal entity behavior and profiling normal behavior. It even seems, MATA, detects but does not prevent. For visibility and preventing threats, various additional tools are needed.

## RESPONSE CAPABILITIES

SYSMON does not contain any response capabilities. Each server running SYSMON could have WEF (Windows Event Forwarding) enabled [8]. The events could be sent to a centralized server for analysis or even sent to MATA. For example, MATA can be the centralized server for Windows Events and does respond to alerts. Stated by [4] “After detecting suspicious activities, known security issues and malicious attacks in near real-time, ATA provides clear, functional, actionable information on a simple attack timeline.”

## ENDPOINT IMPACT



Monitoring my VM with Task Manager, demonstrated that SYSMON has a negligible performance impact. But, I wonder the performance impact on a very active server and how large and fast the log can grow?

## SECURITY CONTROLS

Since SYSMON utilizes the Windows Event Viewer, securing this data that SYSMON reports on is performed by the Windows security for the end point. For example, security could be established for, only, System Administrators to access the even viewer. There is a Sysmon Trojan that first appeared in 2006 [5]. Security on the SYSMON exe itself should be limited to the System Administrator or Security Administrator via Windows security mechanisms. SYSMON runs as a service in the background and if that service is cancelled, then SYSMON logging stops. If an attacker were to gain the necessary privileges, then SYSMON could be stopped, thus its logging stopped, and it is possible this attack could go undetected.

# SPLUNK

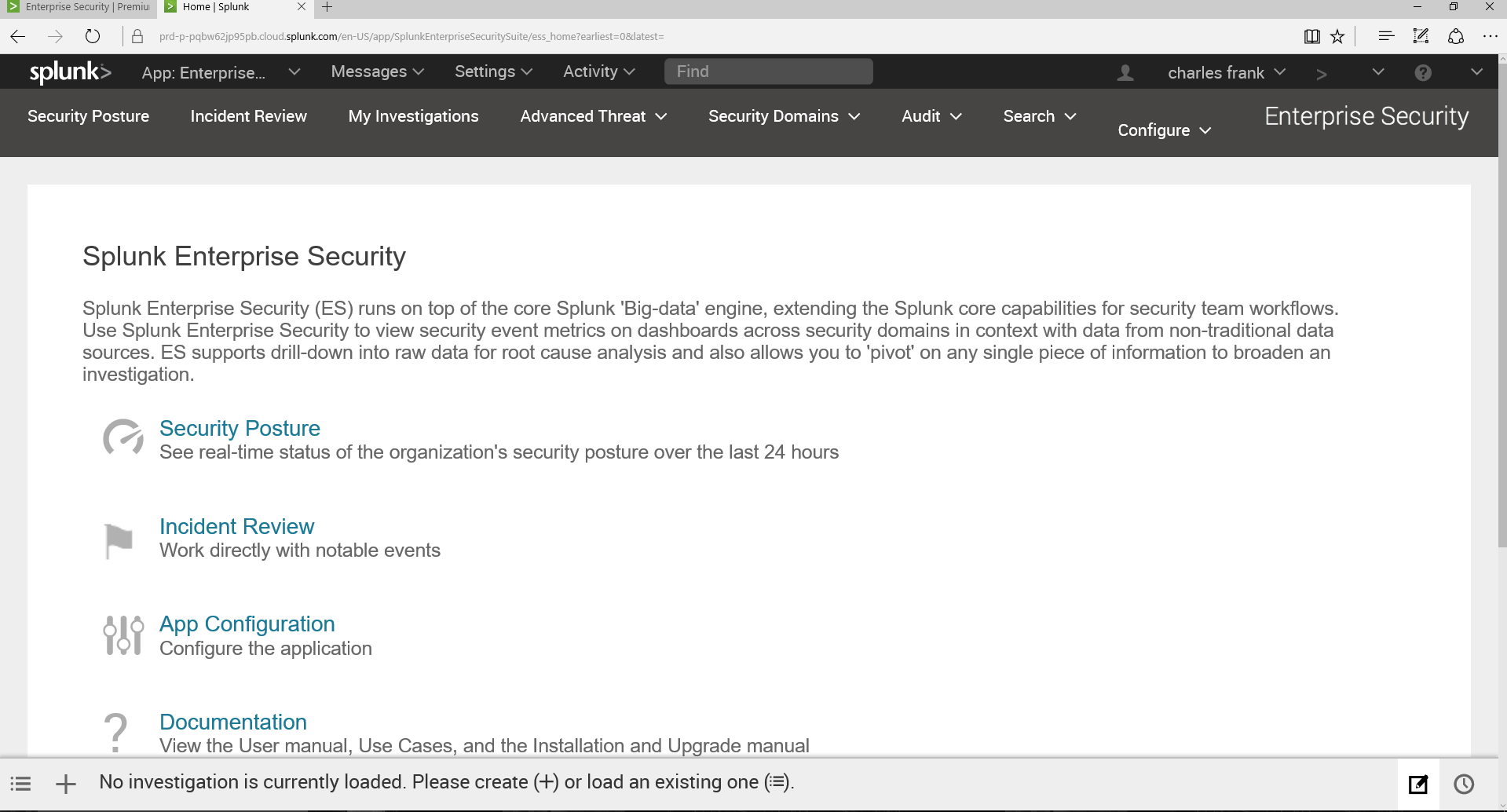
Stated in [9], SPLUNK offers several cybersecurity solutions:

* Security and Fraud
* **Log Management**
* **Splunk Enterprise Security**
* **User Behavior Analytics**
* **Advanced Threat Detection**
* **Insider Threats**
* Compliance
* Fraud

Of particular interest for the purposes of this lab are: Log Management, Splunk Enterprise Security, User Behavior Analytics, Advanced Threat Detection and Insider Threats. SPLUNK provides extensive capabilities for collecting and analyzing log information. Splunk ES (Enterprise Security) provides insight into network, endpoint, access, malware, vulnerability and identity information. Splunk UBA (User Behavior Analytics) discovers known, unknown, and hidden threats using data science, machine learning, behavior baseline, peer group analytics and advanced correlation.

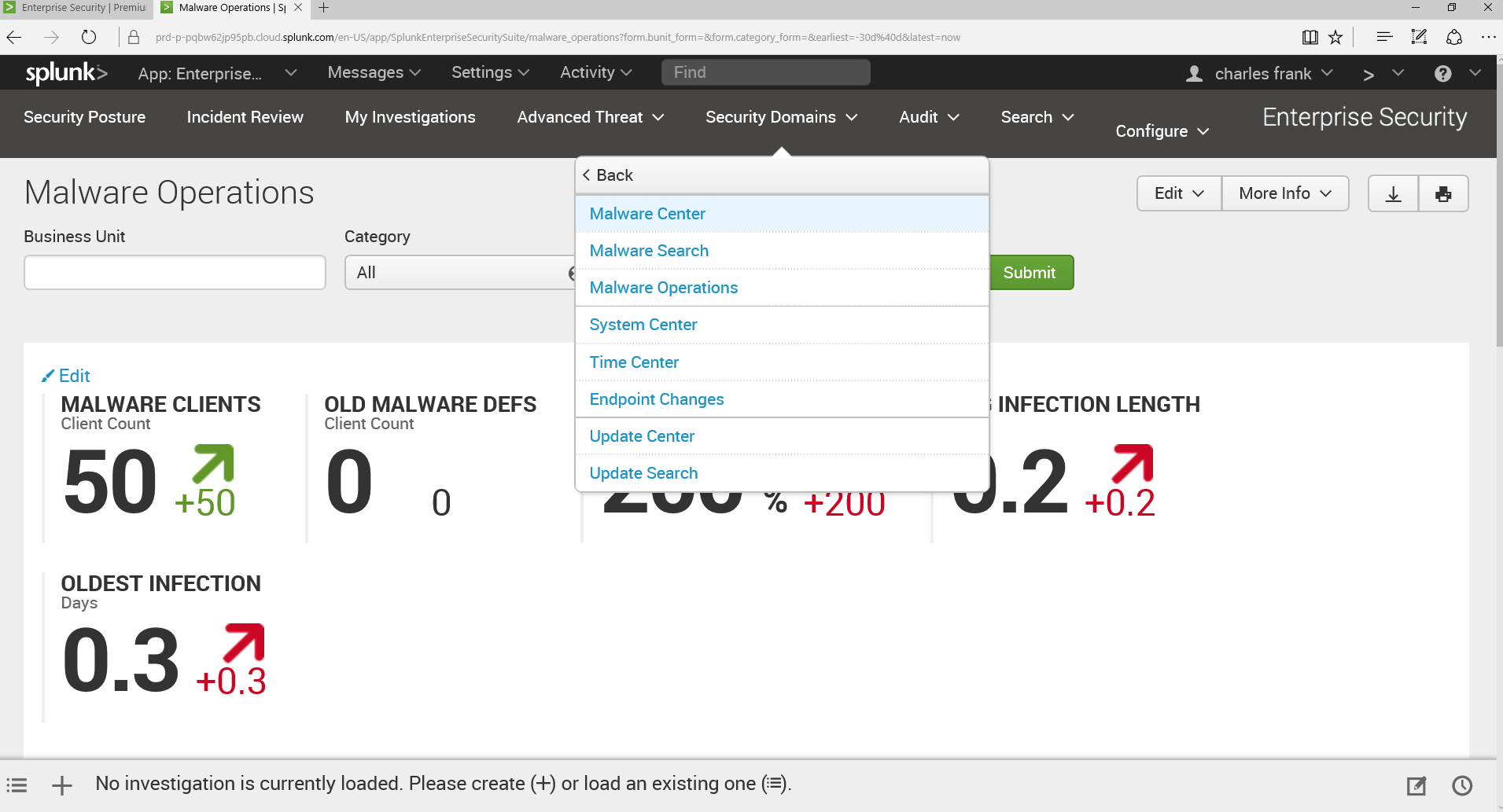


SPLUNK offers a free 7 day evaluation of SPLUNK ES. I am excited that I have discovered this evaluation. I searched high and low for commercial EDR evaluations and could not find one worth while or I had to leave my contact information but I was never contacted back. Plus, SPLUNK has made this easy. No need to download or install anything. The sandbox is ready for access.

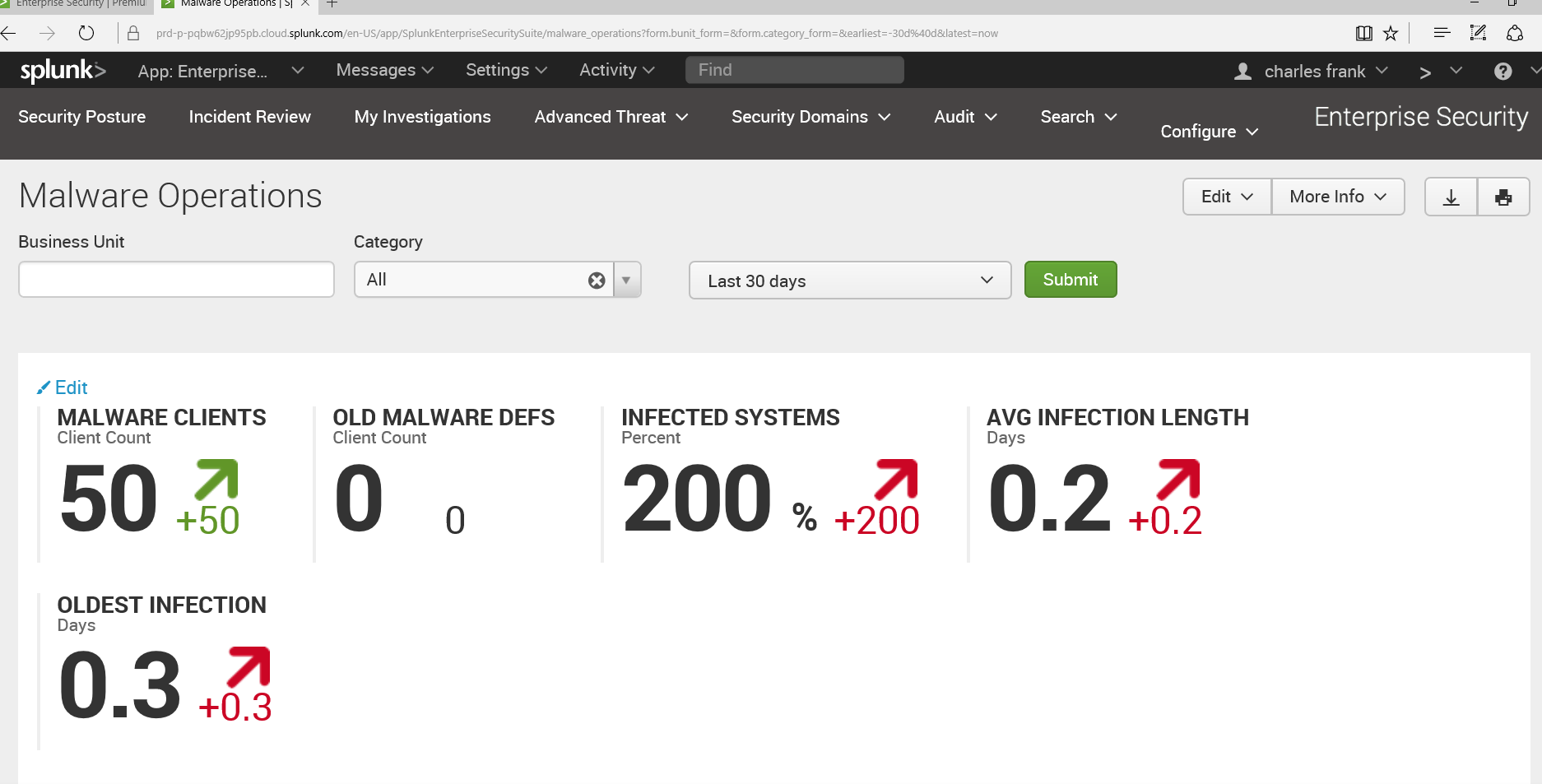


Logging in you are provided with lots of options. I think, there are way too many options to elaborate on for this lab, therefore I will focus on the same questions I focused on for SYSMON.

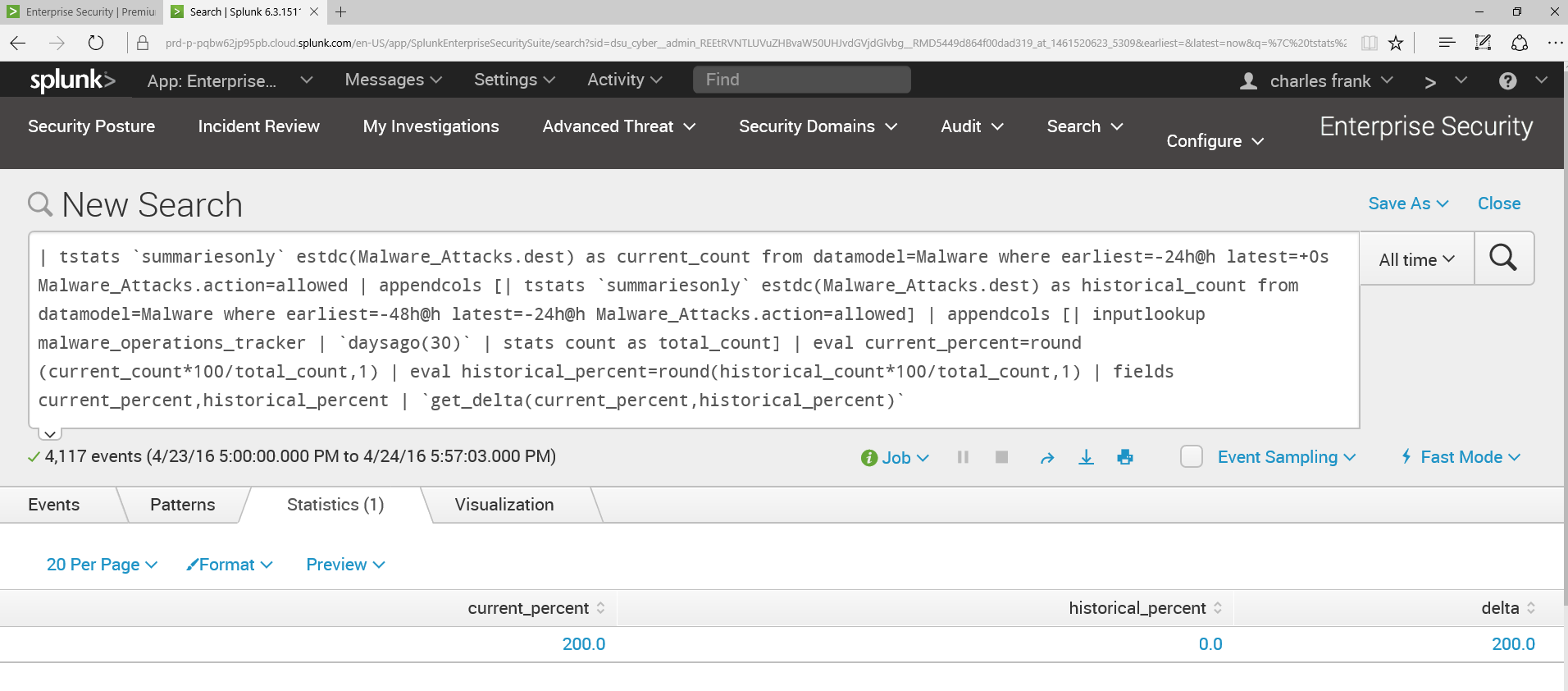
## LEVEL OF VISIBILITY



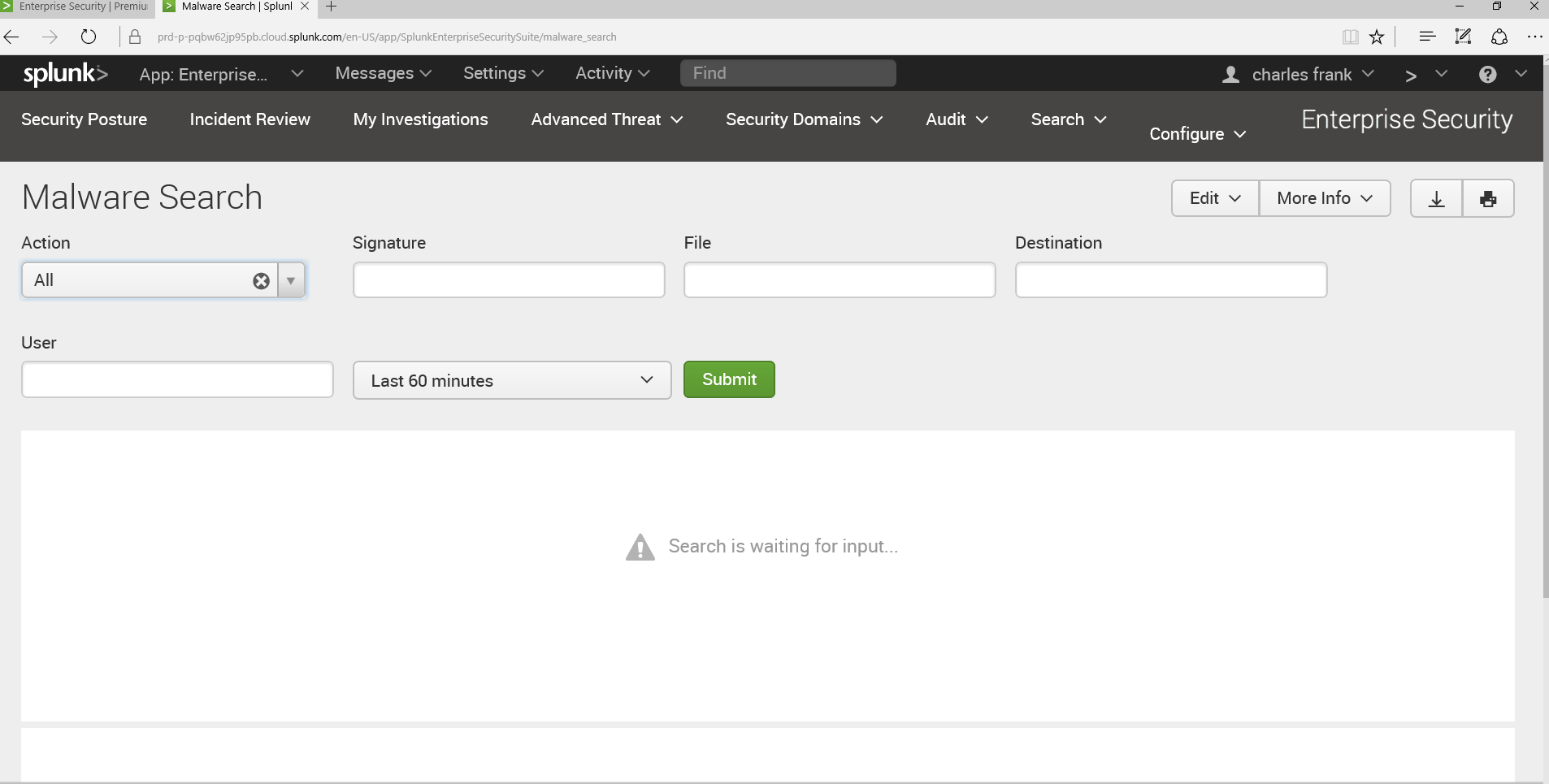
The strength of SPLUNK is in its level of visibility. The SPLUNK “big-data” engine stores extensive amounts of information. For the example above, I have chosen Security Domains -> Malware Operations. Considering this is an Advanced Malware Analysis class, I figured this might be a good choice. ☺



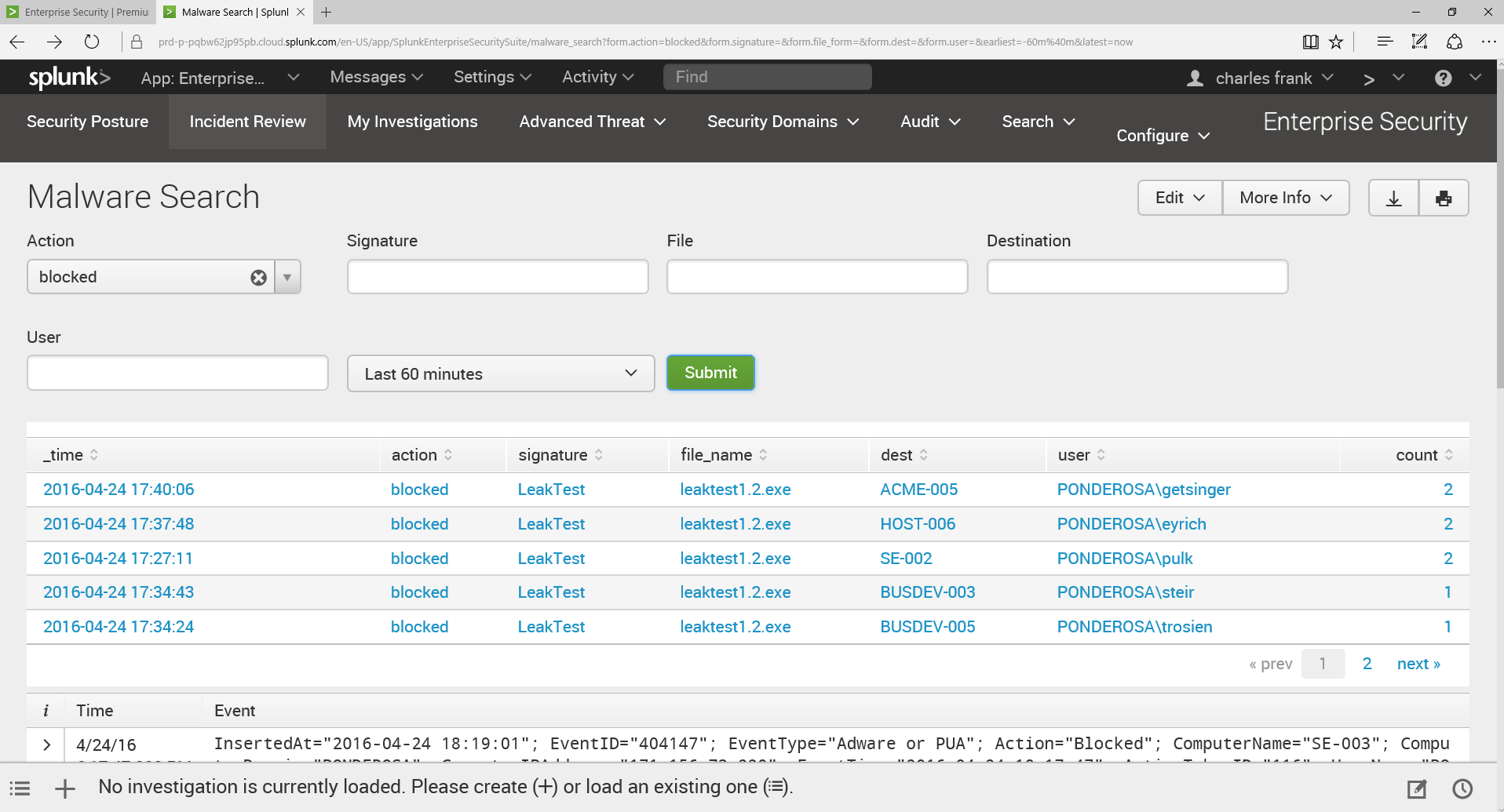
50 Malware Clients and 200% infected Systems. This screen is showing that Malware infection is on the rise as well as the Avg. Infection Length and Oldest Infection.



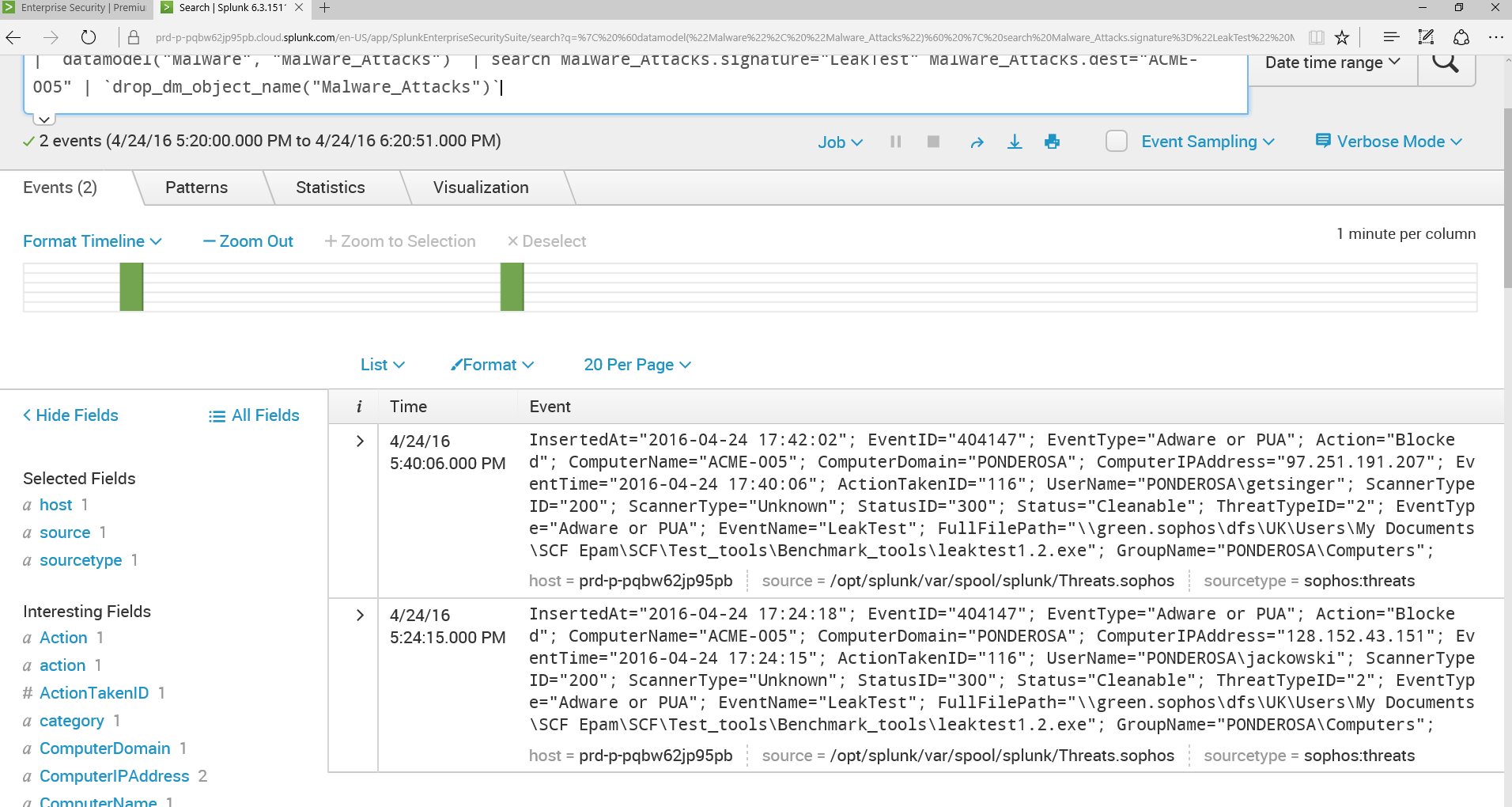
Clicked on infected systems, and the actual SPLUNK search language is displayed along with the result of the 200 percent. There were 4,117 in one day, recorded in the SPLUNK “big data” engine.



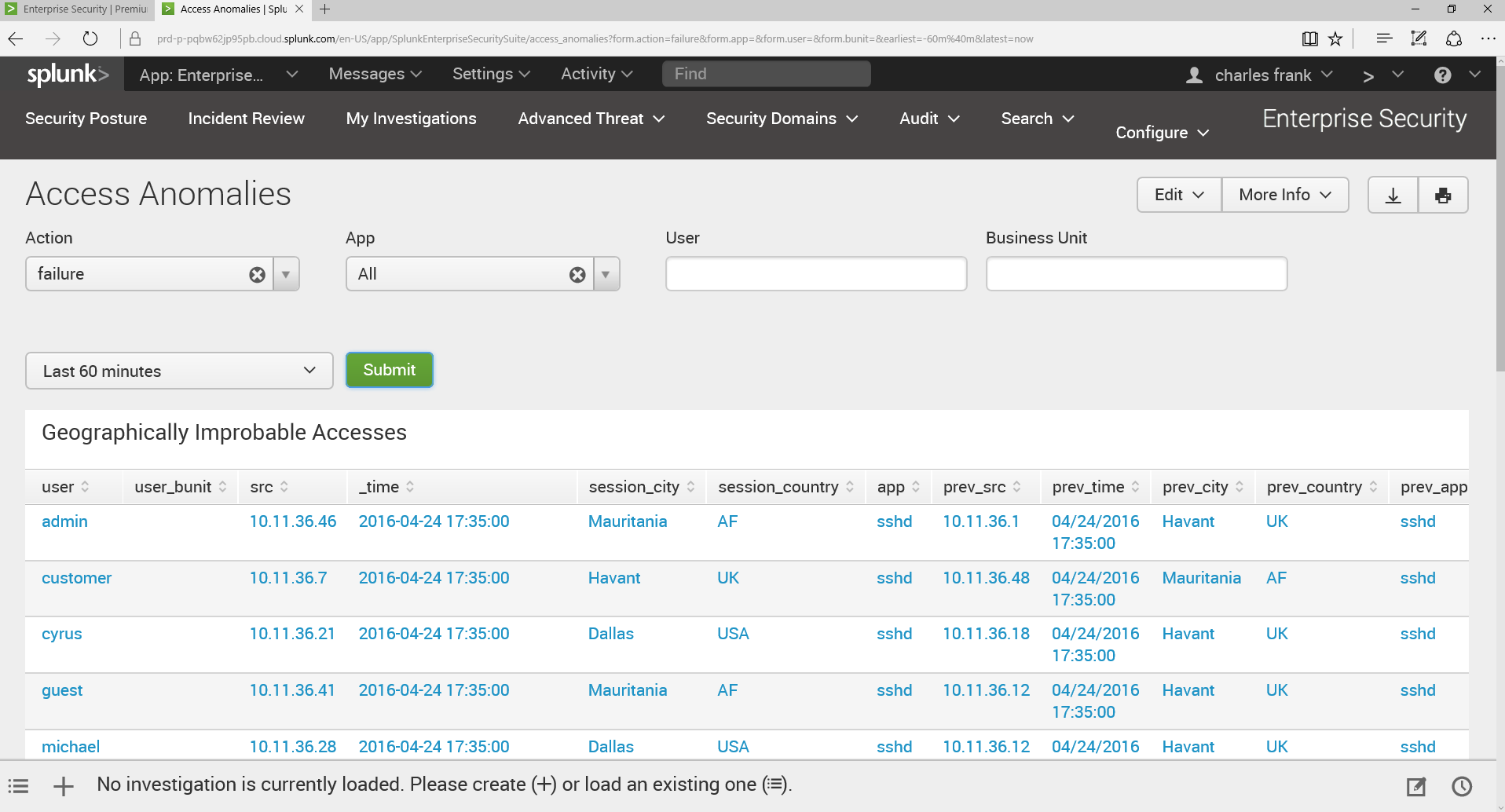
Under Security Domains -> Endpoint -> Malware Search, you are presented this search screen.



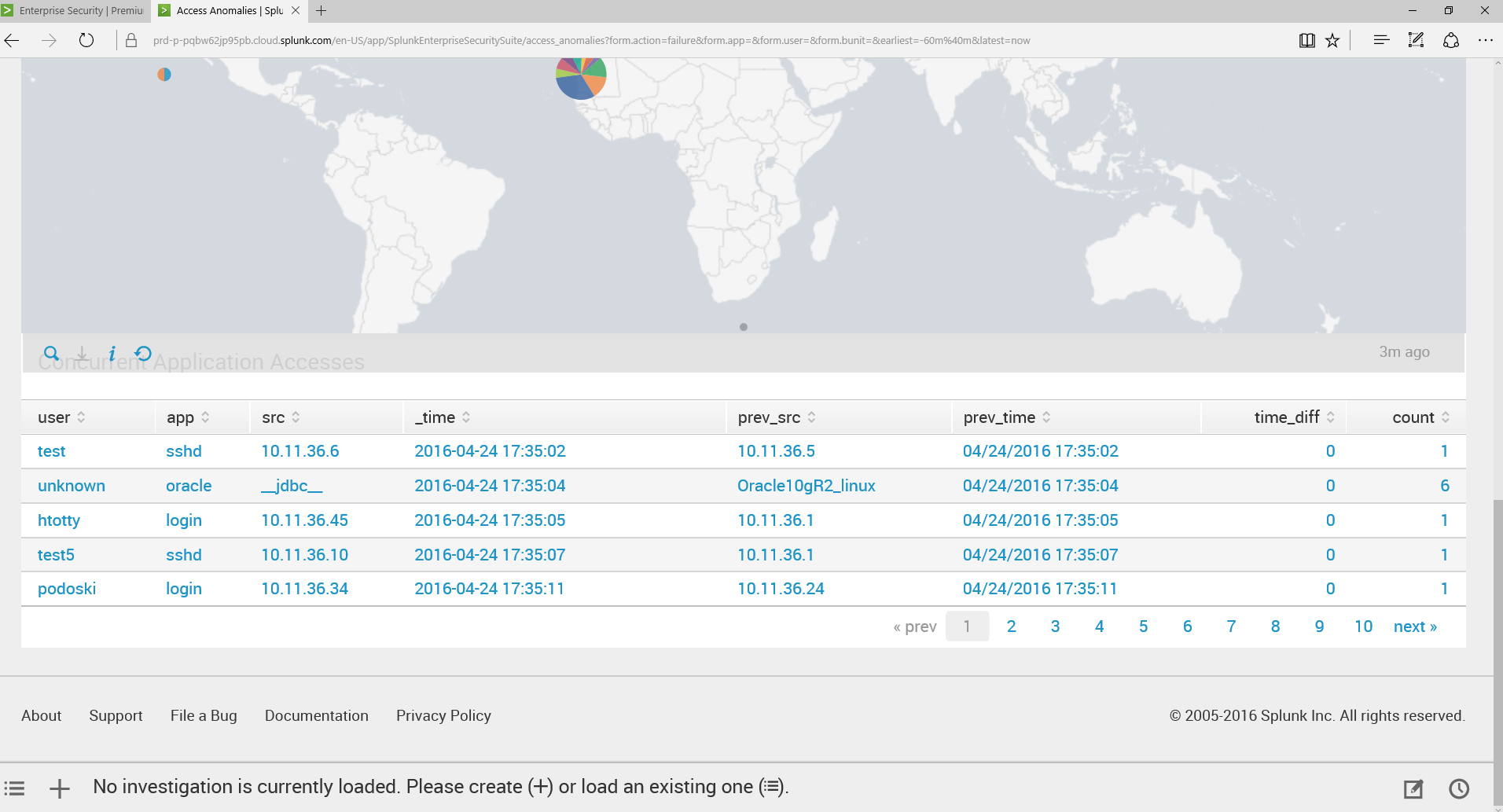
Searched for blocked malware. This is clearly signature based. In the bottom window pane is the actual SPLUNK statement which generated these results.



Clicking on the MALWARE, you are brought into a more detailed screen providing more information about this malware event. Notice, the malware was recognized by SOPHOS threat signature.



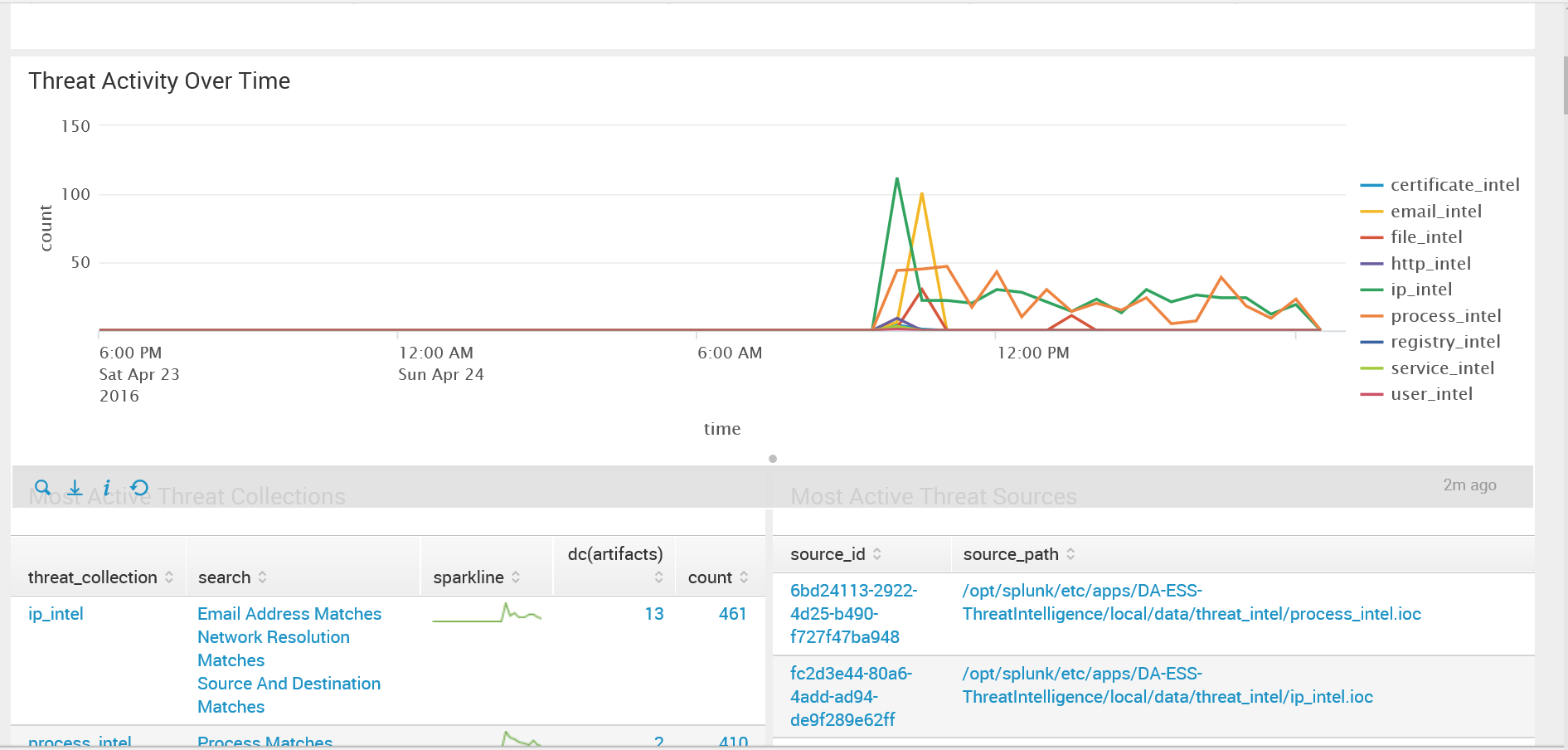
Above, Advanced Threat -> Access Anomalies. This is the behavioral analysis. SPLUNK is identify abnormal user access behavior. I chose access failures. Maybe, if MALWARE went un-detected by signatures, maybe it is trying to communicate with a site that is no longer available?



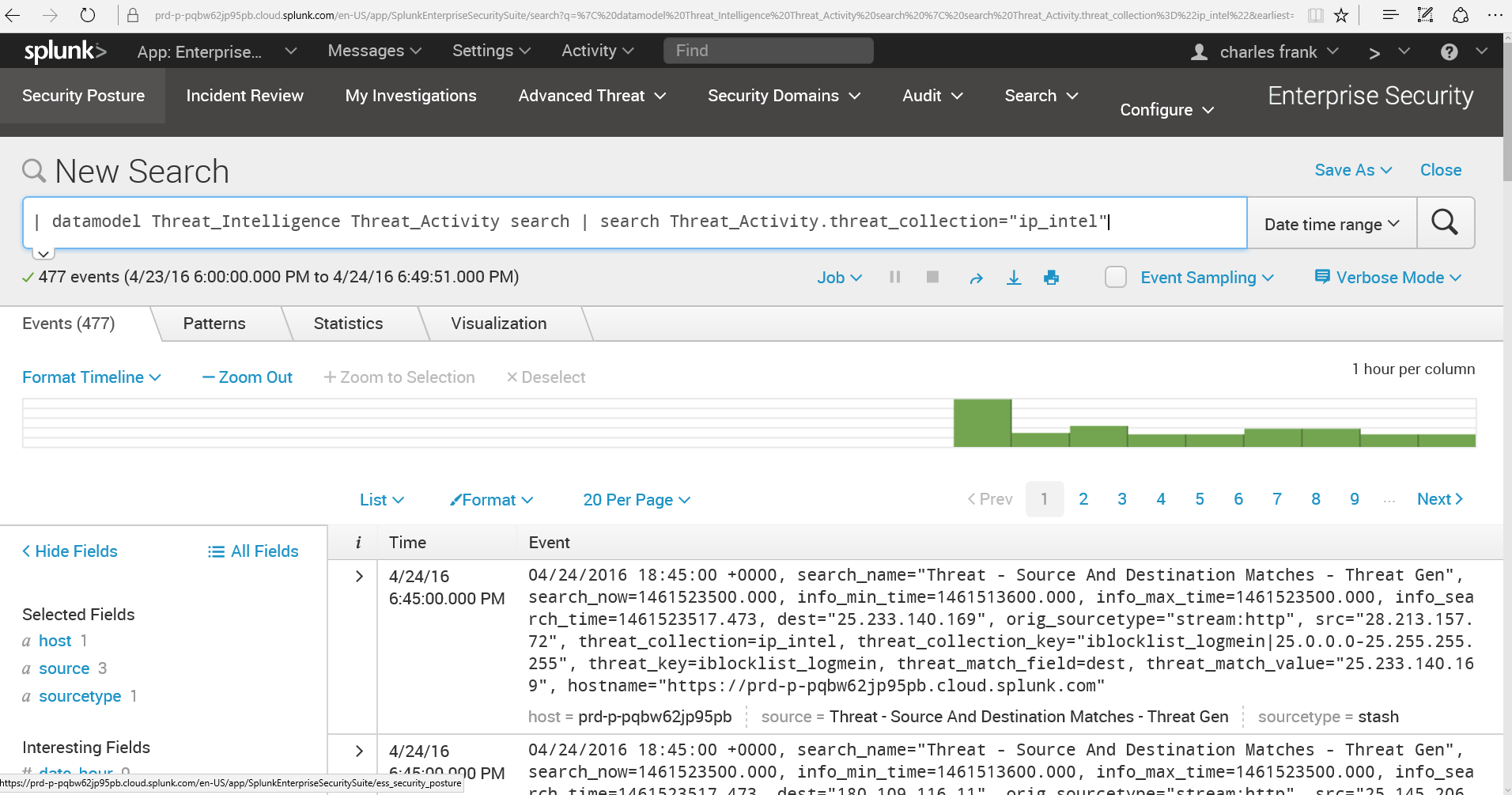
Scrolling down, I get a nice geographic display as well as some additional information concerning the access. For example, on the second line, there is indication of an ORACLE 10G database being communicated thru JDBC.



Clicking on that line, I am able to drill down to all of the ORACLE DB accesses around that time frame.



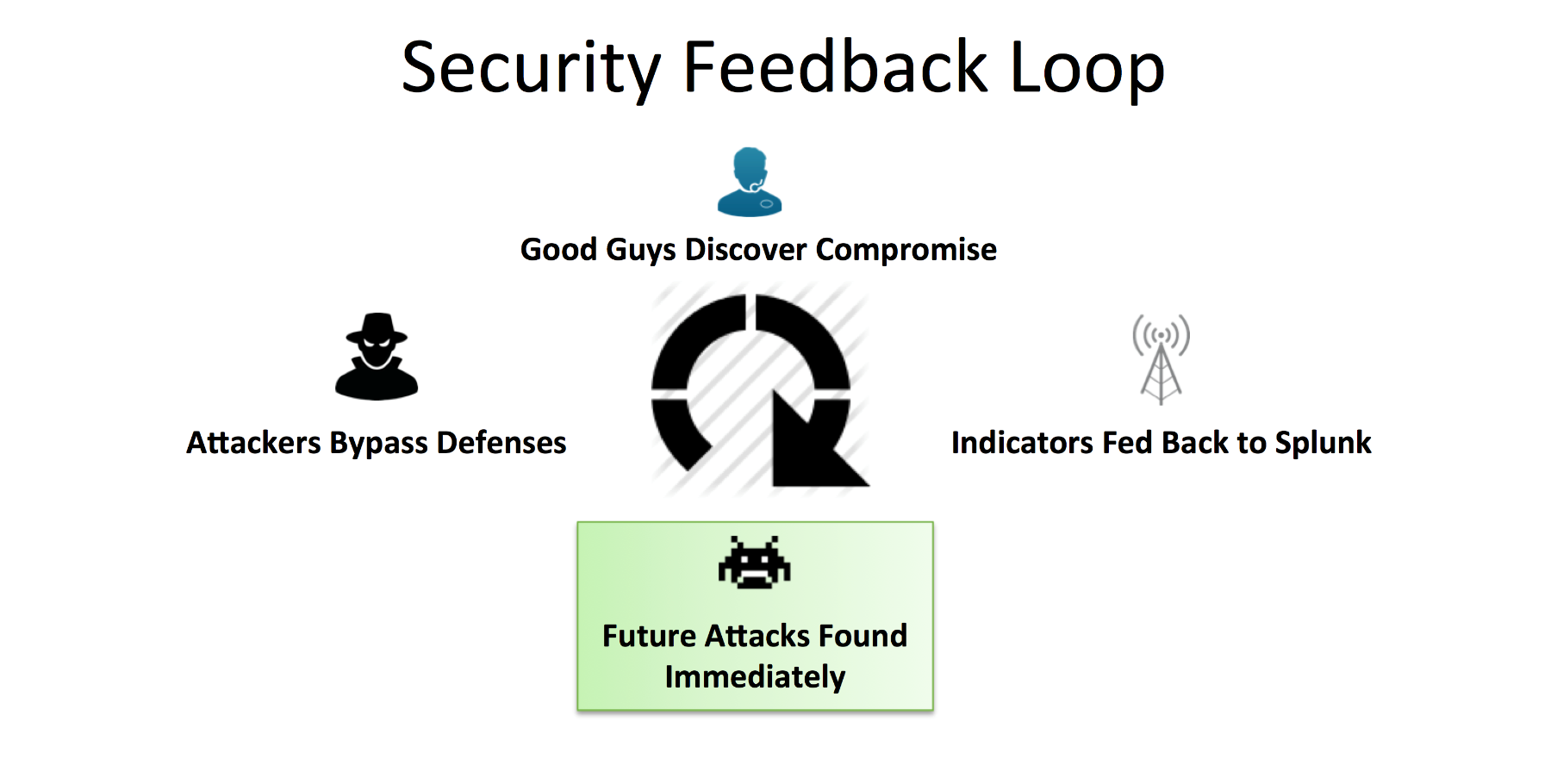
The threat activity is shown over the last 24 hours with the threat collection shown below.



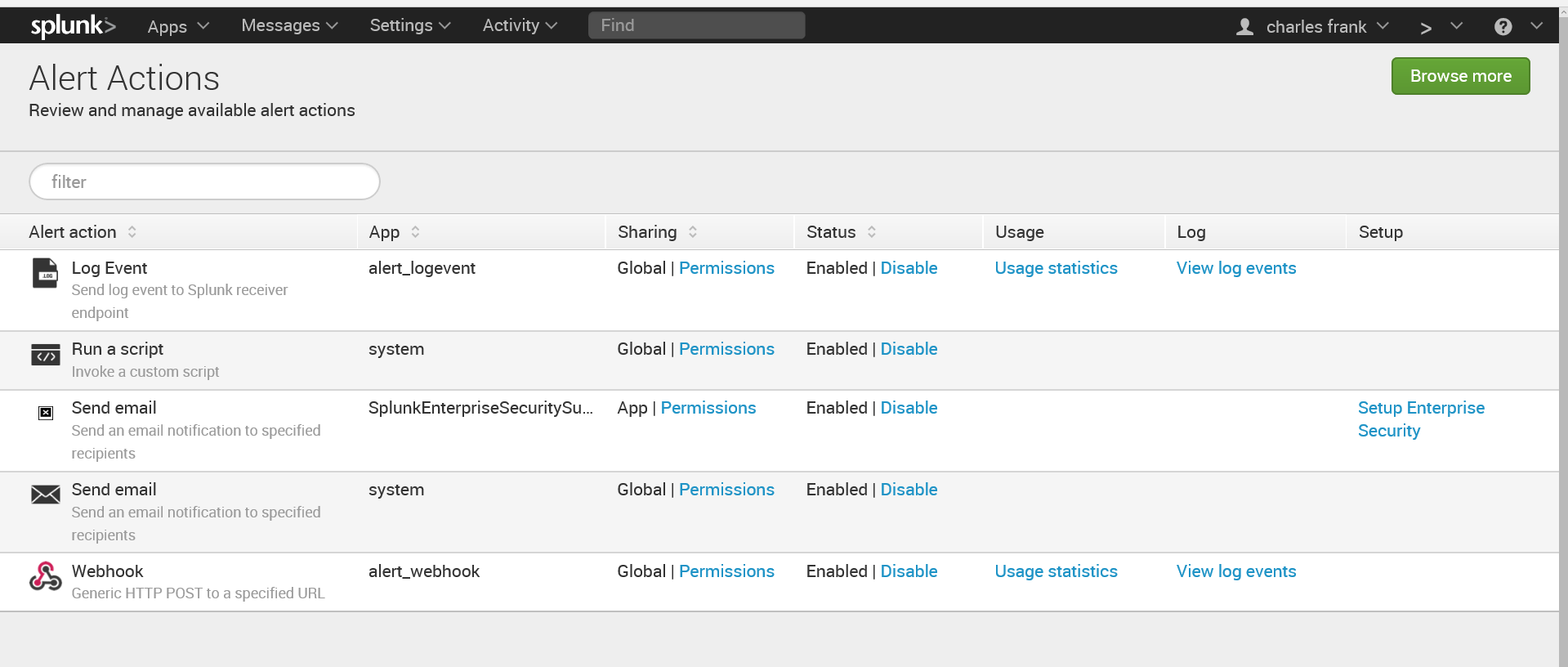
Drilling down into the threat, you get the event information as well as a graph in the upper right hand corner to convey the threat activity.

At this point, I am convinced that SPLUNK provides a high level of visibility. It seems wherever you go in SPLUNK you are provided information and charts and then you drill down even further for more details.

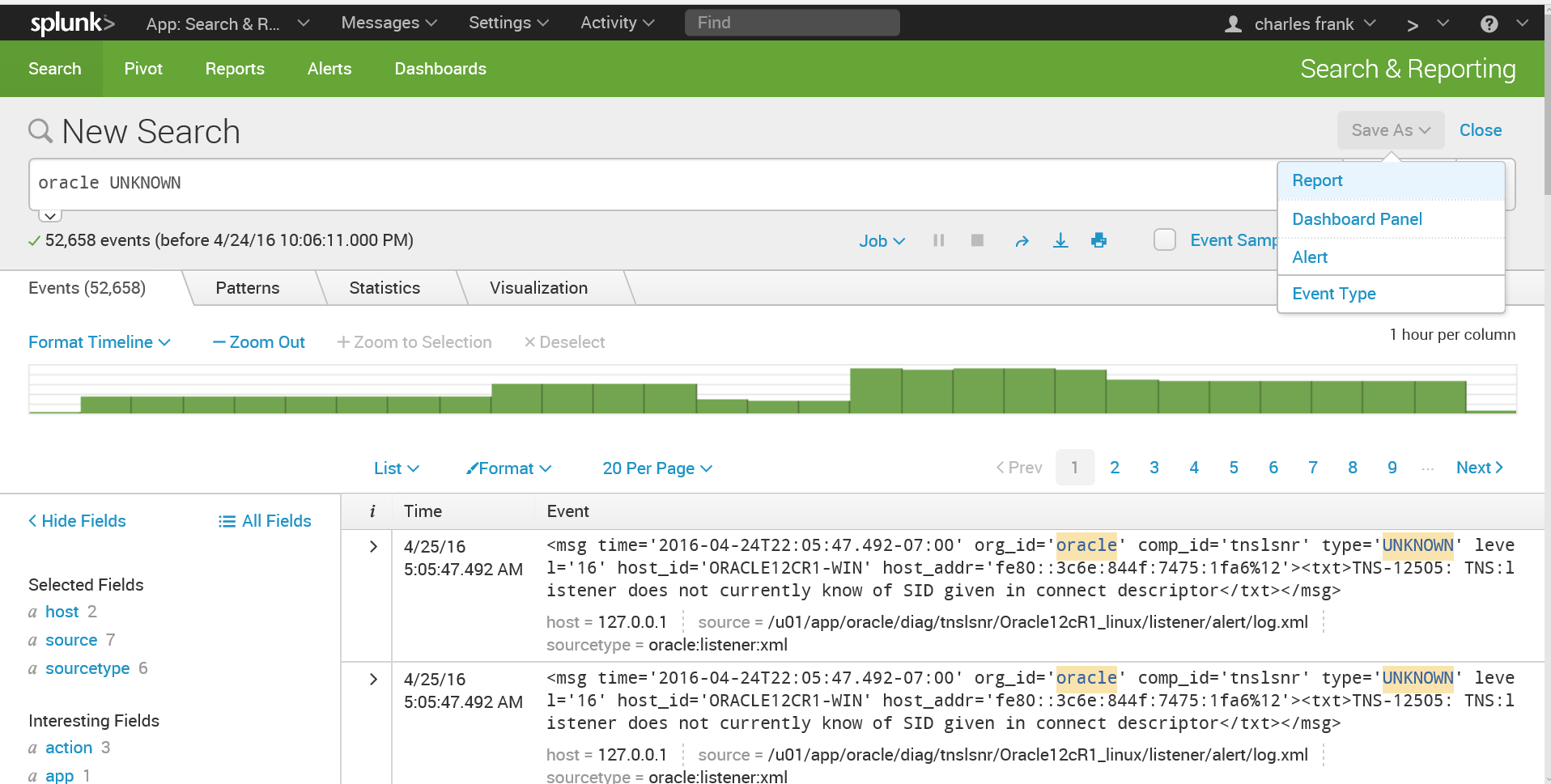
## PREVENT THREATS



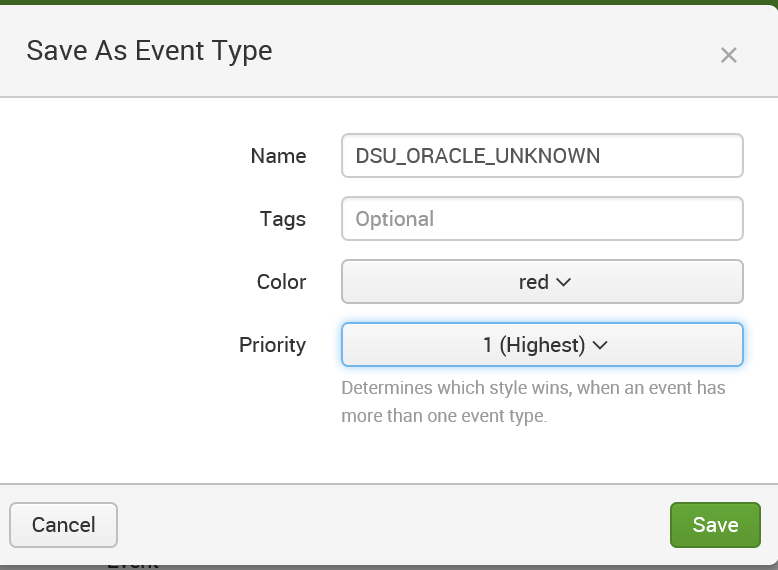
Taken from the ZEUS demo in SPLUNK, indicators get sent to SPLUNK and then SPLUNK will search its “big data” repository to identify the attack.



SPLUNK contains Alert Actions. Based upon an alert, a certain action can be taken. For example, a script could be executed, an email sent …

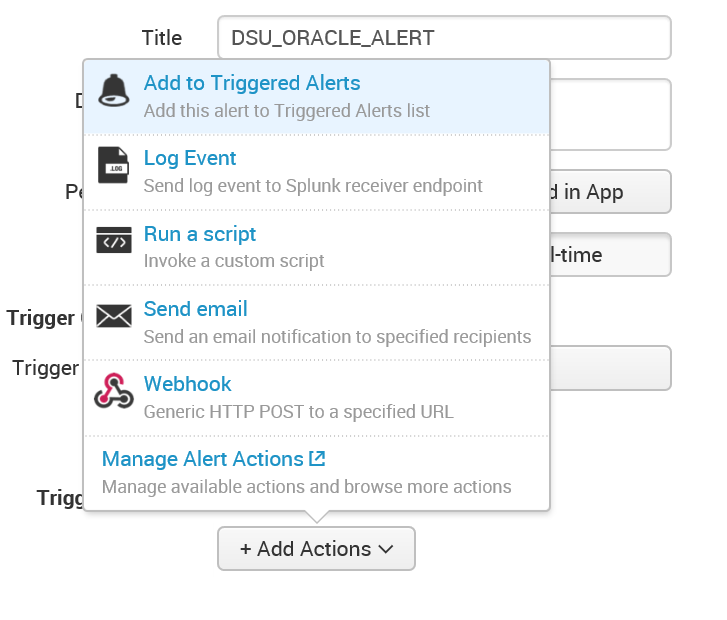


Creating a simple search for UNKNOWN Oracle events. And, I can save the search as a Report. Dashboard Panel, Alert, and Event Type.

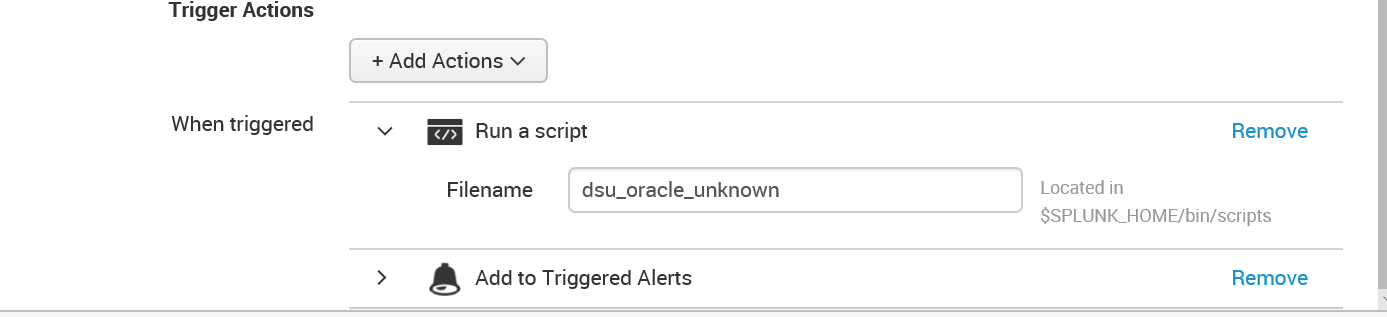


Save as an event type.



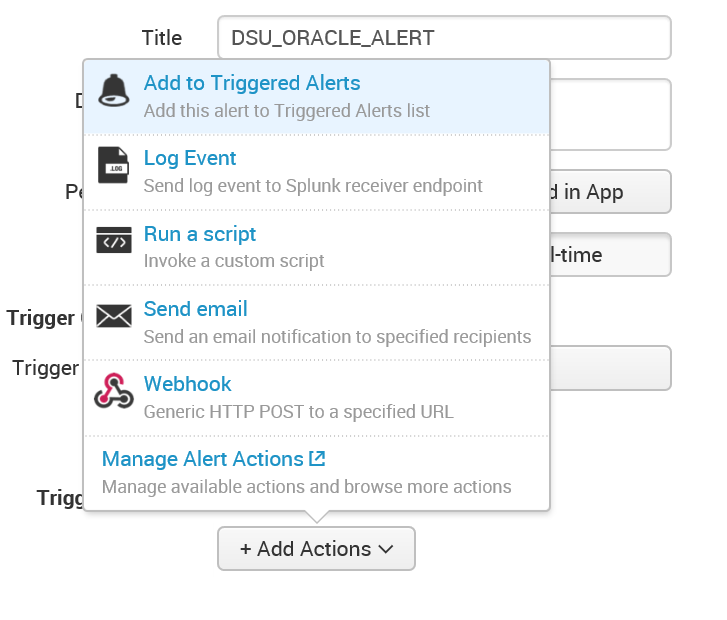
Creating the Real Time Alert. \

Concerning Preventing Threats, this alert could be added to Triggered Alerts and Run a script could be chosen to invoke a custom script.

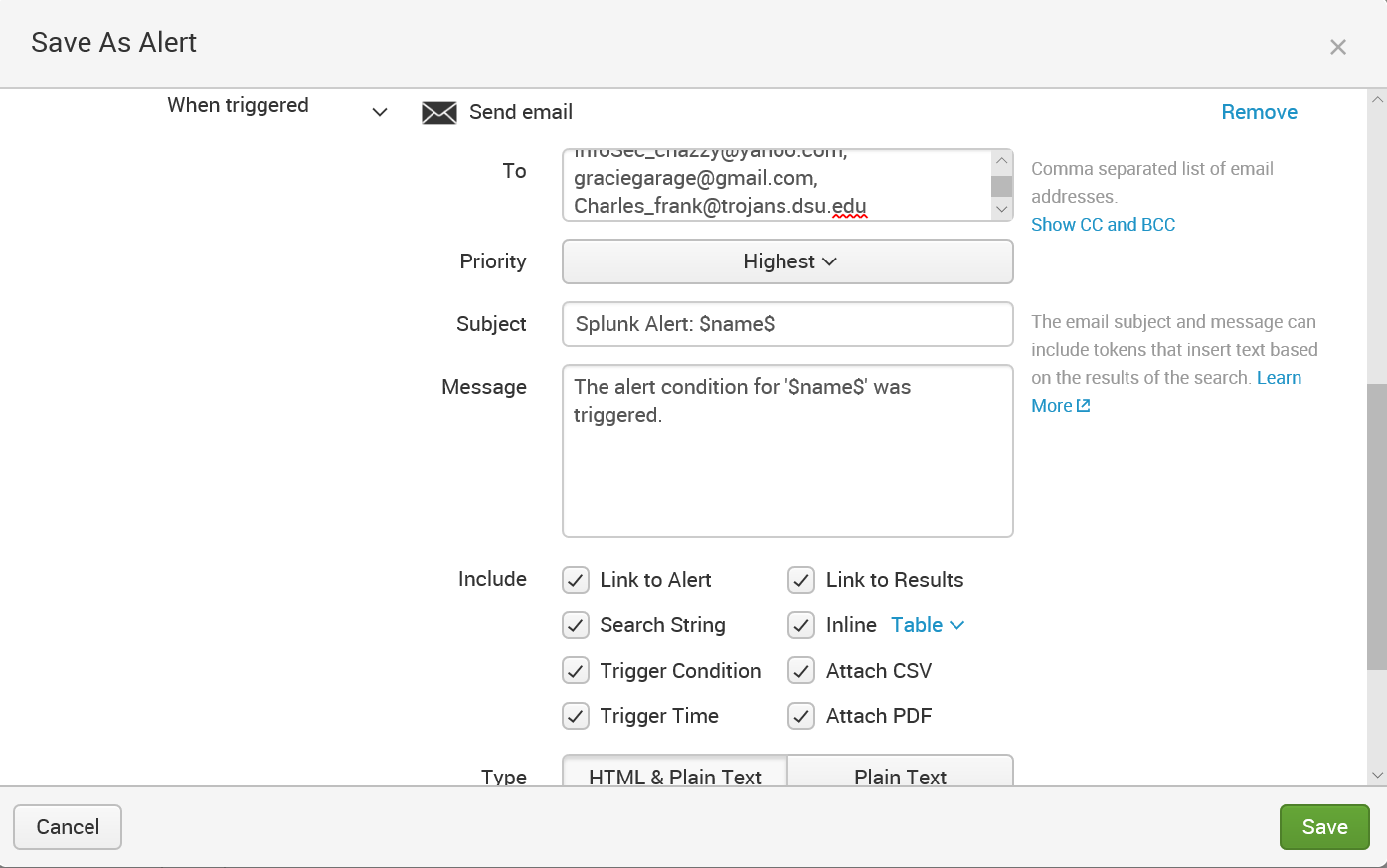


The scripts are contained in $SPLUNK\_HOME/bin/scripts and are written in PYTHON. For this evaluation cloud version, I do not have access to create custom scripts. As stated in [10], the reason for custom PYTHON scripts “you need to gather data from somewhere that doesn't have a logfile … you find that you need an extra feature within the search language that doesn't exist already”.

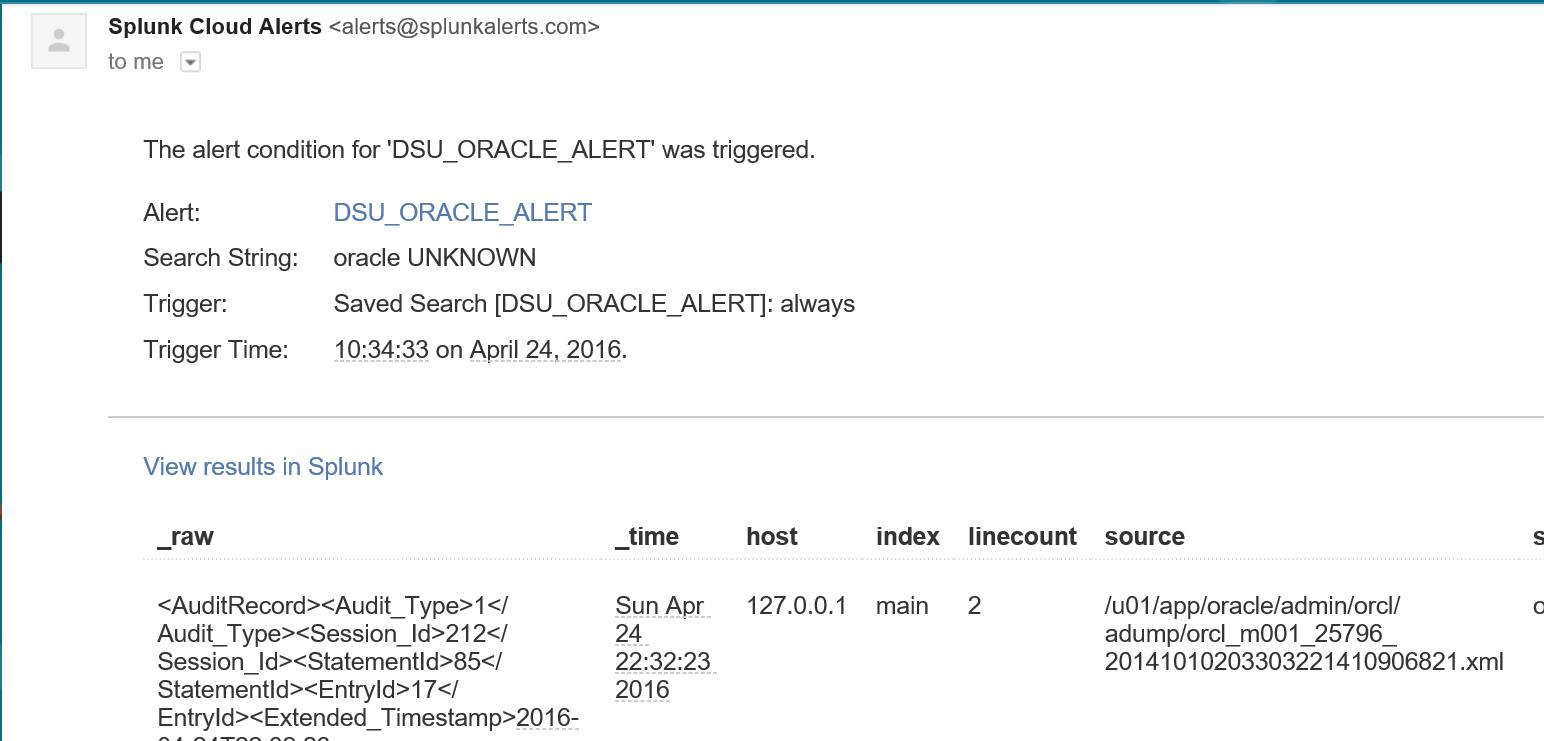
## RESPONSE CAPABILITIES



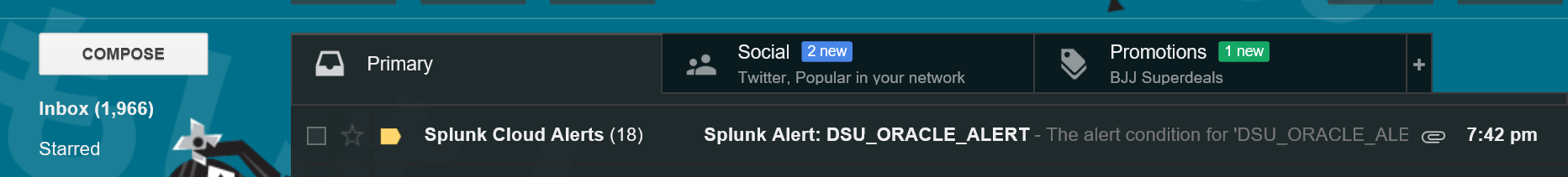
Sending an email is an action that can be added to the alert.



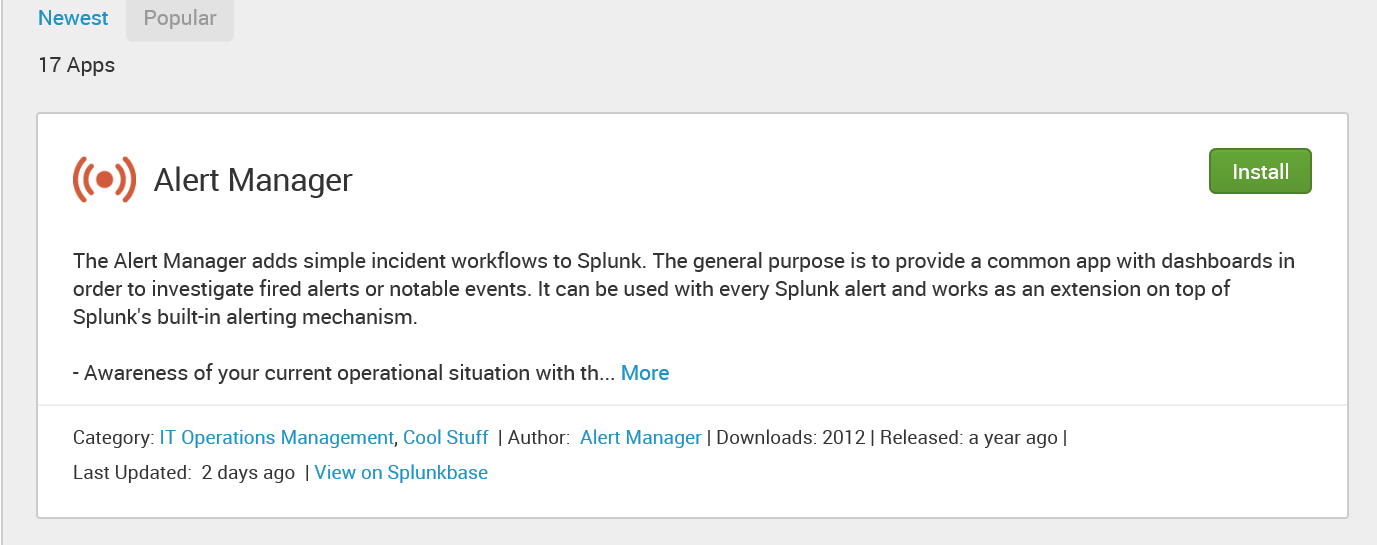
There are several options for email.



The alert went off and I did receive this email, in my GMAIL account graciegarage, about the oracle UNKNOWN error.



Actually, to date, I have received 18 Splunk Cloud Alerts for the Oracle UNKNOWN alert.



Alert Manager, an application add on, can enable workflow for incidents.

## ENDPOINT IMPACT

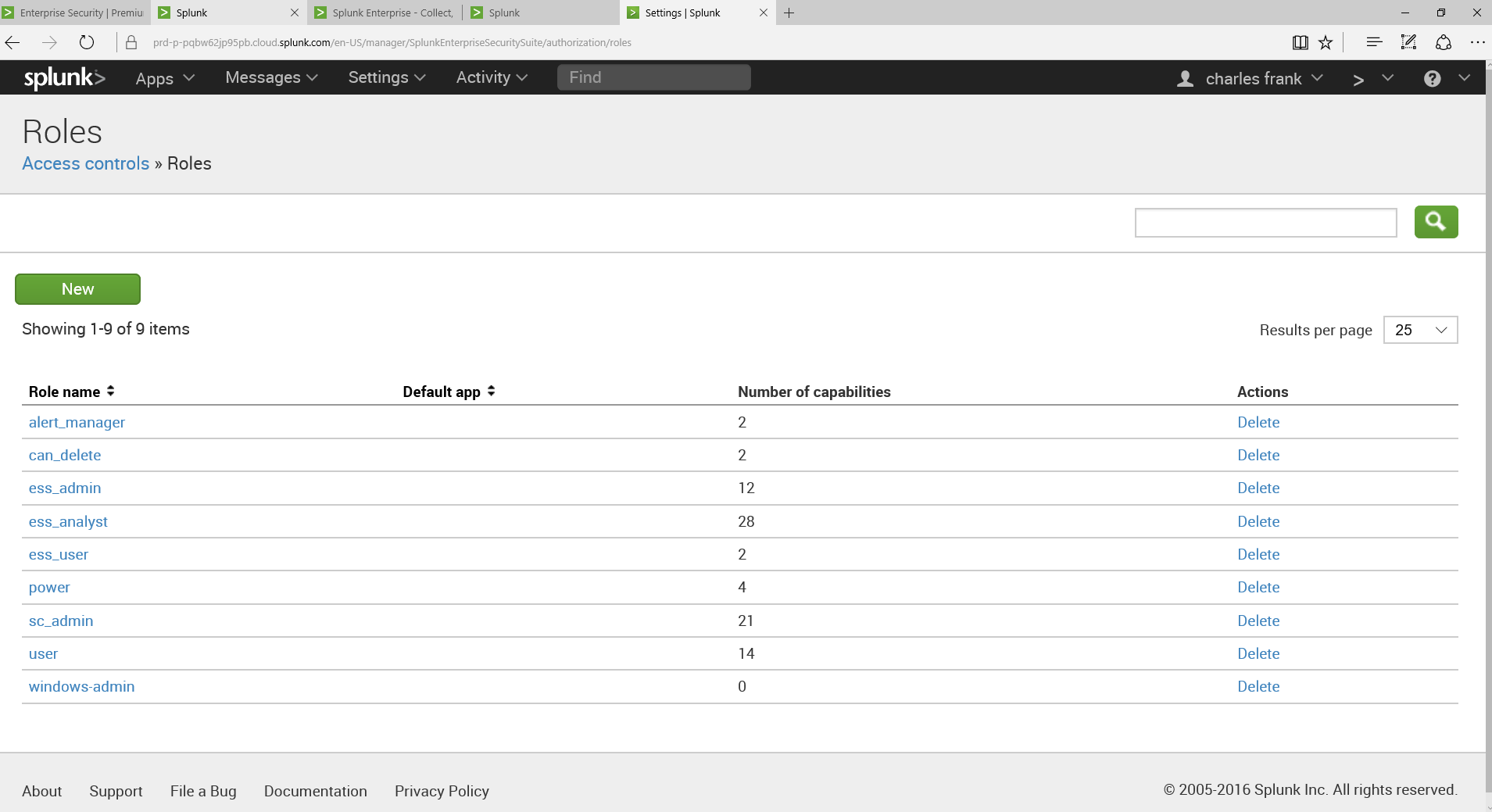
Considering that this is an Evaluation version and I focused more on the functionality of SPLUNK with lots more data available for evaluation, [11] states the following, when dealing with Endpoint Impact “Universal forwarders are centrally managed, require no configuration and are transparent to endpoint operations. Large Splunk customers deploy thousands of universal forwarders to gather data from servers, applications, employee endpoints and any Windows or Unix-based system regardless of location.

Universal forwarders:

* Forward data from remote systems securely in real time
* Have minimal resource overhead and impact on endpoint performance
* Support thousands of machine data formats
* Provide many features such as SSL, compression and buffering “

SPLUNK contains features that trigger alerts, send emails, and there is a workflow add on that can be purchased. Also, there are many dashboards, which I have not shown. With these feature, individuals and teams should be aware of any events alerted on.

## SECURITY CONTROLS

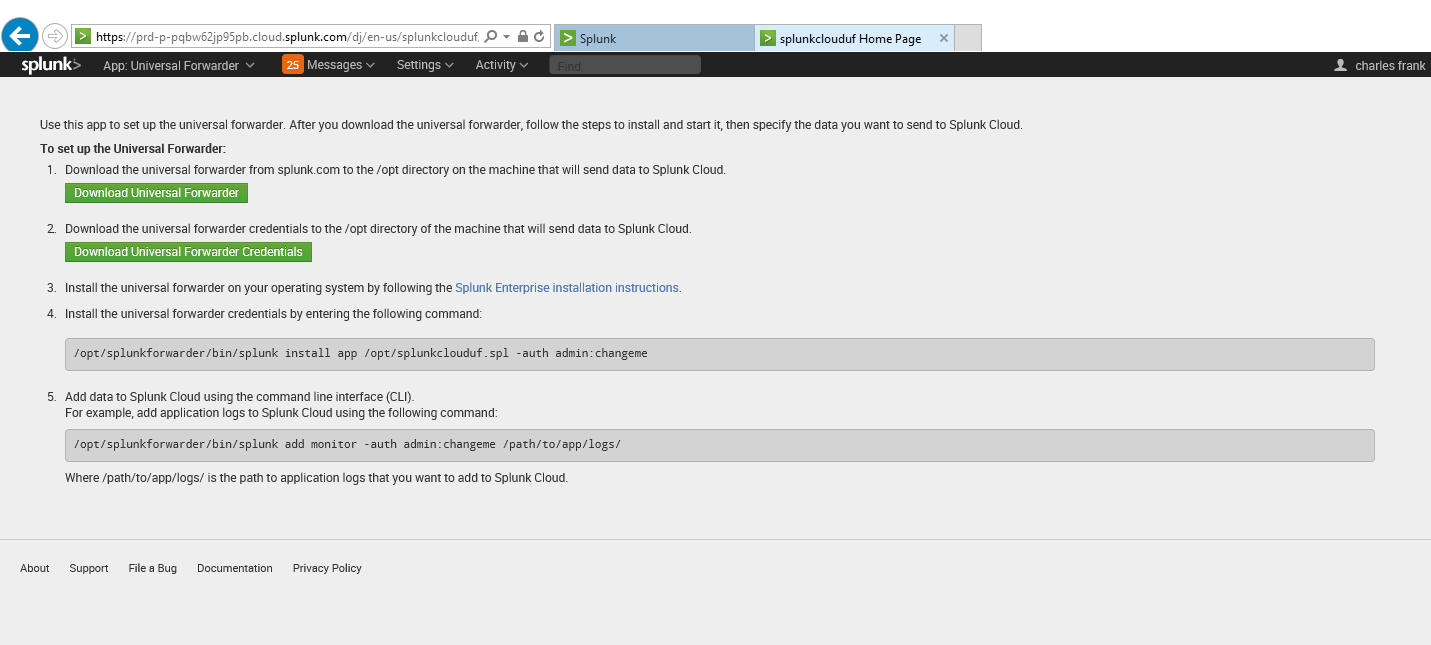


SPLUNK contains RBAC (Role Based Access Control), to assign authorizations to users of SPLUNK. And, the Forwarder, SPLUNK client on each server, forwards data in a secure manner such as using SSL. The installation of the forwarder is described by [12]:

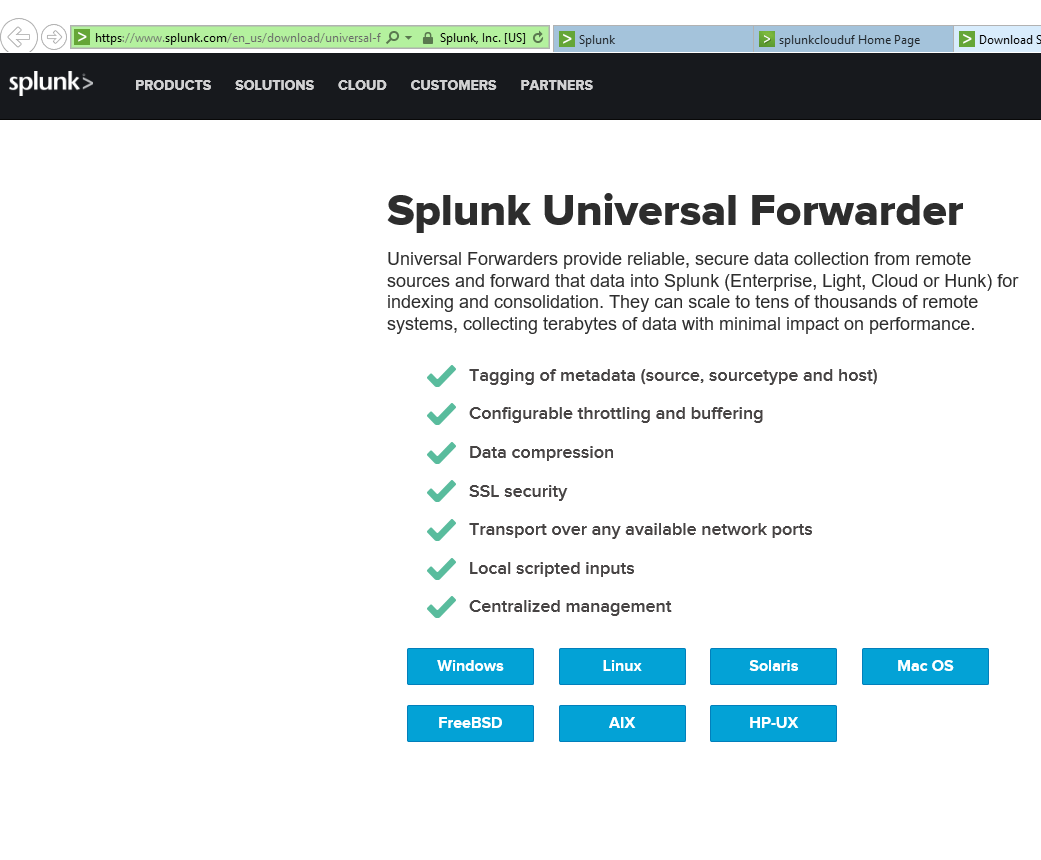
* Create and configure security groups with the user you want the universal forwarder to run as
* Optionally, configure the universal forwarder account as a managed service account.
* Create and configure Group Policy objects for security policy and user rights assignment.
* Assign appropriate user rights to the GPO.
* Deploy the GPO(s) with the updated settings to the appropriate objects.

Clearly, if the forwarder runs on windows, then then basic windows security is needed. Basic OS (Operating System) security is implemented to secure the forwarder. And, it is clearly evident, the forwarder must be available in order for SPLUNK to receive the information it needs to detect events.

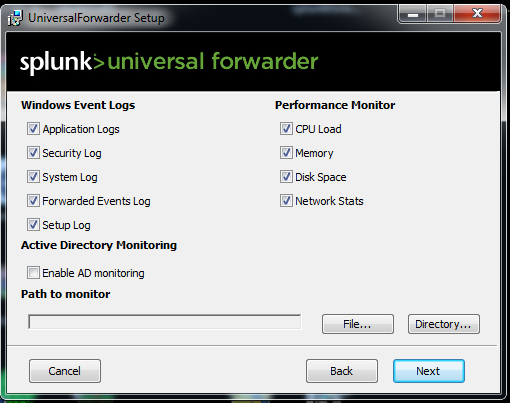
# SYSMON AND SPLUNK INTEGRATION



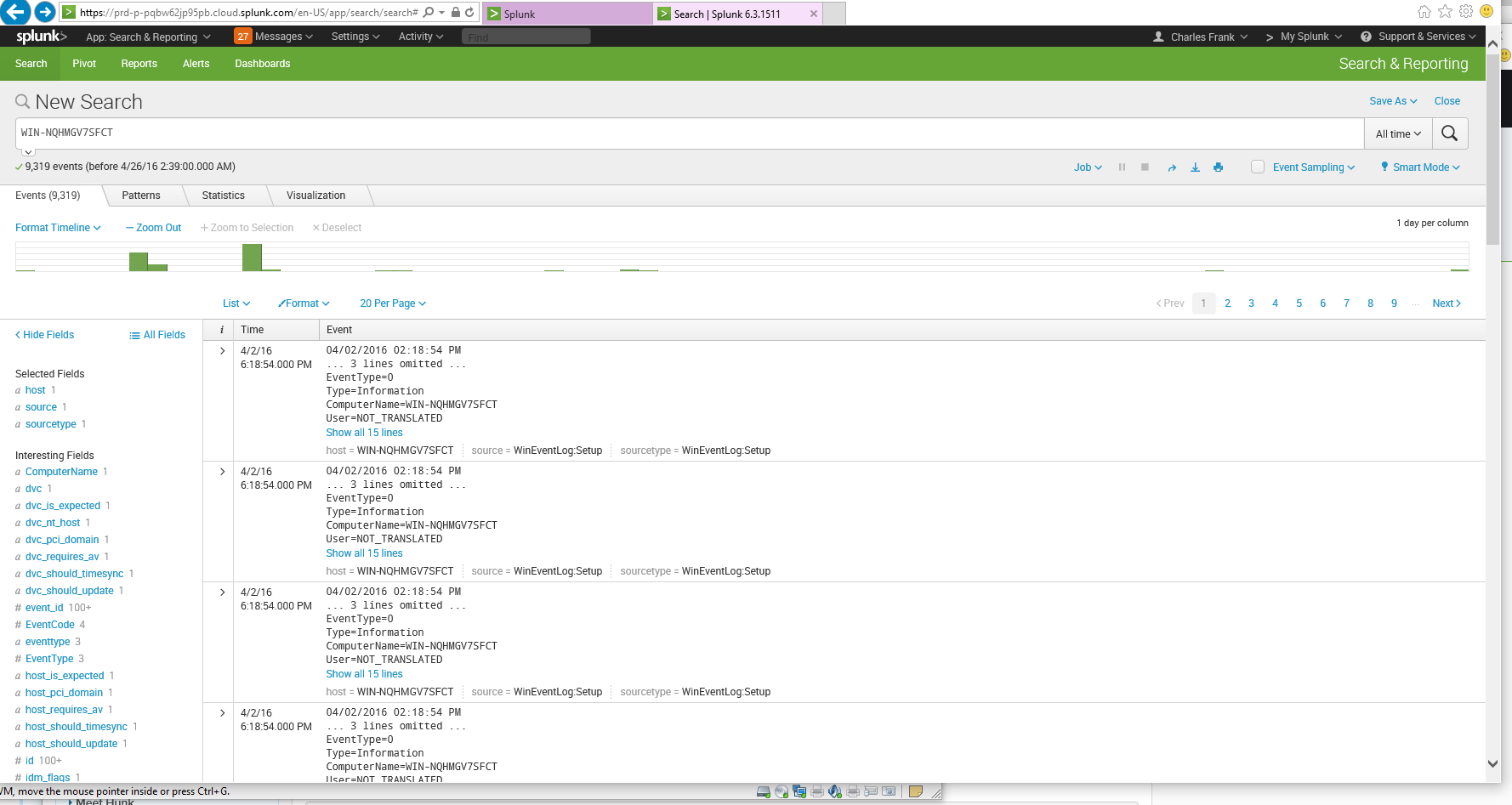
The above directions will be followed to install the forwarder in the VM, mentioned previously, where SYSMON is running.



The forwarder runs on many platforms.

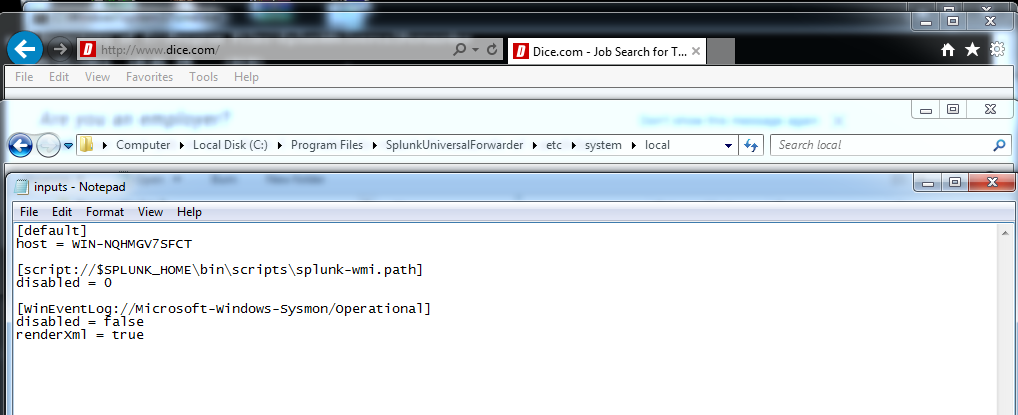


I hope to get the SYSMON Events with choosing all of these options.

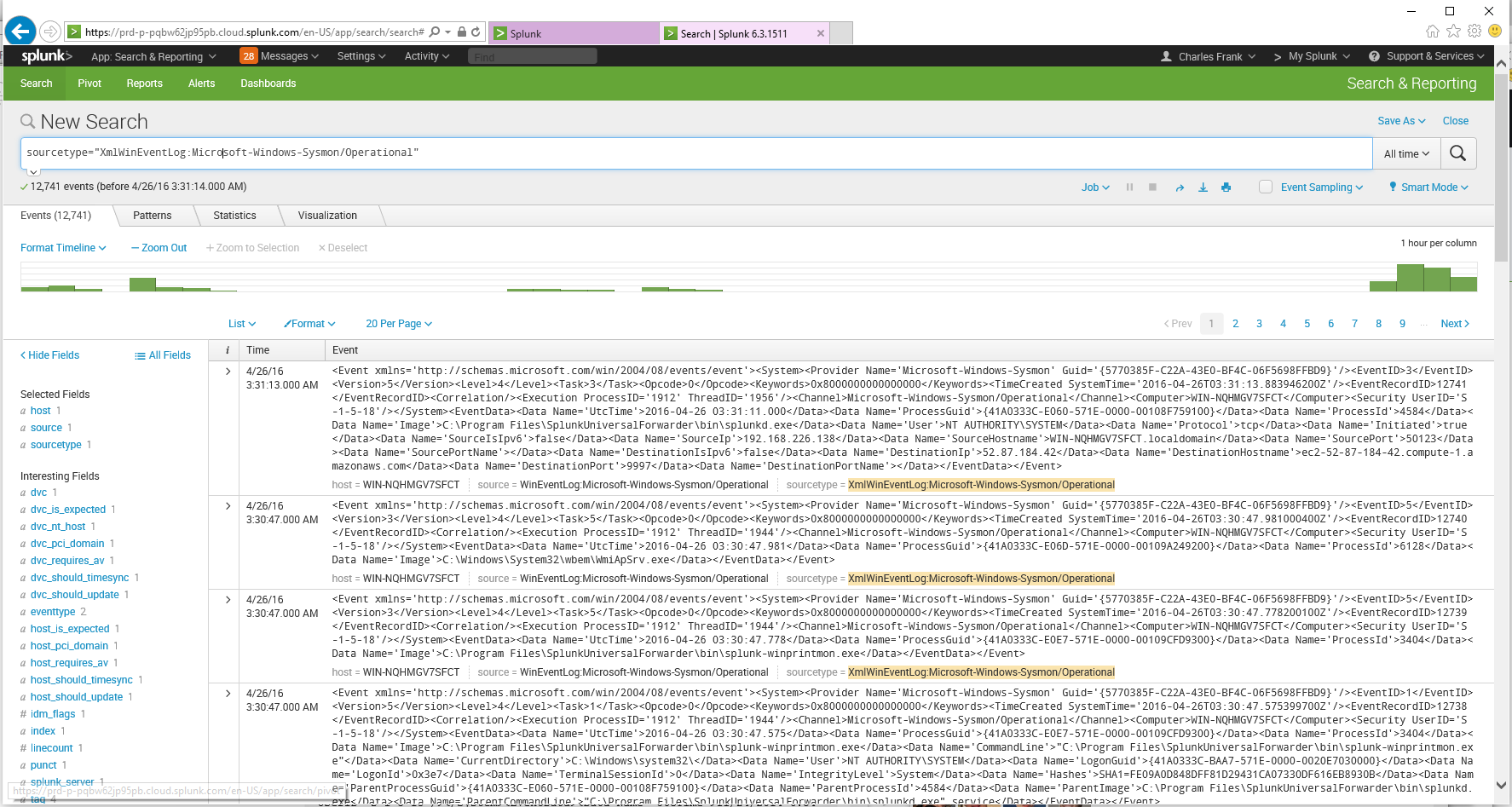


I searched for my VM name and now I see events. I wonder if I can just search for SYSMON recorded events?

## SPECIAL CONFIG FOR SYSMON



According to [13], I made the above inputs.conf change to monitor SYSMON Win Events.



Searching for [sourcetype="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational"], I noow can find my SYSMON events. Now, compared to just SYSMON event viewer, I can search thru the SYSMON events much easier with SPLUNK. More importantly, I can establish an alert for SYSMON events.

## TESLA

I am curious to execute the TESLA CRYPT MALWARE we have been studying in previous labs, to determine the effectiveness of this, SYSMON and SPLUNK, EDR integration to detect malicious activity. I am curious to see what can be determined from the SYSMON event logging and how SPLUNK can be utilized to detect and respond to, via an SPLUNK alert, the TESLA malware.

# REFERENCES

[1] http://www.cybersecuritydocket.com/2015/10/16/edr-tool-review-carbon-black/

[2] https://technet.microsoft.com/en-us/sysinternals/sysmon

[3] http://blogs.splunk.com/2014/11/24/monitoring-network-traffic-with-sysmon-and-splunk/

[4] https://www.microsoft.com/en-us/server-cloud/products/advanced-threat-analytics/overview.aspx#Fragment\_Scenario5

[5] https://www.microsoft.com/security/portal/threat/encyclopedia/entry.aspx?Name=Trojan%3AWin32%2FSysmon

[6] https://en.wikipedia.org/wiki/OSSEC

[7] http://www.crowdstrike.com/blog/sysmon-2/

[8] http://windowsitpro.com/security/q-what-windows-platforms-support-windows-event-forwarding-and-collection

[9] https://www.splunk.com/en\_us/solutions/solution-areas/security-and-fraud.html

[10] https://answers.splunk.com/answers/25658/whats-the-point-of-custom-python-scripts.html

[11] http://www.splunk.com/en\_us/products/splunk-enterprise/features/forwarders.html

[12] http://docs.splunk.com/Documentation/Splunk/6.0.6/Forwarding/DeployaWindowsdfmanually

[13]

http://blogs.splunk.com/2014/11/24/monitoring-network-traffic-with-sysmon-and-splunk/