
MaxProd Technologies
&
Maendeleolab
Presents
OPERATIONALIZE
YOUR SIEM SKILLS w/ SPLUNK
APR 3 2021
Free Event | Hands-On Experience

Meet the Instructor – Marcus Bowie

- Founder of MaxProd Technologies
- Co-Founder of MARJUN, LLC
- Cyber Security Engineer | Department of Energy
- CEH, AccessData Examiner, ITILv3
- 12+ years of exp in Information Technology
- Supported Cyber Operations @ Department of State, DHS CBP, Department of Energy

MAXPROD TECHNOLOGIES

Objectives:

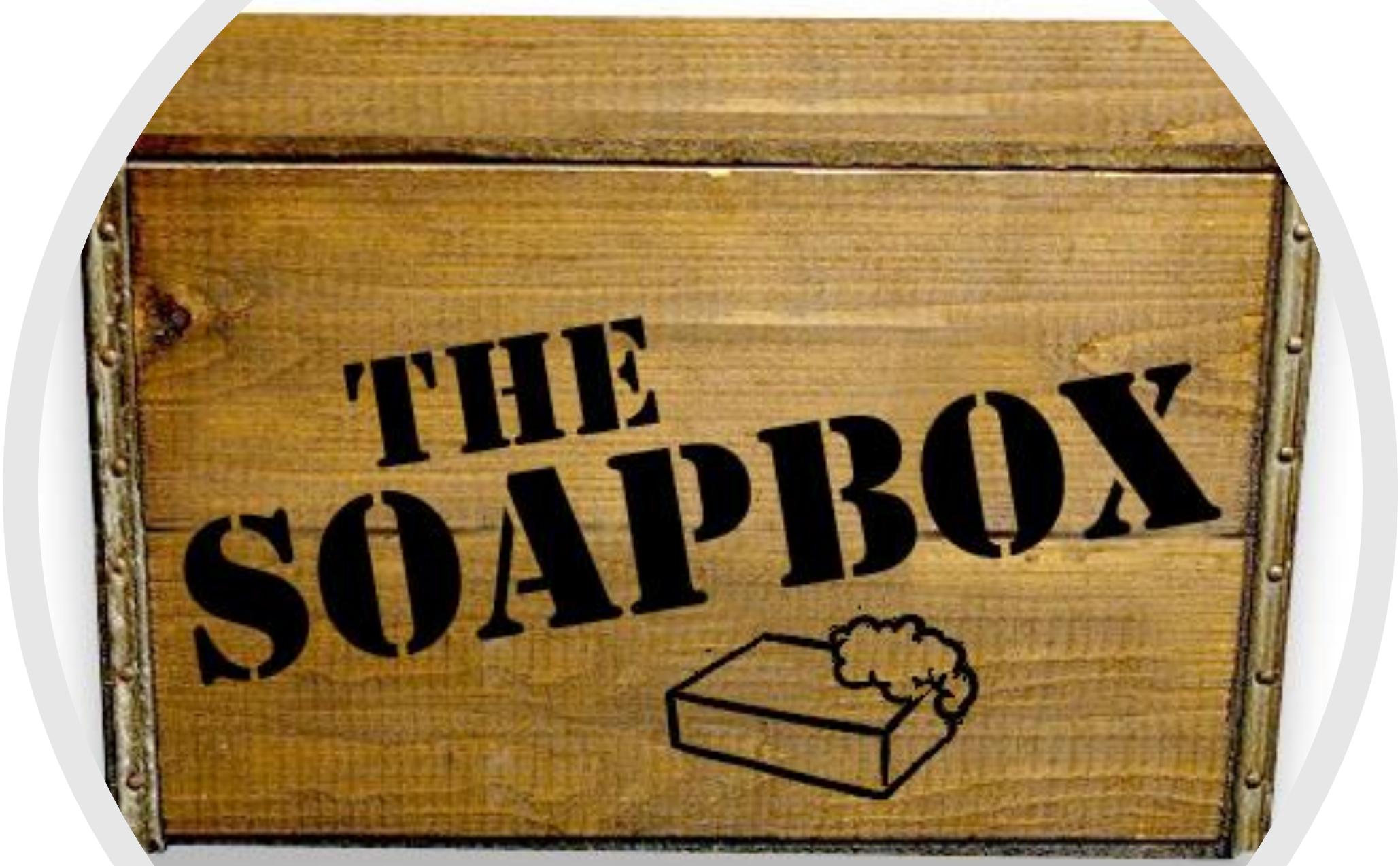
- Show you some ways to monitor the network
- Show you some ways to monitor the endpoint
- Show you some ways to perform threat hunting
- Show you some ways on how to investigate an incident

MAXPROD TECHNOLOGIES

RULES

MAXPROD TECHNOLOGIES

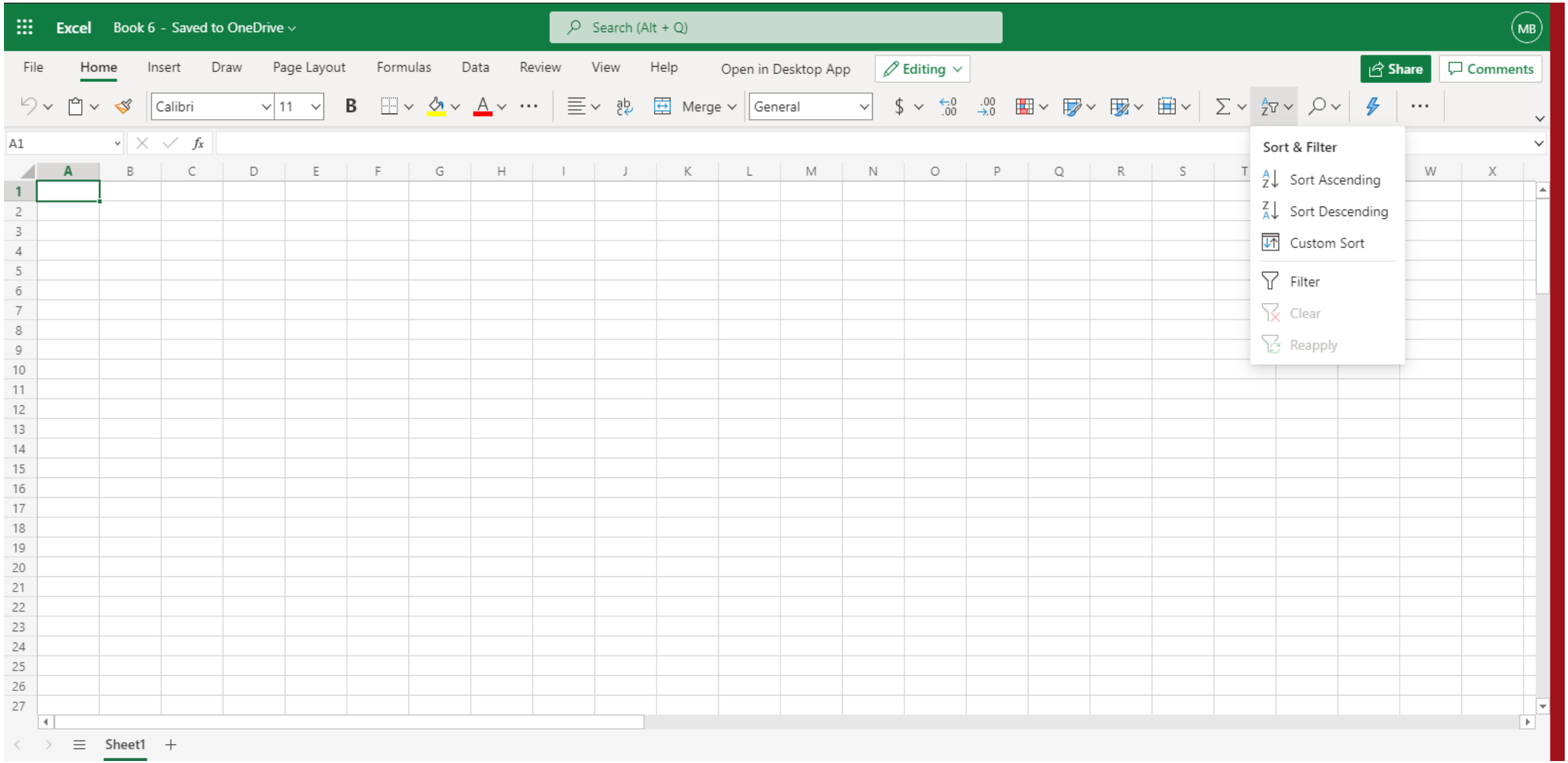
This Photo by Unknown author is licensed under CC BY-SA.


THE
SOAPBOX

WHAT IS SPLUNK?

- SIEM – Security Incident Event Management system
- Used to ingest an organization's data and view it in a single pane of glass

MAXPROD TECHNOLOGIES


Excel
Book 6 - Saved to OneDrive
Search (Alt + Q)
MB
File
Home
Insert
Draw
Page Layout
Formulas
Data
Review
View
Help
Open in Desktop App
Editing
Share
Comments
Calibri
11
Merge
General
A1
Sort & Filter
Sort Ascending
Sort Descending
Custom Sort
Filter
Clear
Reapply
Sheet1

5 Main Functions of Splunk:

- Index data
- Search and investigate events/incidents
- Add knowledge/data
- Monitor and alert events/incidents
- Report and analyze data/events/incidents

MAXPROD TECHNOLOGIES

Tier 1 SOC Analyst's Role:

- Search and investigate events/incidents
- Monitor and alert events/incidents
- Report and analyze data/events/incidents

MAXPROD TECHNOLOGIES

5 Components to (SPL) Splunk Language:

- **Search Terms**
  - field_name="value" or value
- **Command**
  - Creating charts, Compute statistics, Formatting
- **Functions**
  - How we want to chart, compute and valuate the results
- **Arguments**
  - Variables that we want to apply to the function
- **Clauses**
  - How we want the results grouped or defined

Splunk Fields & Interesting Fields:

- Field names are **case-sensitive**
- Values are **NOT** case-sensitive
- If you see 'a' next to the field name, the values are strings
- If you see '#' next to the field name, the values are numbers
- **ONLY** select the interesting fields that are of upmost importance to put into the search bar **(I.e. Excel Spreadsheet columns/filter button)**
- **The more defined your search is, the better the results.**

3 Search Modes:

- Fast – Disabled by default. Only returns back what's essential
- Smart - ***Default mode***. It toggles behavior based on the type of search being run
- Verbose – Returns everything

MAXPROD TECHNOLOGIES

Splunk Search Color System:

- Boolean Operators and Command Modifiers = **Orange**
  - **AND, OR, NOT, by, as**
- Commands = **Blue**
  - **table, stats, top, rare**
- Arguments = **Green**
  - **earliest, latest**
- Functions = **Purple**
  - **count, values**

Dark Theme?
Username > Preferences > SPL Editor > Themes > Dark Theme

CyberReverend's Splunk Term Legend:

index - (TextBook)

- Multiple **sourcetypes** (Chapters)
- Multiple **channels** (Topics)
- Multiple **sources** (Authors)
  - Where it's coming from

"*" = "Wildcard"

| = "Pipe"

- Shift + the key above or around the enter/return key

3 Splunk Roles:

- **Administrator** - Can install apps, and create knowledge objects for all users.
- **Power** - Can create and share knowledge objects for users of an app and do real-time searches
- **User** - Will only see their own knowledge objects and those shared with them.

MAXPROD TECHNOLOGIES

Using Splunk:

- In order to use the boss of the SOC dataset enter the following command:

- index="botsv2" **earliest=**0

MAXPROD TECHNOLOGIES

Difference between Event and Incident:

- **Event** - Normal, expected, or planned activity
- **Incident** – An event or abnormal activity that requires an investigation

MAXPROD TECHNOLOGIES

Incidents of Interest:

- Malicious Logic
- Phishing
- Misuse
- Unauthorized Access
- Suspicious Network Activity
- And many more....

MAXPROD TECHNOLOGIES

Monitoring =
Know Your Environment:

Log Sources

- What type of logs(data) are being collected and ingested into Splunk?

Network Range

- What am I defending?

IDS/IPS
AV Solution

- What are my alarm systems in my network?

Firewall

- Who's coming in & out of my house?
- What's going on at my perimeter?

Log Sources

MAXPROD TECHNOLOGIES

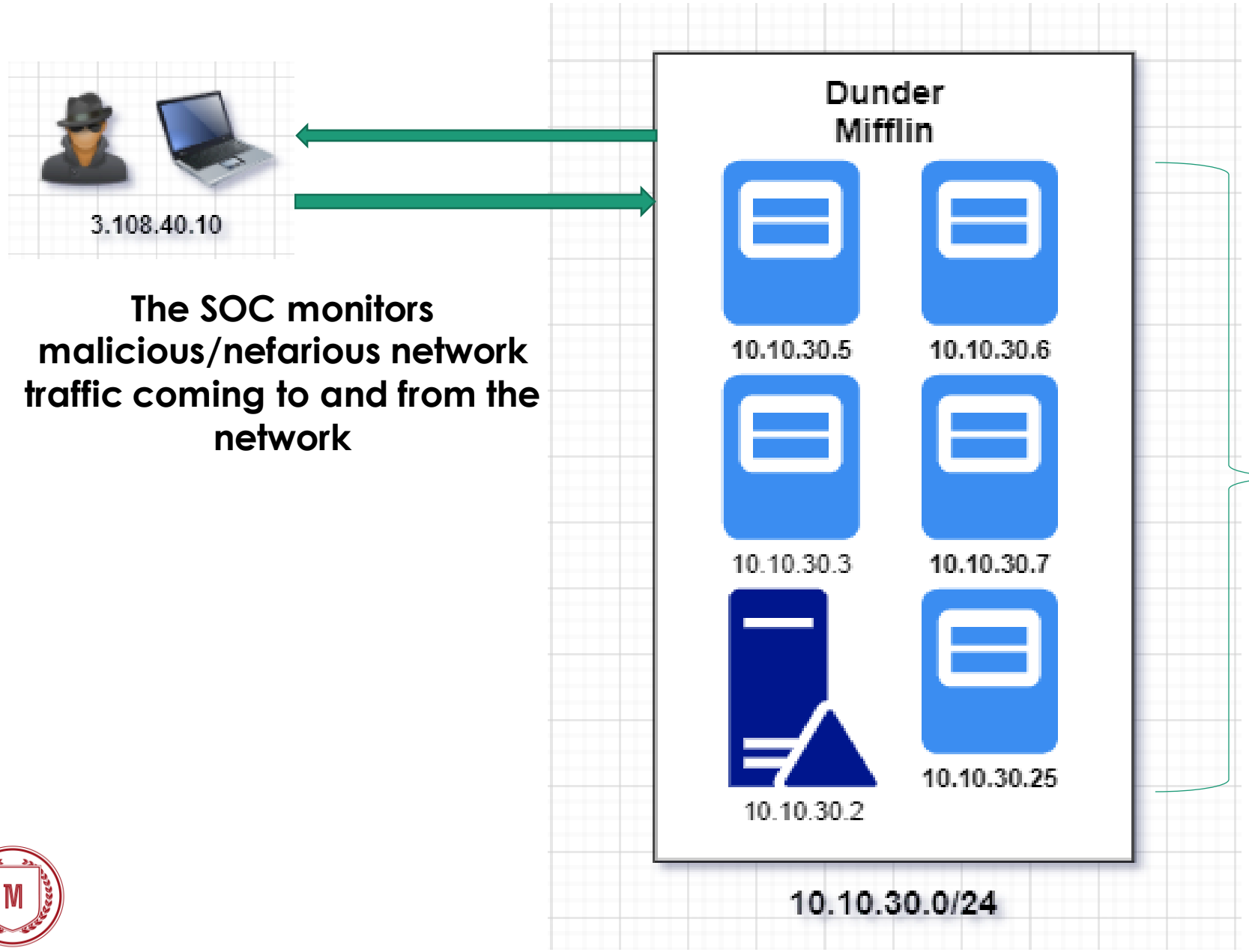
Log Sources Splunk Search:

```
index="*" sourcetype="*"
| stats count by index,sourcetype
```

MAXPROD TECHNOLOGIES

Network Range

MAXPROD TECHNOLOGIES



The SOC monitors malicious/nefarious network traffic coming to and from the network

The SOC monitors malicious/nefarious endpoint activity going on inside of the network

Network Range Splunk Searches

Workstations:

```
index="*" sourcetype="wineventlog"  Workstation_Name="*" Source_Network_Address="*"
```

Computers:

```
index="*" sourcetype="wineventlog"  ComputerName="*"
```

Users:

```
index="*" sourcetype="wineventlog"   ComputerName="*" Security_ID="*"|  stats count by Security_ID
```

User Login Windows Workstation Activity:

```
index="*" sourcetype="wineventlog"  EventCode="4624" ComputerName="*" Security_ID="*"  | stats values(ComputerName)  by Security_ID
```

Network Range Splunk Searches

User Failed Login Attempts Windows Workstation Activity:

```
index="botsv2" earliest=0 index="*" sourcetype="*" EventCode="4625" Failure_Reason="Unknown user name or bad password." | stats count by Account_Name,ComputerName
```

Network Domain:

```
index="botsv2" earliest=0 index="*" sourcetype="*" EventCode="*" Account_Domain="*" | stats values(ComputerName) by Account_Domain
```

Failed Login on Linux Hosts

```
index="botsv2" earliest=0 index="*" sourcetype="*"  sourcetype=linux_audit  res=failed
```

AV Solution

MAXPROD TECHNOLOGIES

Symantec

A security software suite that consists of anti-malware, intrusion prevention and firewall features for server and desktop computers.

Symantec Splunk Search

```
Index="*" sourcetype="symantec:ep:security:file"
| stats count by signature
```

IDS/IPS

MAXPROD TECHNOLOGIES

Suricata

an open source network threat detection engine that provides capabilities including intrusion detection (IDS), intrusion prevention (IPS) and network security monitoring. It does extremely well with deep packet inspection and pattern matching which makes it incredibly useful for threat and attack detection.

Suricata Splunk Search

```
index="*" sourcetype="suricata" "alert.signature"="*"
| stats count by alert.signature
```

Firewall

MAXPROD TECHNOLOGIES

Palo Alto

A firewall is a network security device that grants or rejects network access to traffic flows between an untrusted zone and a trusted zone

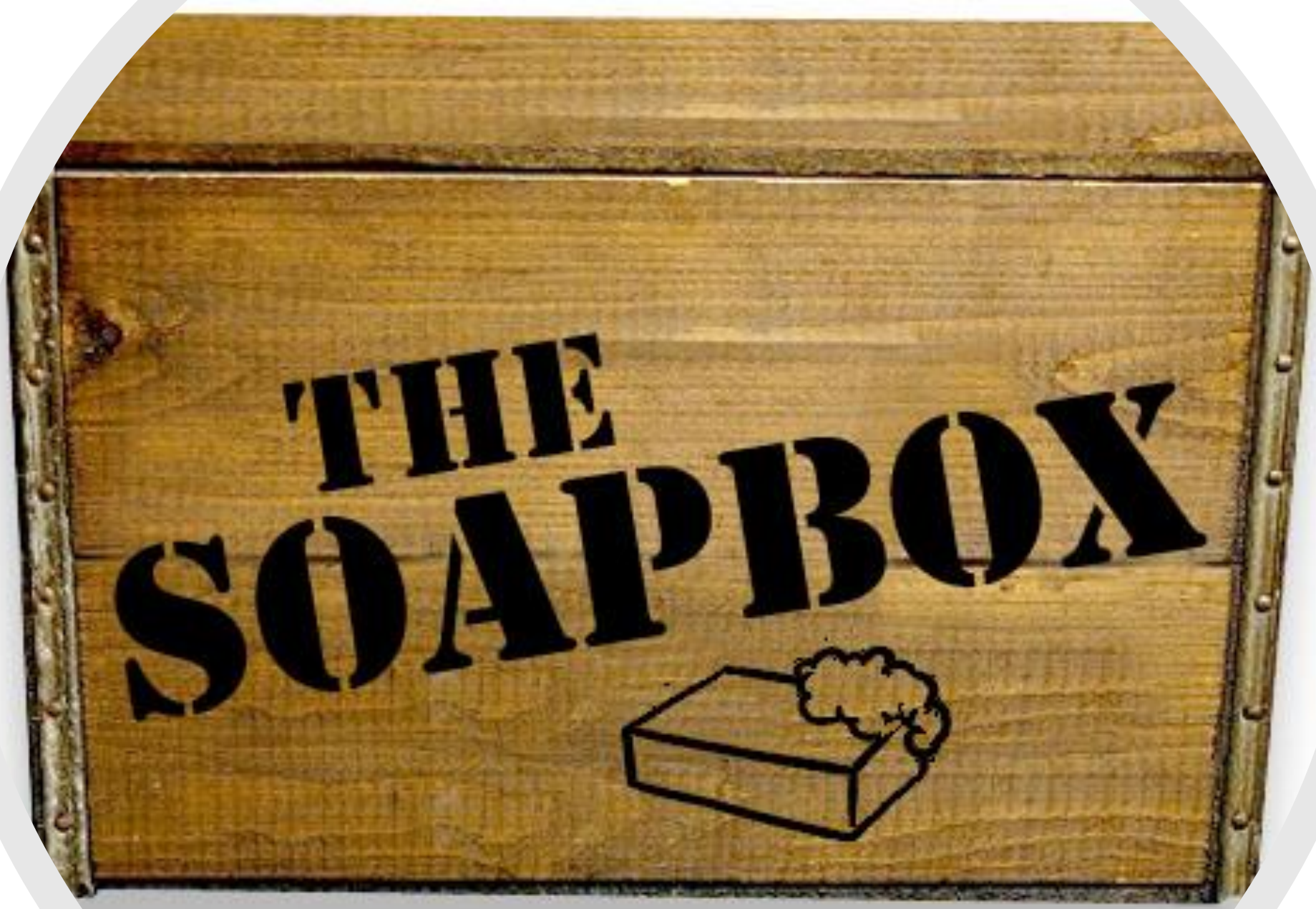
Palo Alto Splunk Search

```
index="botsv2" earliest=0 index="*" sourcetype="pan:traffic"
```


HOUSTON,
WE HAVE
A PROBLEM!
APOLLO 13

Threat Hunting

MAXPROD TECHNOLOGIES


THE
SOAPBOX

Advance Persistent Threat (APT)

is a stealthy threat actor, typically a nation state or state-sponsored group, which gains unauthorized access to a computer network and remains undetected for an extended period.

MAXPROD TECHNOLOGIES

Tactics, Techniques, and Procedures (TTPs)

The different ways to perform an attack on a network.

MAXPROD TECHNOLOGIES

Live-Off-The-Land-Binaries (LOLBAS)

Operating system signed files that can perform the following:

- Execute and compile various code
- Download, upload and copy files
- Maintain persistence
- Bypass user access controls (UAC)
- Steal credentials
- Perform memory and process dumps
- Perform spyware activities
- Evade or modify various logs
- Hijacking or side-loading Dynamic Link Libraries (DLLs)

MAXPROD TECHNOLOGIES

Indicators of Compromise (IOCs)

Virus signatures and IP addresses, MD5 hashes of malware files, or URLs or domain names of botnet command and control servers. After IoCs have been identified via a process of incident response and computer forensics, they can be used for early detection of future attack attempts using intrusion detection systems and antivirus software.

Examples of an IOC (Indicator of Compromise):

- File Name(s), File Hash(es), IP Address, URL(s), Mutex(es)

Objective: If given an IOC (Indicator of Compromise), what would you do with it?

Investigation

MAXPROD TECHNOLOGIES

Malware Questions:

- What happened?
- What time did it happen?
- What host was involved?
- Who was the user involved?
- Who was the user logged into the system at the time of the incident?
- How many systems are infected?
- Where on the system is the malware located?
- Did the malware execute?
- Were there any network connections made after the malware executed?
- Did the malware drop any more files?
- Was anything exfilled from the network?

MAXPROD TECHNOLOGIES

Phishing Questions:

- What happened?
- What time did it happen?
- Who sent the email?
- How many users received the email?
- Was the email forwarded to anyone?
- Did the email contain any links or attachments?
- Did the user click on any links or attachments?
- Did anything drop on the box?
- If yes, did it execute?
- How many users has the presence of this malware?
- Were there any network connections after execution?
- How many systems are infected?
- Was anything exfilled from the network?

MAXPROD TECHNOLOGIES

Exercise

MAXPROD TECHNOLOGIES

1. A Federal law enforcement agency reports that Taedonggang often spearphishes its victims with zip files that have to be opened with a password. What is the name of the attachment sent to Frothly by a malicious Taedonggang actor?

2. The Taedonggang APT group encrypts most of their traffic with SSL. What is the "SSL Issuer" that they use for the majority of their traffic? Answer guidance: Copy the field exactly, including spaces.

3. To maintain persistence in the Frothly network, Taedonggang APT configured several Scheduled Tasks to beacon back to their C2 server. What single webpage is most contacted by these Scheduled Tasks? Answer guidance: Remove the path and type a single value with an extension. Answer example: index.php or images.html

4. What is the public IPv4 address of the server running www.brewertalk.com?

5. Amber found the executive contact information and sent him an email. What is the CEO's name? Provide the first and last name.

Summary

MAXPROD TECHNOLOGIES

What did you learn?

- https://akima.taleo.net/careersection/akimallc_cs/jobdetail.ftl?job=QIV00739&tz=GMT-05%3A00&tzname=America%2FChicago&src=JB-10064
- https://gray-tier-technologies.breezy.hr/p/7257c12c3d72
- https://dtt.taleo.net/careersection/10260/jobdetail.ftl?lang=en&job=E21NATSASCDK103-ITL4&src=JB-16801
- https://careers.leidos.com/jobs/6150658-tier-2-incident-response-night-shift?tm_job=R-00047393&tm_event=view&tm_company=2502&utm_source=Indeed

MAXPROD TECHNOLOGIES

Resume Verbiage

- Utilized SIEM to monitor, identify and investigate malicious logic, misuse, alteration/compromise of data, endpoint threat detection and incidents on the network
- Performed analysis on various log to determine events, incidents or false positives
- Created content searches for endpoint and network detection on various tools mirroring the MITRE ATT&CK Matrix

MAXPROD TECHNOLOGIES

Thank You!

MAXPROD TECHNOLOGIES

Special Thanks!!!

Wifey
Pat Bisselele
Bryan Budget
Chris Marbra