Leonard M. Estos
Cybersecurity Researcher & Technical Author
Edmonton, Alberta, Canada
2025

Project Name: **Project Splunk Installation and Sample Analyzes**

Project Overview:

This project presents a simplified yet functional **Security Operations Center (SOC)** architecture designed for home lab experimentation and learning. It simulates real-world SOC workflows using open-source tools, enabling hands-on experience with threat detection, incident response, and automation.

The **goal** is to empower aspiring SOC analysts and cybersecurity enthusiasts with a practical environment to understand how data flows through a security ecosystem from endpoint agents to centralized analysis platforms.

Resources:

1. Splunk Enterprise Website: *https://www.splunk.com/*

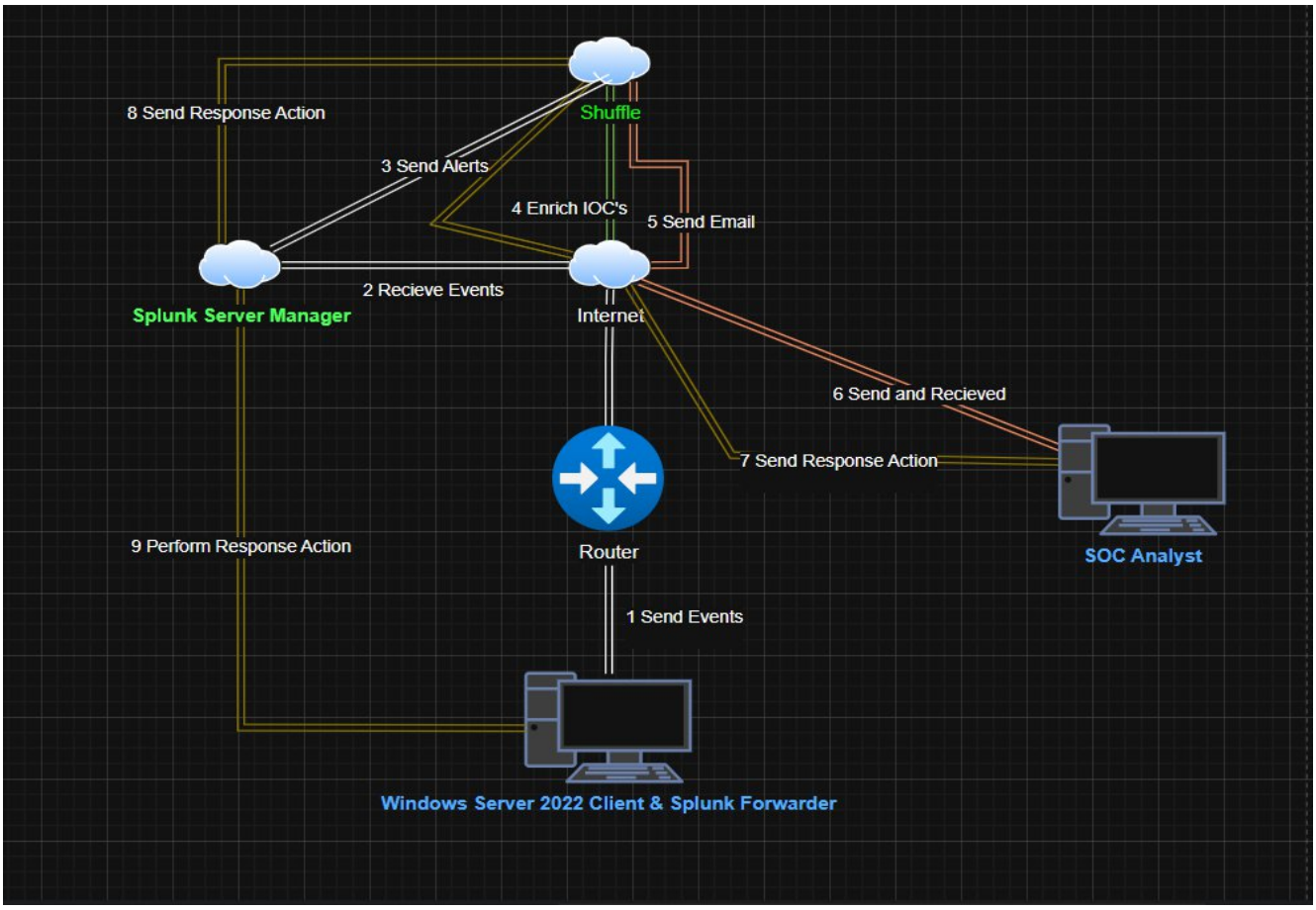
2. How to install SPLUNK in Kali Linux: https://www.youtube.com/watch?v=hJhwzGR_Y5Q

3. How to access SPLUNK in my Kali Linux: http://172.26.154.185:8000 or http://localhost:8000

4. SPLUNK 101: **IP/Traffic | DORA Process** = **Discover** message, **Offer** message, **Request** message, **Acknowledge** message = all the message has their own **Packets**.

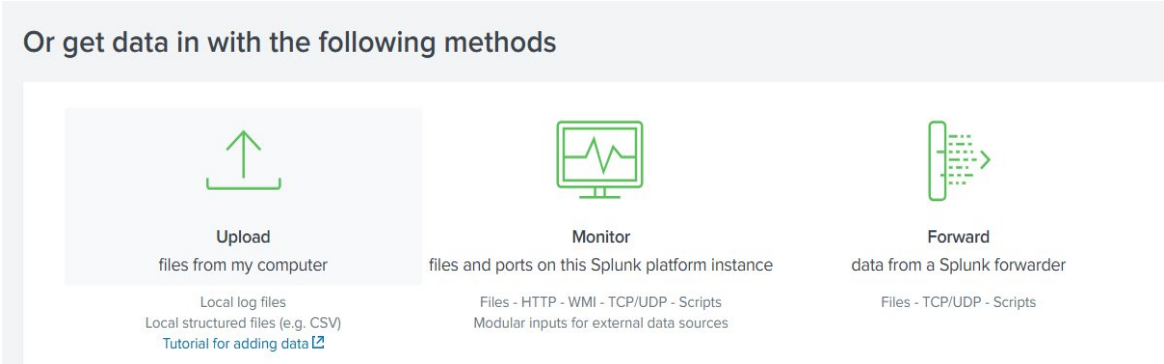
5. Sample Query and Logs Analysis:

   5.1 https://www.youtube.com/watch?v=LbR5cqqaFVk&t=1s
   5.2 GitHub - 0xrajneesh/Splunk-Projects-For-Beginners: Unlock the power of Splunk SIEM for comprehensive log analysis. Collaborate and innovate with our Splunk Log Analysis Projects on GitHub
   5.3 **Splunk Log Analysis.docx**
   = *:\Ogz\CyberSecurity\01_HowTo\1_Documentation\13_SecuringMyEnterprise\SOC_Analyst\SPLUNK_SIEM\Project\Leo_Project*

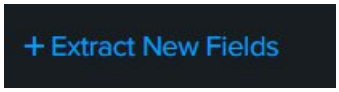


Hands-on: This will be applicable once Splunk Manager installation has been completed.

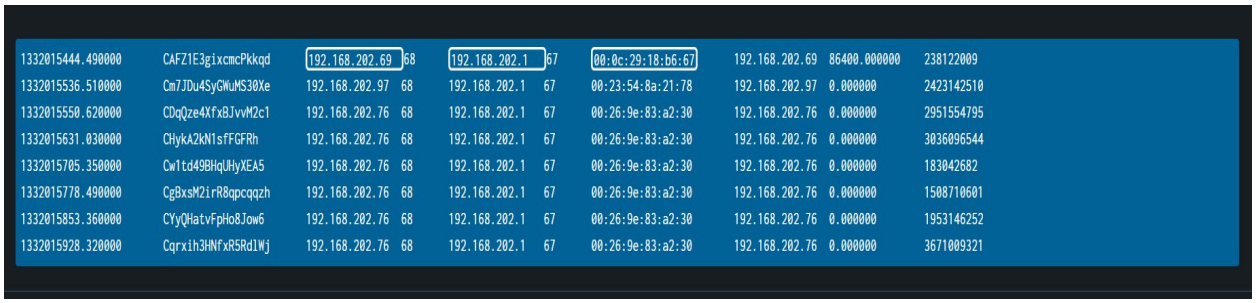
1. Download first a sample **DHCP logs** = Sample logs is located in *E:\Ogz\CyberSecurity\01_HowTo\1_Documentation\13_SecuringMyEnterprise\SOC_Analyst\SPLUNK_SIEM\Project\Leo_Project\dhcp.log*
2. Upload your Raw Data to SPLUNK for analyses. **Go to Settings > Click Add Data > Click Upload**



3. Create a new **FIELDS**, click Extract **New Fields**



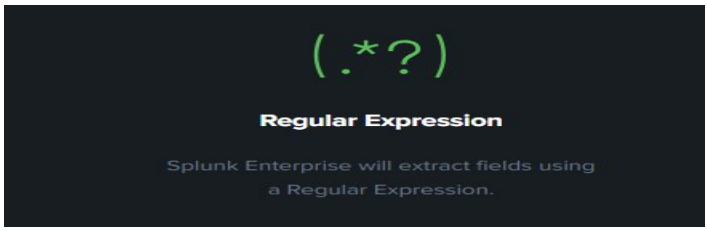
4. Click the **group of raw data** to make a new Fields



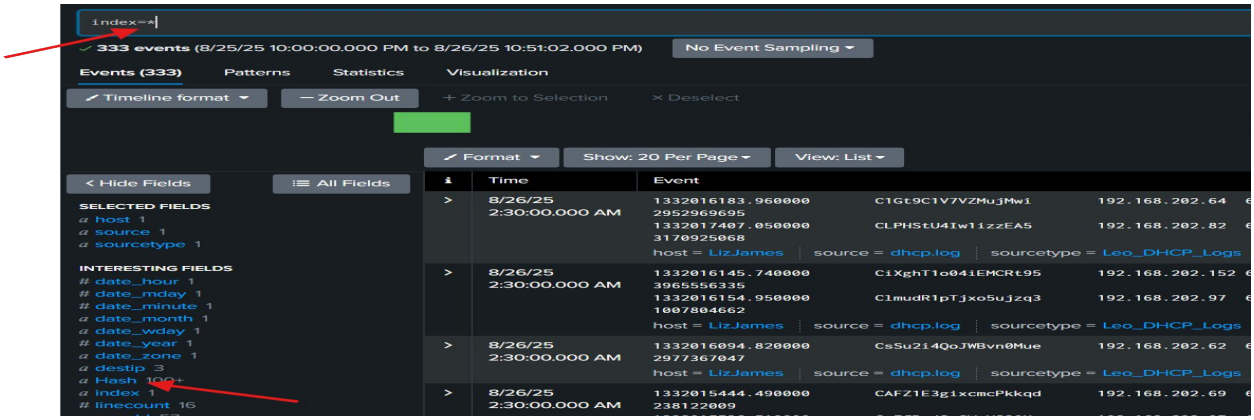
1332015444.490000	CAFZ1E3gixcmcPkkqd	192.168.202.69	68	192.168.202.1	67	00:0c:29:18:b6:67	192.168.202.69	86400.000000	238122009
1332015536.510000	Cm7JDu4SyGWuMS30Xe	192.168.202.97	68	192.168.202.1	67	00:23:54:8a:21:78	192.168.202.97	0.000000	2423142510
1332015550.620000	CDqQze4XfxBJvvM2c1	192.168.202.76	68	192.168.202.1	67	00:26:9e:83:a2:30	192.168.202.76	0.000000	2951554795
1332015631.030000	CHyka2kN1sfFGFRh	192.168.202.76	68	192.168.202.1	67	00:26:9e:83:a2:30	192.168.202.76	0.000000	3036096544
1332015705.350000	Cw1td49BHqUHyXEA5	192.168.202.76	68	192.168.202.1	67	00:26:9e:83:a2:30	192.168.202.76	0.000000	183042682
1332015778.490000	CgBxsM2irR8qpcqqzh	192.168.202.76	68	192.168.202.1	67	00:26:9e:83:a2:30	192.168.202.76	0.000000	1508710601
1332015853.360000	CYyQHatvFpHo8Jow6	192.168.202.76	68	192.168.202.1	67	00:26:9e:83:a2:30	192.168.202.76	0.000000	1953146252
1332015928.320000	CqrxIh3HNfxR5RdlWj	192.168.202.76	68	192.168.202.1	67	00:26:9e:83:a2:30	192.168.202.76	0.000000	3671009321

5. Click Next

6. Choose **Regular Expression** > Click Next



7. **Double clicks** a data that you want to create a new **Field Name** e.g. Hash
8. Click Add Extraction > Click Next > Click Next again > Click Finish
9. **The new Field will be added in the Interesting Fields.**
10. Type **index=*** to check the new added Fields below.



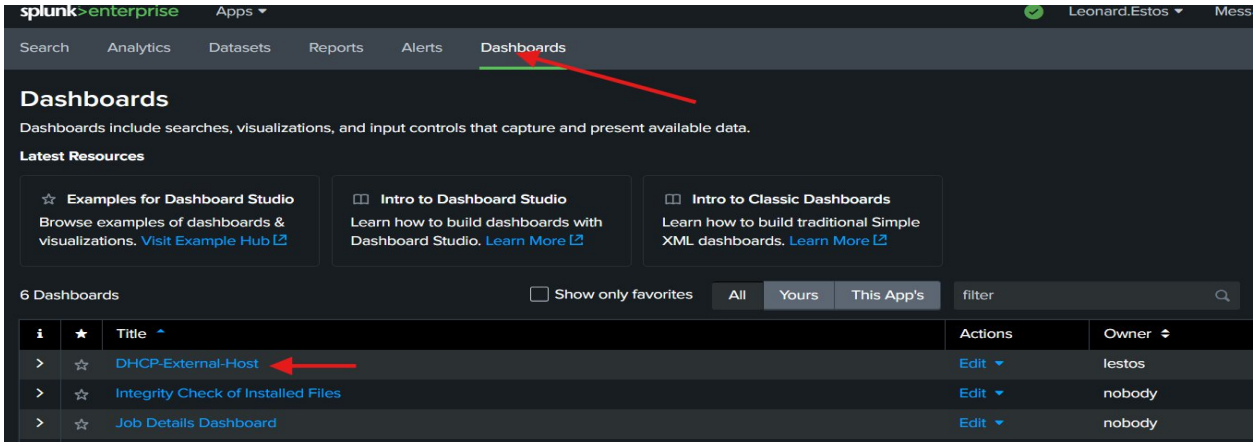
Proceed with sample query/search below.

Sample: **index=*** **(search all)**
source="dhcp.log" host="LizJames" sourcetype="Leo_DHCP_Logs" **(Initial Search)**
index=* sourcetype="leo_dhcp_logs" | table srcip, destip
index=* sourcetype="leo_dhcp_logs" | top limit=10 srcip
index=* sourcetype="leo_dhcp_logs" | timechart span=1d count by leased_ip
index=* sourcetype="leo_dhcp_logs" | top limit=10 srcip, destip | dedup srcip, destip

How to create a new Dashboard in Splunk:

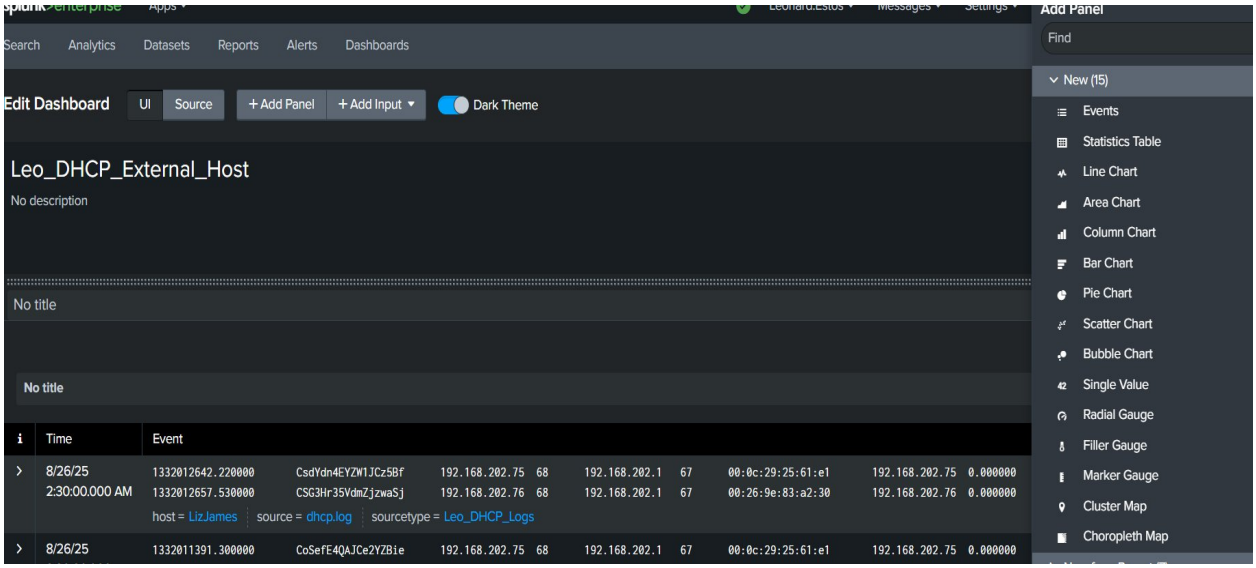
1. How to create a **new Dashboard** – The purpose of this is that your will not need to run the query again, just to to Dashboards only and check your created Dashboards

   1.1 Run query index=* sourcetype="leo_dhcp_logs" | top limit=10 srcip, destip | dedup srcip, destip
   1.2 Click SAVE AS > New Dashboard > Click Save to Dashboard
   1.3 View this in the Dashboard

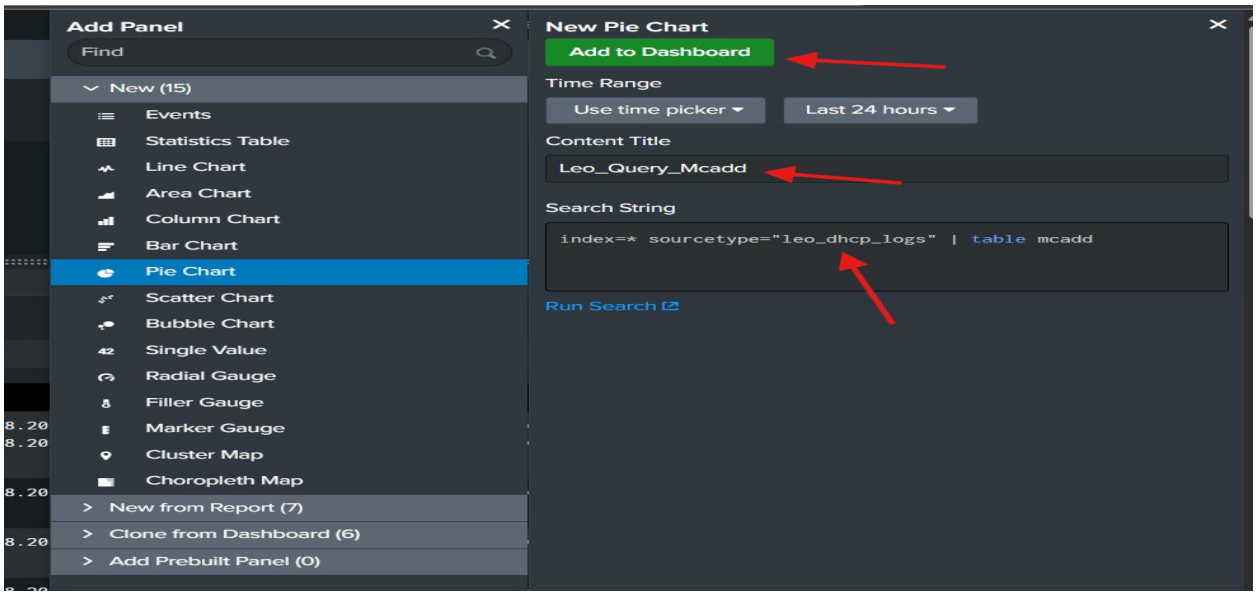


2. How to create a Dashboard with Graph for reporting.

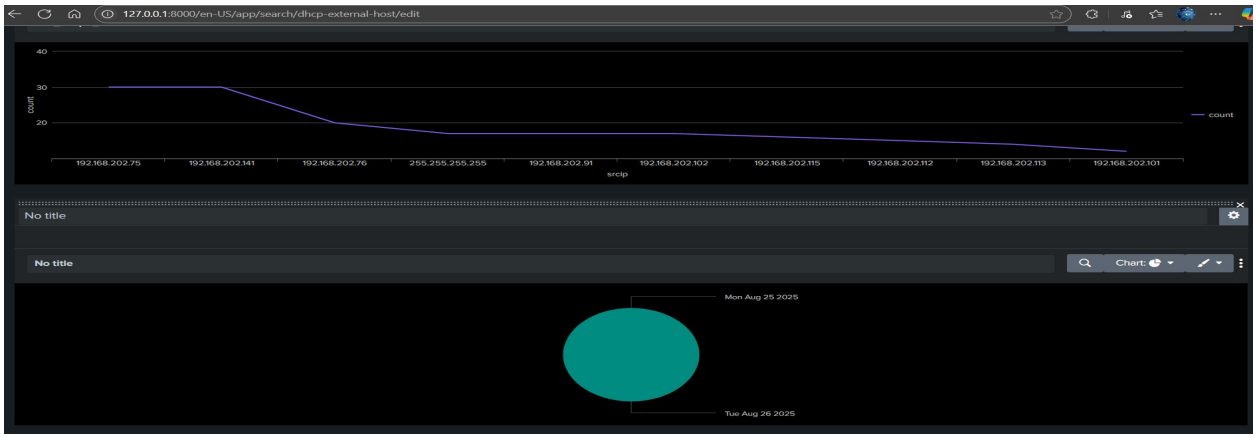
   2.1 Click your Dashboard > Click Leo_DHCP_External_Host > Click EDIT > Click Add Panel
   2.2 Choose any report that you want like graph



2.3 Put the Content Title > Search String/Query > ADD To Dashboard



2.4 Click SAVE > See Output Dashboard below.



DNS Logs Analyses:

1. Upload the DNS logs
2. Initial query once uploaded or default search.

   source="dns.log" host="LizJames" sourcetype="Leo_DNS_Logs"

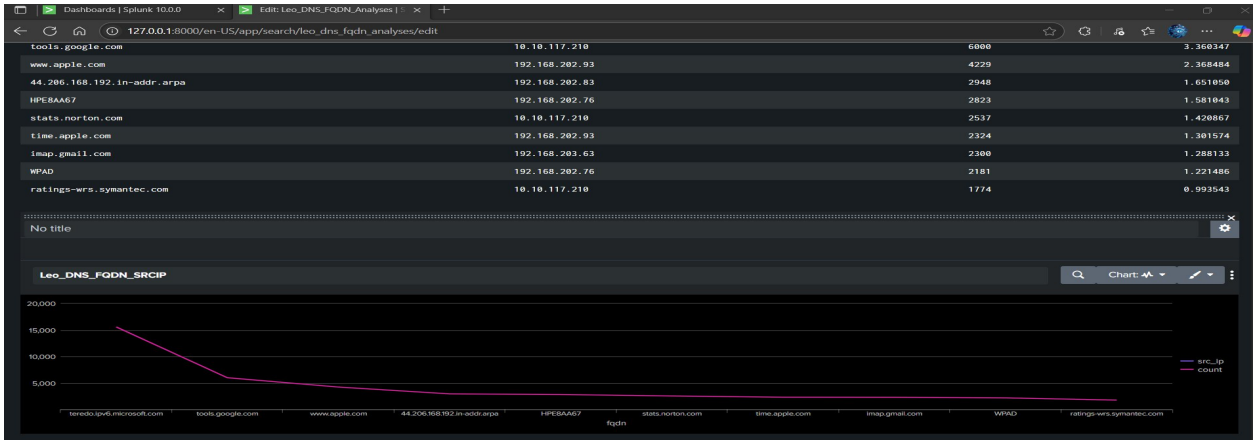
3. Sample queries available in GitHub: https://github.com/0xrajneesh/Splunk-Projects-For-Beginners/blob/main/Project%231-analyzing-dns-log-using%20splunk-siem.md

4. Note, create your own **FIELDS** first and do the query below.

   index=* sourcetype=Leo_DNS_Logs | top fqdn, src_ip
   index=* sourcetype=Leo_DNS_Logs | top limit=20 fqdn

"This query retrieves the top 20 fully qualified domain names (FQDNs) accessed, based on frequency, from the Leo_DNS_Logs sourcetype. High-frequency access to certain domains may indicate potential malicious activity or abnormal behavior worth investigating. "

5. Create a New Dashboard and Panel Report



🛡 **Threat Intelligence Workflow: Mitigation, Identification, Analysis, Response, and Detection. This section outlines key tools and steps for performing threat intelligence and reconnaissance activities.**

1. Malicious Artifact Verification – VirusTotal

Use VirusTotal to inspect suspicious digital artifacts:

- File: Upload and scan for malware signatures.
- URL: Check for phishing or malicious redirects.
- IP Address: Investigate known malicious hosts.
- Domain: Analyze domain reputation and associated threats.

VirusTotal aggregates data from multiple antivirus engines and threat intelligence sources to provide a comprehensive risk assessment.

2. Reconnaissance & Analysis – MXToolbox

Access MXToolbox Super Tool for domain and network reconnaissance:

- DNS Lookup
- Blacklist Check
- SMTP Diagnostics
- WHOIS Information
- IP Geolocation

MXToolbox is valuable for identifying misconfigurations, open relays, and potential indicators of compromise (IOCs).

SPLUNK Enterprise Security: **This will be the SOC Analyst use all the time.**

" When you train Smarter, you defend Stronger"
Leonard Estos