The University of Texas at Austin
Informatics
School of Information

The University of Texas System

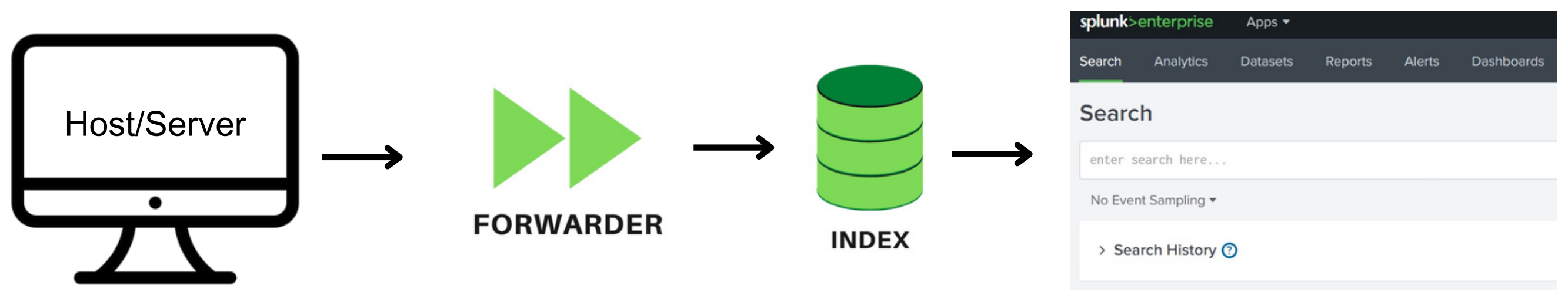
The University of Texas System - Information Security Office
Ethan Wen | Fall 2024 | Supervisor: Thomas Lane

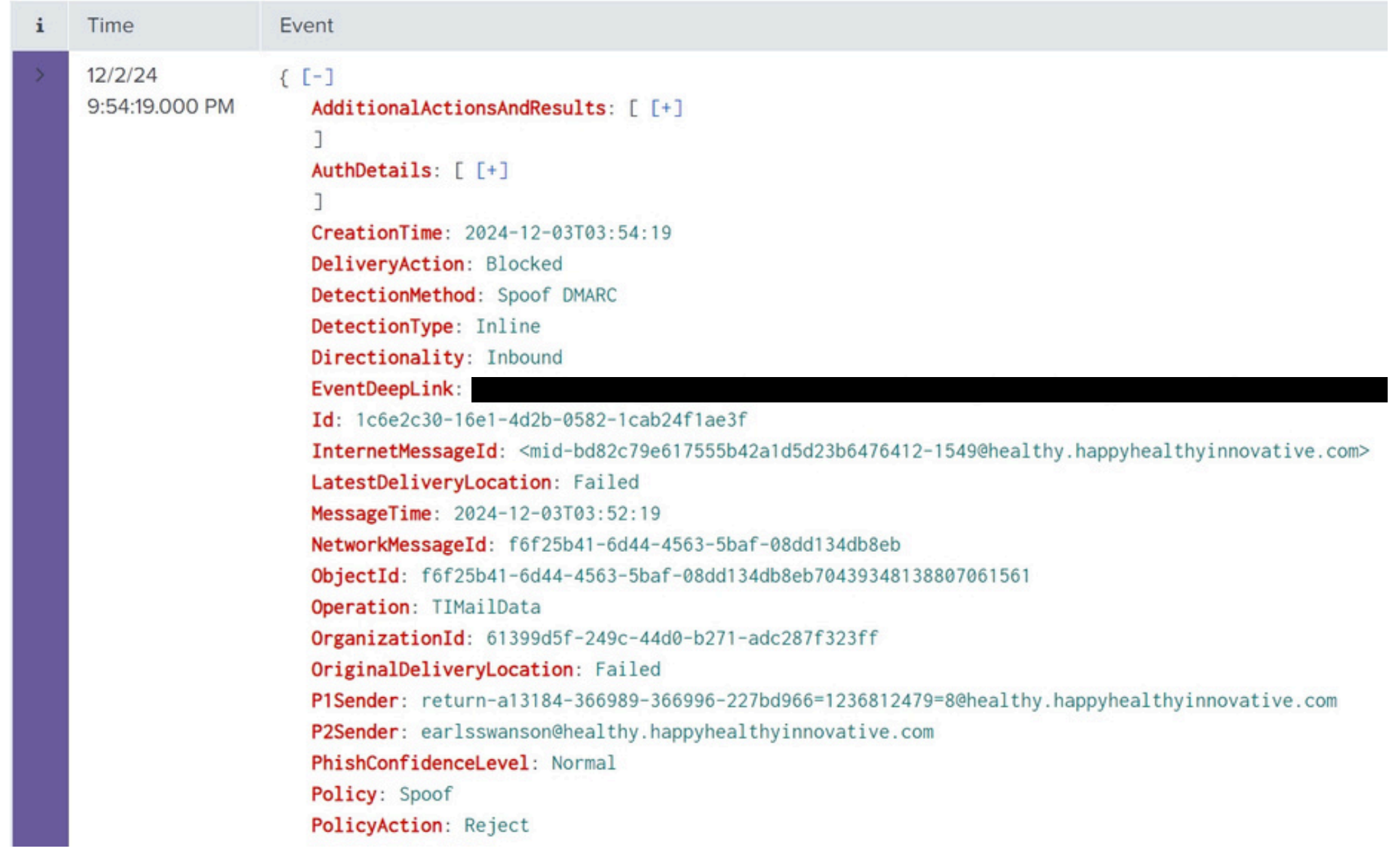
Revamping Security Operation Center (SOC) Dashboards in Splunk

Abstract

This applied project addresses the underutilization of Splunk by UT System SOC interns due to knowledge gaps in infrastructure and SPL (Search Processing Language). It aims to leverage Splunk's data visualization and real-time analytics capabilities, improving the SOC's ability to **monitor and respond to security events effectively**. The primary objectives are to develop a comprehensive understanding of SPL, create documentation for future interns, design "Search Macros", and create SOC dashboards for current needs.

Raw data forwarded to Splunk Indexers are ingested and separated into individual events which can be queried through the Search Head.





i	Time	Event
>	12/2/24 9:54:19.000 PM	{ [-] AdditionalActionsAndResults: [[+]] AuthDetails: [[+]] CreationTime: 2024-12-03T03:54:19 DeliveryAction: Blocked DetectionMethod: Spoof DMARC DetectionType: Inline Directionality: Inbound EventDeepLink: [redacted] Id: 1c6e2c30-16e1-4d2b-0582-1cab24f1ae3f InternetMessageId: <mid-bd82c79e617555b42a1d5d23b6476412-1549@healthy.happyhealthyinnovative.com> LatestDeliveryLocation: Failed MessageTime: 2024-12-03T03:52:19 NetworkMessageId: f6f25b41-6d44-4563-5baf-08dd134db8eb ObjectId: f6f25b41-6d44-4563-5baf-08dd134db8eb70439348138807061561 Operation: TIMailData OrganizationId: 61399d5f-249c-44d0-b271-adc287f323ff OriginalDeliveryLocation: Failed P1Sender: return-a13184-366989-366996-227bd966=1236812479=8@healthy.happyhealthyinnovative.com P2Sender: earlsswanson@healthy.happyhealthyinnovative.com PhishConfidenceLevel: Normal Policy: Spoof PolicyAction: Reject

Ex: Splunk Event regarding a quarantined email

Methodology

1. **Data Exploration**
   - Understanding the type of events stored in each index
   - Reviewing useful/familiar attributes shared between events that should be monitored
2. **Cross-Referencing data from Microsoft Defender XDR**
   - Ensuring that the number of events/attributes were available on both platforms
   - Reviewing .csv files to tune search queries on missing alerts/events from Defender
3. **Tuning SPL Queries**
   - Creating Search Macros - eliminating the need for saving long queries
   - Further tuning the queries to normalize attributes between the events for better comprehension
4. **Enhancing Data**
   - Included an attribute on the Departments that each employee (attached to the event) was part of through a csv lookup addition to the query
   - Added .kml files to bring in geographic data for visualizations requiring maps
5. **Creating Visualizations**
   - Tailoring the saved search for each visualization required (pie chart, maps, individual statistics, bar chart, statistics table)
6. **Implementing Search Tokens**
   - Integrating search tokens in some search queries and providing inputs

Outcomes

Dashboards monitoring real-time Splunk Events for Quarantined Emails and Data Loss Prevention Policy Alerts

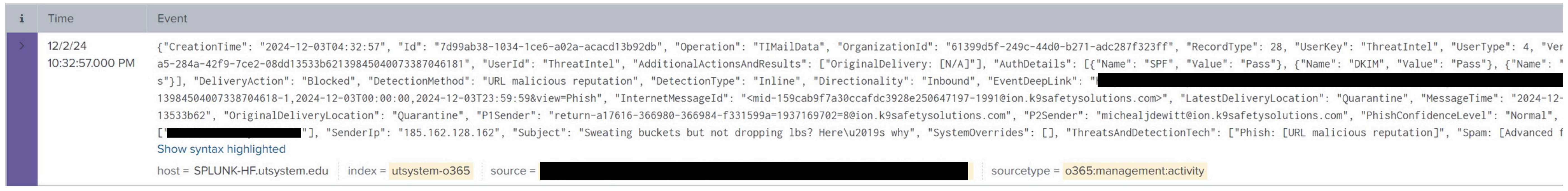
User inputs allowing interns/employees to filter out alerts based on attributes without the need to craft an SPL query

Future Goals

Incorporating other security events so as to monitor and represent them through data visualizations rather than logs for better insights (ex: Which department is impacted the most?)

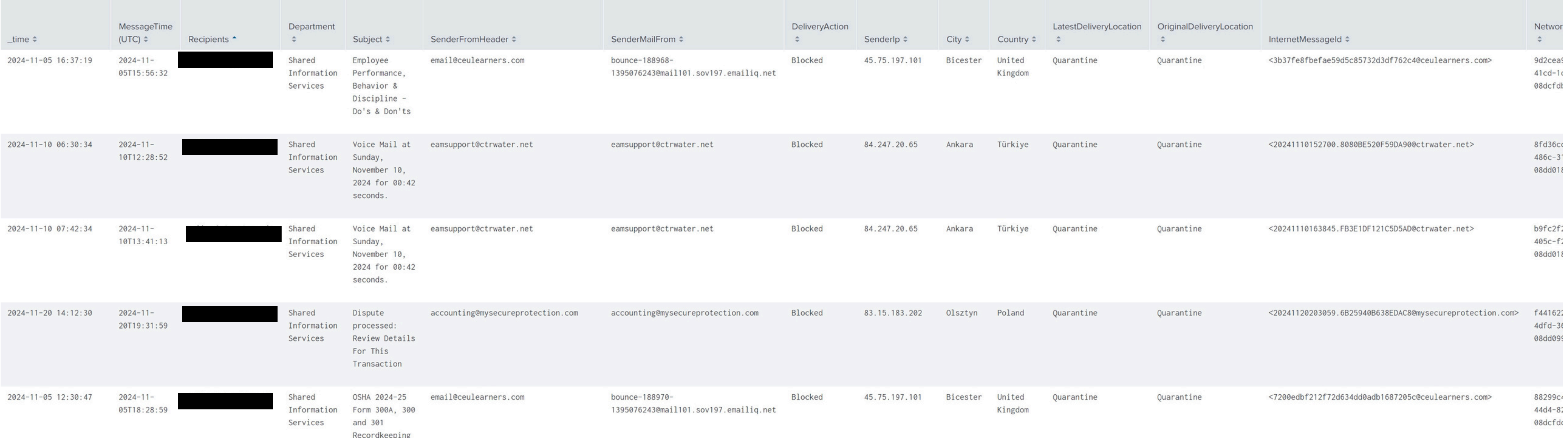
Predictive Analytics to forecast future security events

Raw data (JSON Format)



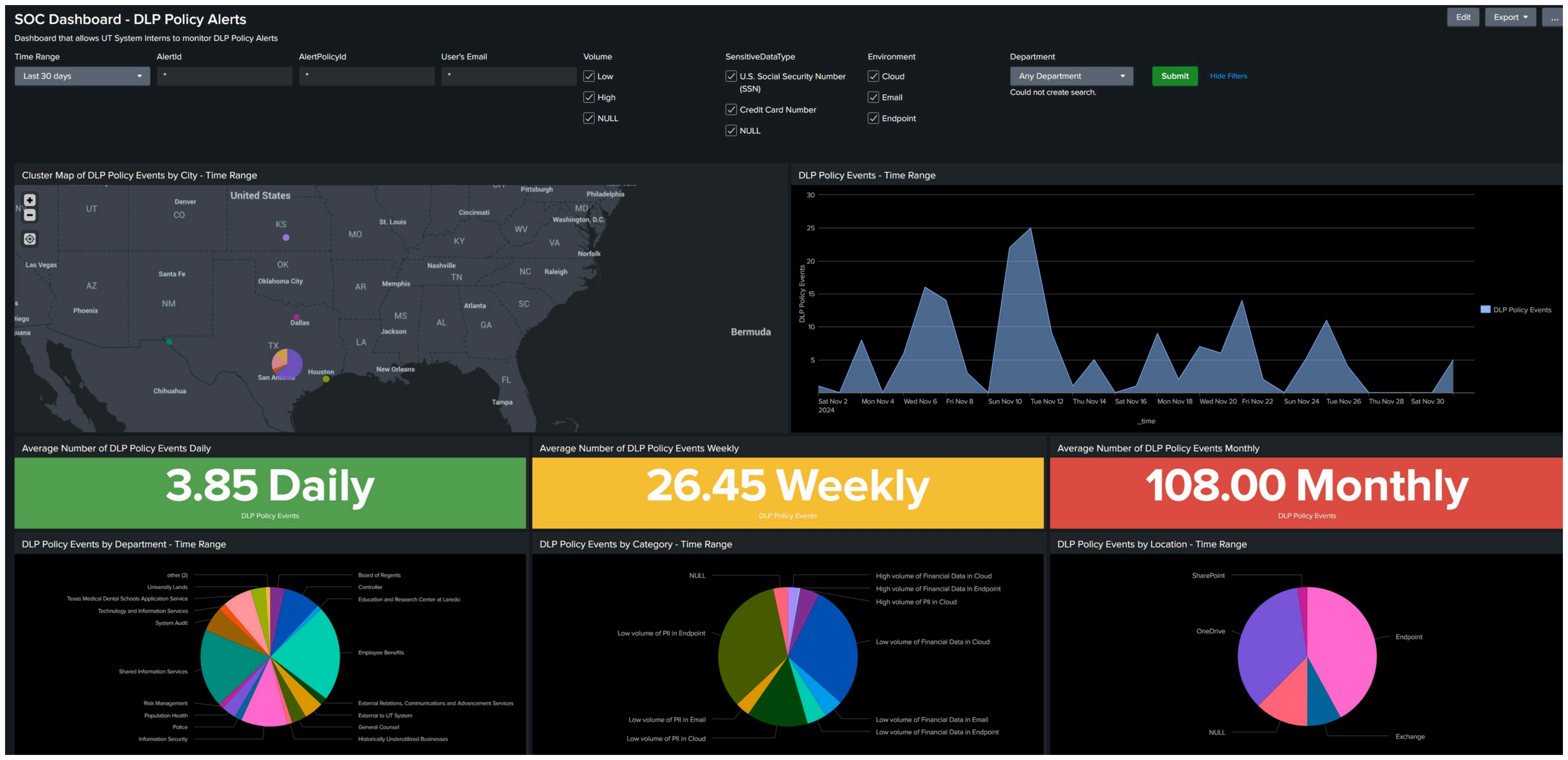
i	Time	Event
>	12/2/24 10:32:57.000 PM	{"CreationTime": "2024-12-03T04:32:57", "Id": "7d99ab38-1034-1ce6-a02a-acacd13b92db", "Operation": "TIMailData", "OrganizationId": "61399d5f-249c-44d0-b271-adc287f323ff", "RecordType": 28, "UserKey": "ThreatIntel", "UserType": 4, "Ver a5-284a-42f9-7ce2-08dd13533b62139845040073387046181", "UserId": "ThreatIntel", "AdditionalActionsAndResults": ["OriginalDelivery: [N/A]"], "AuthDetails": [{"Name": "SPF", "Value": "Pass"}, {"Name": "DKIM", "Value": "Pass"}, {"Name": " s"}], "DeliveryAction": "Blocked", "DetectionMethod": "URL malicious reputation", "DetectionType": "Inline", "Directionality": "Inbound", "EventDeepLink": "[redacted] 13984504007338704618-1,2024-12-03T00:00:00,2024-12-03T23:59:59&view=Phish", "InternetMessageId": "<mid-159cab9f7a30ccafdc3928e250647197-1991@ion.k9safetysolutions.com>", "LatestDeliveryLocation": "Quarantine", "MessageTime": "2024-12- 13533b62", "OriginalDeliveryLocation": "Quarantine", "P1Sender": "return-a17616-366980-366984-f331599a=1937169702=8@ion.k9safetysolutions.com", "P2Sender": "michealjdewitt@ion.k9safetysolutions.com", "PhishConfidenceLevel": "Normal", ["[redacted]"], "SenderIp": "185.162.128.162", "Subject": "Sweating buckets but not dropping lbs? Here\u2019s why", "SystemOverrides": [], "ThreatsAndDetectionTech": ["Phish: [URL malicious reputation]", "Spam: [Advanced f Show syntax highlighted host = SPLUNK-HF.utsystem.edu index = utsystem-o365 source = [redacted] sourcetype = o365:management:activity

Statistics Table (from SPL Queries)



_time	MessageTime (UTC)	Recipients	Department	Subject	SenderFromHeader	SenderMailFrom	DeliveryAction	SenderIp	City	Country	LatestDeliveryLocation	OriginalDeliveryLocation	InternetMessageId	Networ
2024-11-05 16:37:19	2024-11-05T15:56:32	[redacted]	Shared Information Services	Employee Performance, Behavior & Discipline - Do's & Don'ts	email@ceulearners.com	bounce-188968-1395076243@mail101.sov197.emailiq.net	Blocked	45.75.197.101	Bicester	United Kingdom	Quarantine	Quarantine	<3b37fe8fbefae59d5c85732d3df762c4@ceulearners.com>	9d2cea 41cd-1 08dcfd
2024-11-10 06:30:34	2024-11-10T12:28:52	[redacted]	Shared Information Services	Voice Mail at Sunday, November 10, 2024 for 00:42 seconds.	eamsupport@ctrwater.net	eamsupport@ctrwater.net	Blocked	84.247.20.65	Ankara	Türkiye	Quarantine	Quarantine	<20241110152700.8080BE520F59DA90@ctrwater.net>	8fd36c 486c-3 08dd01
2024-11-10 07:42:34	2024-11-10T13:41:13	[redacted]	Shared Information Services	Voice Mail at Sunday, November 10, 2024 for 00:42 seconds.	eamsupport@ctrwater.net	eamsupport@ctrwater.net	Blocked	84.247.20.65	Ankara	Türkiye	Quarantine	Quarantine	<20241110163845.FB3E1DF121C5D5AD@ctrwater.net>	b9fc2f 405c-f 08dd01
2024-11-20 14:12:30	2024-11-20T19:31:59	[redacted]	Shared Information Services	Dispute processed: Review Details For This Transaction	accounting@mysecureprotection.com	accounting@mysecureprotection.com	Blocked	83.15.183.202	Olsztyn	Poland	Quarantine	Quarantine	<20241120203059.6B25940B638EDAC8@mysecureprotection.com>	f44162 4dfd-3 08dd09
2024-11-05 12:30:47	2024-11-05T18:28:59	[redacted]	Shared Information Services	OSHA 2024-25 Form 300A, 300 and 301 Recordkeeping	email@ceulearners.com	bounce-188970-1395076243@mail101.sov197.emailiq.net	Blocked	45.75.197.101	Bicester	United Kingdom	Quarantine	Quarantine	<7200edbf212f72d634dd0adb1687205c@ceulearners.com>	88299c 44d4-8 08dcfd

Dashboard (ex: monitoring DLP Policy Alerts)



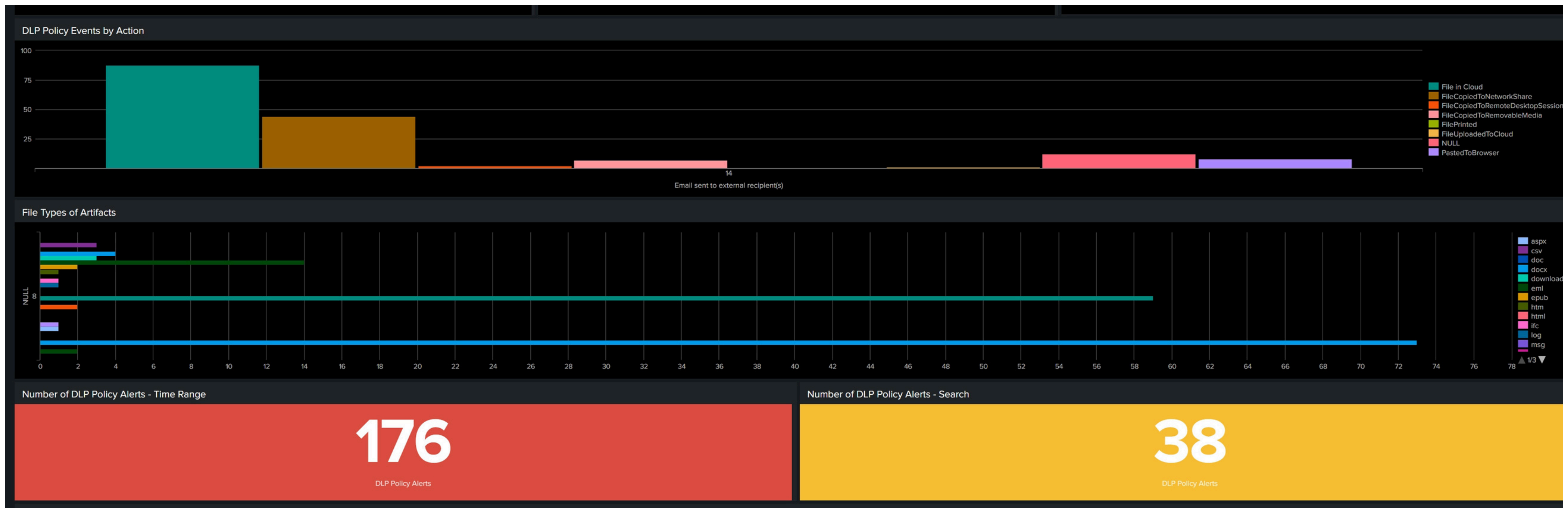
SOC Dashboard - DLP Policy Alerts

Dashboard that allows UT System Interns to monitor DLP Policy Alerts

Time Range: Last 30 days
AlertId: *
AlertPolicyId: *
User's Email: *
Volume: ☑ Low ☑ High ☑ NULL
SensitiveDataType: ☑ U.S. Social Security Number (SSN) ☑ Credit Card Number ☑ NULL
Environment: ☑ Cloud ☑ Email ☑ Endpoint
Department: Any Department
Could not create search.

Average Number of DLP Policy Events Daily: 3.85 Daily (DLP Policy Events)
Average Number of DLP Policy Events Weekly: 26.45 Weekly (DLP Policy Events)
Average Number of DLP Policy Events Monthly: 108.00 Monthly (DLP Policy Events)

Edit
Export
...
Submit
Hide Filters
Cluster Map of DLP Policy Events by City - Time Range
United States
UT
CO
Denver
KS
MO
St. Louis
Cincinnati
KY
WV
VA
MD
Washington, D.C.
Pittsburgh
Philadelphia
Norfolk
Las Vegas
AZ
Phoenix
NM
Santa Fe
OK
Oklahoma City
AR
Memphis
Nashville
TN
NC
Raleigh
SC
Atlanta
GA
AL
MS
Jackson
LA
TX
Dallas
San Antonio
Houston
New Orleans
FL
Tampa
Chihuahua
Bermuda
DLP Policy Events - Time Range
30
25
20
15
10
5
DLP Policy Events
Sat Nov 2 2024
Mon Nov 4
Wed Nov 6
Fri Nov 8
Sun Nov 10
Tue Nov 12
Thu Nov 14
Sat Nov 16
Mon Nov 18
Wed Nov 20
Fri Nov 22
Sun Nov 24
Tue Nov 26
Thu Nov 28
Sat Nov 30
_time
DLP Policy Events by Department - Time Range
other (2)
University Lands
Texas Medical Dental Schools Application Service
Technology and Information Services
System Audit
Shared Information Services
Risk Management
Population Health
Police
Information Security
Board of Regents
Controller
Education and Research Center at Laredo
Employee Benefits
External Relations, Communications and Advancement Services
External to UT System
General Counsel
Historically Underutilized Businesses
DLP Policy Events by Category - Time Range
NULL
Low volume of PII in Endpoint
Low volume of PII in Email
Low volume of PII in Cloud
High volume of Financial Data in Cloud
High volume of Financial Data in Endpoint
High volume of PII in Cloud
Low volume of Financial Data in Cloud
Low volume of Financial Data in Email
Low volume of Financial Data in Endpoint
DLP Policy Events by Location - Time Range
SharePoint
OneDrive
NULL
Endpoint
Exchange



Number of DLP Policy Alerts - Time Range: 176 (DLP Policy Alerts)
Number of DLP Policy Alerts - Search: 38 (DLP Policy Alerts)