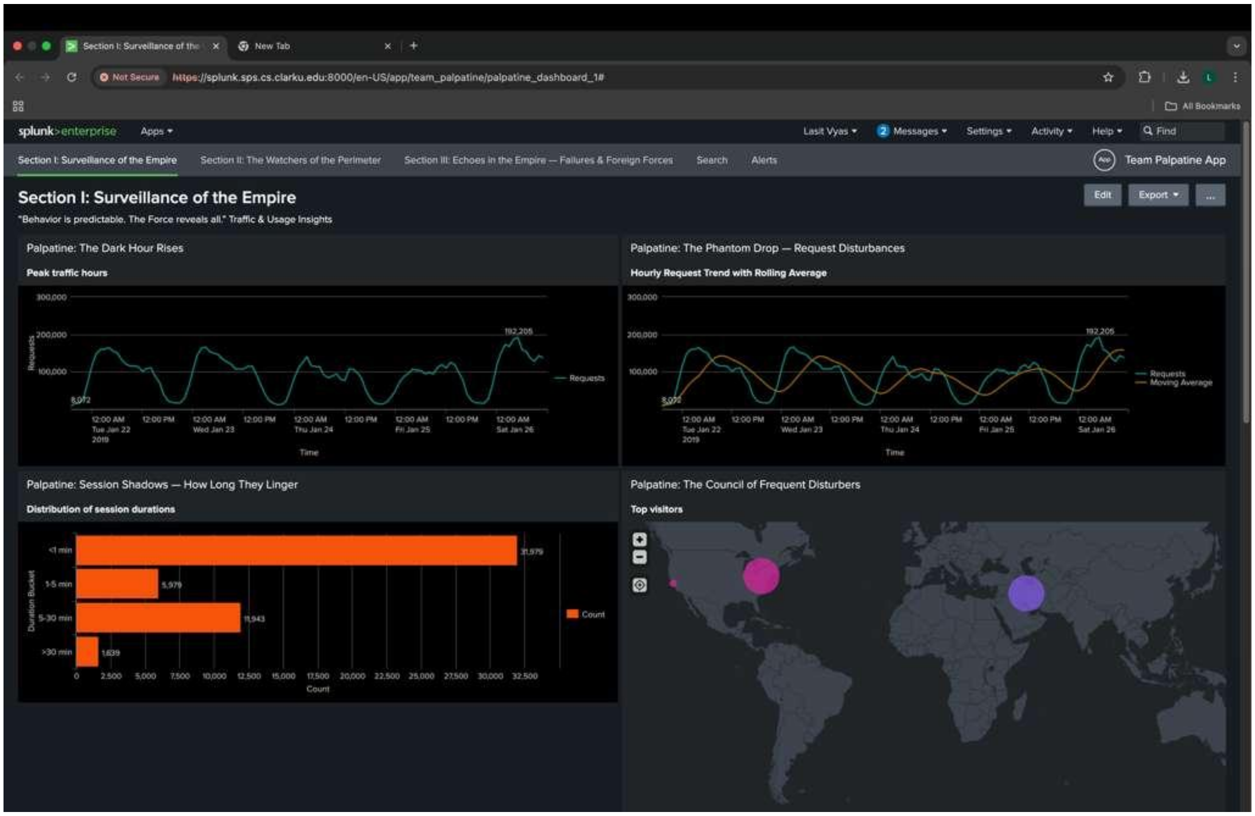

Section I: Surveillance of the
New Tab
Not Secure
https://splunk.sps.cs.clarku.edu:8000/en-US/app/team_palpatine/palpatine_dashboard_1#
All Bookmarks
splunk>enterprise
Apps ▾
Lasit Vyas ▾
2 Messages ▾
Settings ▾
Activity ▾
Help ▾
Find
Section I: Surveillance of the Empire
Section II: The Watchers of the Perimeter
Section III: Echoes in the Empire — Failures & Foreign Forces
Search
Alerts
Team Palpatine App
Edit
Export ▾
...

Section I: Surveillance of the Empire

"Behavior is predictable. The Force reveals all." Traffic & Usage Insights

Palpatine: The Dark Hour Rises

Peak traffic hours

Palpatine: The Phantom Drop — Request Disturbances

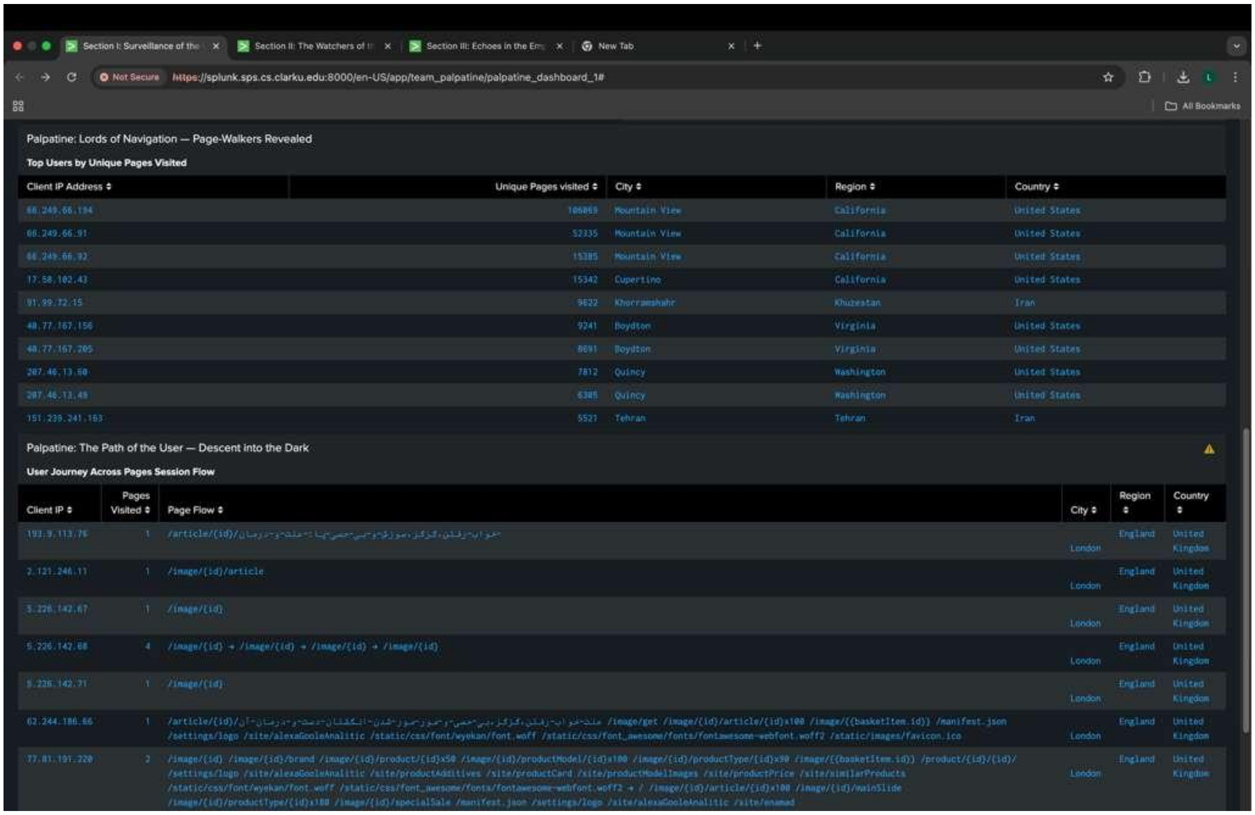
Hourly Request Trend with Rolling Average

Palpatine: Session Shadows — How Long They Linger

Distribution of session durations

Palpatine: The Council of Frequent Disturbers

Top visitors


Section I: Surveillance of the
Section II: The Watchers of t
Section III: Echoes in the Em
New Tab
Not Secure
https://splunk.sps.cs.clarku.edu:8000/en-US/app/team_palpatine/palpatine_dashboard_1#
All Bookmarks

Palpatine: Lords of Navigation — Page-Walkers Revealed

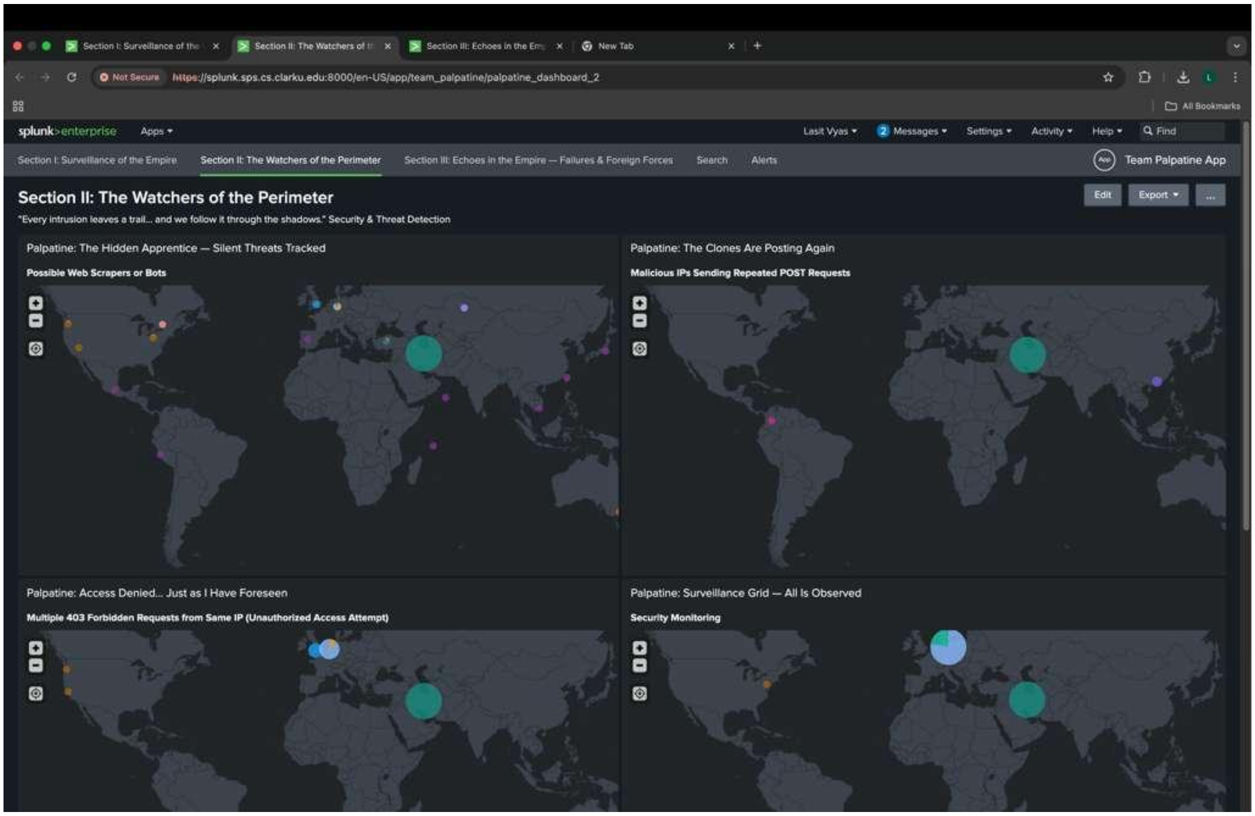
Top Users by Unique Pages Visited

Client IP Address ⇕	Unique Pages visited ⇕	City ⇕	Region ⇕	Country ⇕
66.249.66.194	106869	Mountain View	California	United States
66.249.66.91	52335	Mountain View	California	United States
66.249.66.92	15385	Mountain View	California	United States
17.58.102.43	15342	Cupertino	California	United States
91.99.72.15	9622	Khorramshahr	Khuzestan	Iran
40.77.167.156	9241	Boydton	Virginia	United States
40.77.167.205	8691	Boydton	Virginia	United States
207.46.13.60	7812	Quincy	Washington	United States
207.46.13.49	6385	Quincy	Washington	United States
151.239.241.163	5521	Tehran	Tehran	Iran

Palpatine: The Path of the User — Descent into the Dark

User Journey Across Pages Session Flow

Client IP ⇕	Pages Visited ⇕	Page Flow ⇕	City ⇕	Region ⇕	Country ⇕
193.9.113.76	1	/article/{id}/خواب-رفتن،گزگز،سوزش-و-بی-حسی-پا؛-علت-و-درمان	London	England	United Kingdom
2.121.246.11	1	/image/{id}/article	London	England	United Kingdom
5.226.142.67	1	/image/{id}	London	England	United Kingdom
5.226.142.68	4	/image/{id} → /image/{id} → /image/{id} → /image/{id}	London	England	United Kingdom
5.226.142.71	1	/image/{id}	London	England	United Kingdom
62.244.186.66	1	/article/{id}/علت-خواب-رفتن،گزگز،بی-حسی-و-سوزسوز-شدن-انگشتان-دست-و-درمان-آن /image/get /image/{id}/article/{id}x100 /image/{{basketItem.id}} /manifest.json /settings/logo /site/alexaGooleAnalitic /static/css/font/wyekan/font.woff /static/css/font_awesome/fonts/fontawesome-webfont.woff2 /static/images/favicon.ico	London	England	United Kingdom
77.81.191.220	2	/image/{id} /image/{id}/brand /image/{id}/product/{id}x50 /image/{id}/productModel/{id}x100 /image/{id}/productType/{id}x90 /image/{{basketItem.id}} /product/{id}/{id}/ /settings/logo /site/alexaGooleAnalitic /site/productAdditives /site/productCard /site/productModelImages /site/productPrice /site/similarProducts /static/css/font/wyekan/font.woff /static/css/font_awesome/fonts/fontawesome-webfont.woff2 → / /image/{id}/article/{id}x100 /image/{id}/mainSlide /image/{id}/productType/{id}x100 /image/{id}/specialSale /manifest.json /settings/logo /site/alexaGooleAnalitic /site/enamad	London	England	United Kingdom


Section I: Surveillance of the
Section II: The Watchers of t
Section III: Echoes in the Em
New Tab
Not Secure
https://splunk.sps.cs.clarku.edu:8000/en-US/app/team_palpatine/palpatine_dashboard_2
All Bookmarks
splunk>enterprise
Apps
Lasit Vyas
2 Messages
Settings
Activity
Help
Find
Section I: Surveillance of the Empire
Section II: The Watchers of the Perimeter
Section III: Echoes in the Empire — Failures & Foreign Forces
Search
Alerts
Team Palpatine App
Edit
Export
...

Section II: The Watchers of the Perimeter

"Every intrusion leaves a trail... and we follow it through the shadows." Security & Threat Detection

Palpatine: The Hidden Apprentice — Silent Threats Tracked

Possible Web Scrapers or Bots

Palpatine: The Clones Are Posting Again

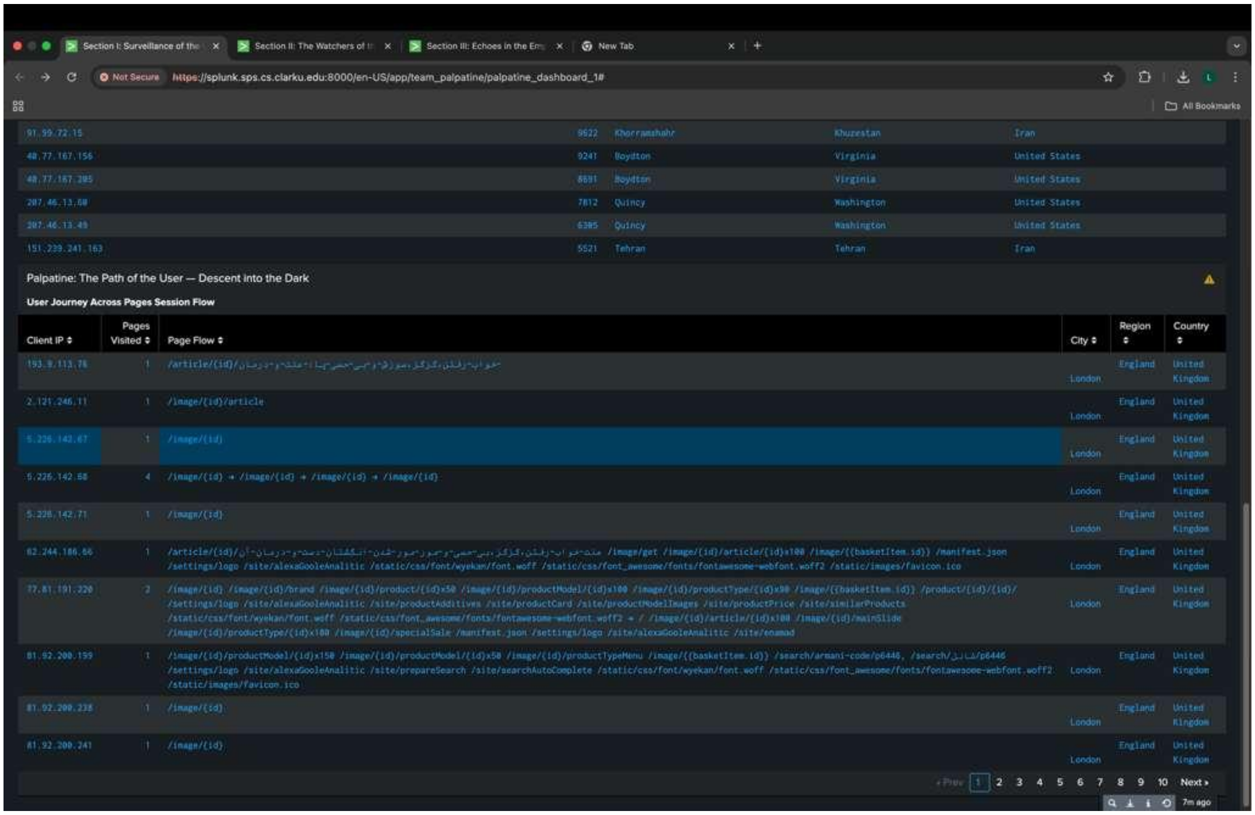
Malicious IPs Sending Repeated POST Requests

Palpatine: Access Denied... Just as I Have Foreseen

Multiple 403 Forbidden Requests from Same IP (Unauthorized Access Attempt)

Palpatine: Surveillance Grid — All Is Observed

Security Monitoring

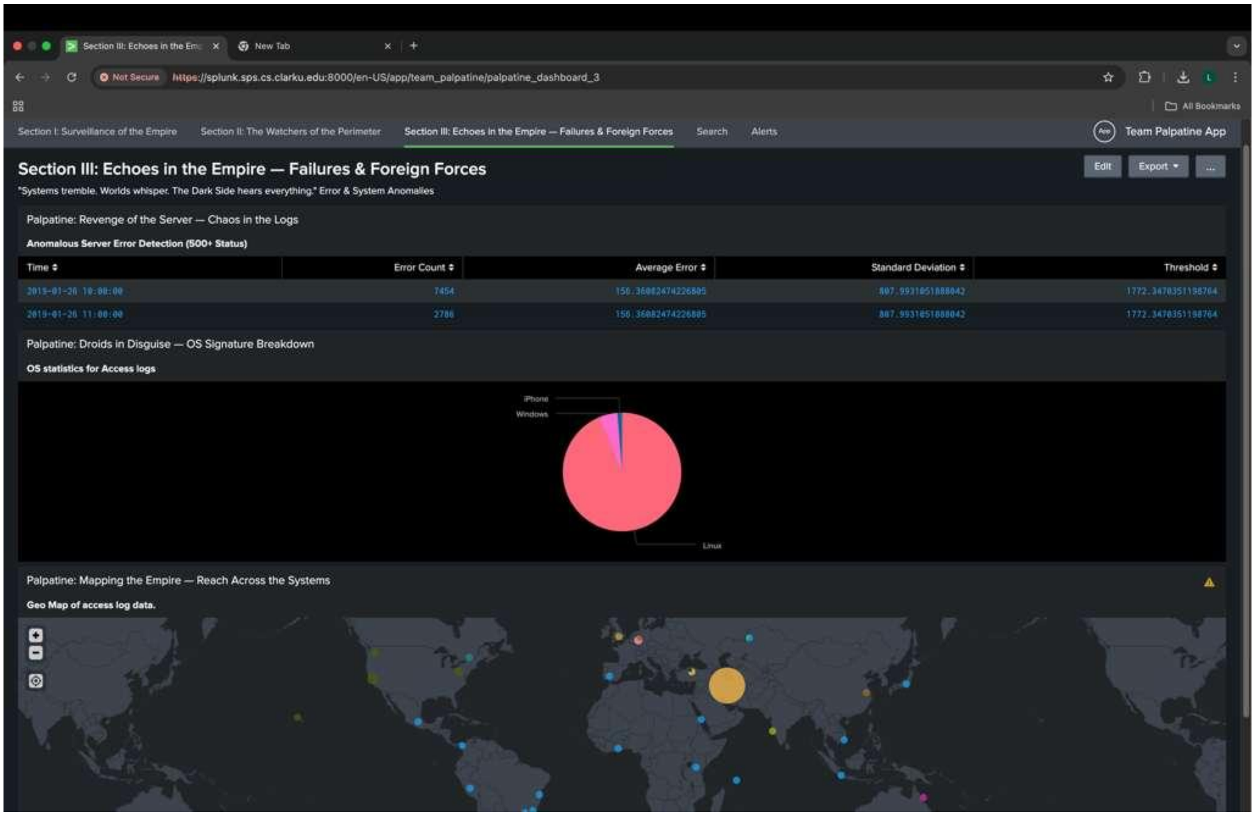

Section I: Surveillance of the
Section II: The Watchers of t
Section III: Echoes in the Em
New Tab
Not Secure
https://splunk.sps.cs.clarku.edu:8000/en-US/app/team_palpatine/palpatine_dashboard_1#
All Bookmarks

91.99.72.15	9622	Khorramshahr	Khuzestan	Iran
40.77.167.156	9241	Boydton	Virginia	United States
40.77.167.205	8691	Boydton	Virginia	United States
207.46.13.68	7812	Quincy	Washington	United States
207.46.13.49	6305	Quincy	Washington	United States
151.239.241.163	5521	Tehran	Tehran	Iran

Palpatine: The Path of the User — Descent into the Dark

User Journey Across Pages Session Flow

Client IP ⇕	Pages Visited ⇕	Page Flow ⇕	City ⇕	Region ⇕	Country ⇕
193.9.113.76	1	/article/{id}/خواب-رفتن،گزگز،سوزن-سوزن-و-بی-حسی-ها؛-علت-و-درمان	London	England	United Kingdom
2.121.246.11	1	/image/{id}/article	London	England	United Kingdom
5.226.142.67	1	/image/{id}	London	England	United Kingdom
5.226.142.68	4	/image/{id} → /image/{id} → /image/{id} → /image/{id}	London	England	United Kingdom
5.226.142.71	1	/image/{id}	London	England	United Kingdom
62.244.186.66	1	/article/{id}/علت-خواب-رفتن،گزگز،بی-حسی-و-سوز-سوزن-شدن-انگشتان-دست-و-درمان-آن /image/get /image/{id}/article/{id}x100 /image/{{basketItem.id}} /manifest.json /settings/logo /site/alexaGooleAnalitic /static/css/font/wyekan/font.woff /static/css/font_awesome/fonts/fontawesome-webfont.woff2 /static/images/favicon.ico	London	England	United Kingdom
77.81.191.220	2	/image/{id} /image/{id}/brand /image/{id}/product/{id}x50 /image/{id}/productModel/{id}x100 /image/{id}/productType/{id}x90 /image/{{basketItem.id}} /product/{id}/{id}/ /settings/logo /site/alexaGooleAnalitic /site/productAdditives /site/productCard /site/productModelImages /site/productPrice /site/similarProducts /static/css/font/wyekan/font.woff /static/css/font_awesome/fonts/fontawesome-webfont.woff2 → / /image/{id}/article/{id}x100 /image/{id}/mainSlide /image/{id}/productType/{id}x100 /image/{id}/specialSale /manifest.json /settings/logo /site/alexaGooleAnalitic /site/enamad	London	England	United Kingdom
81.92.200.159	1	/image/{id}/productModel/{id}x150 /image/{id}/productModel/{id}x50 /image/{id}/productTypeMenu /image/{{basketItem.id}} /search/armani-code/p6446, /search/شانل/p6446 /settings/logo /site/alexaGooleAnalitic /site/prepareSearch /site/searchAutoComplete /static/css/font/wyekan/font.woff /static/css/font_awesome/fonts/fontawesome-webfont.woff2 /static/images/favicon.ico	London	England	United Kingdom
81.92.200.238	1	/image/{id}	London	England	United Kingdom
81.92.200.241	1	/image/{id}	London	England	United Kingdom



Section III: Echoes in the Emp ×
New Tab ×
+
Not Secure
https://splunk.sps.cs.clarku.edu:8000/en-US/app/team_palpatine/palpatine_dashboard_3
All Bookmarks
Section I: Surveillance of the Empire
Section II: The Watchers of the Perimeter
Section III: Echoes in the Empire — Failures & Foreign Forces
Search
Alerts
Team Palpatine App
Edit
Export ▾
...

Section III: Echoes in the Empire — Failures & Foreign Forces

"Systems tremble. Worlds whisper. The Dark Side hears everything." Error & System Anomalies

Palpatine: Revenge of the Server — Chaos in the Logs

Anomalous Server Error Detection (500+ Status)

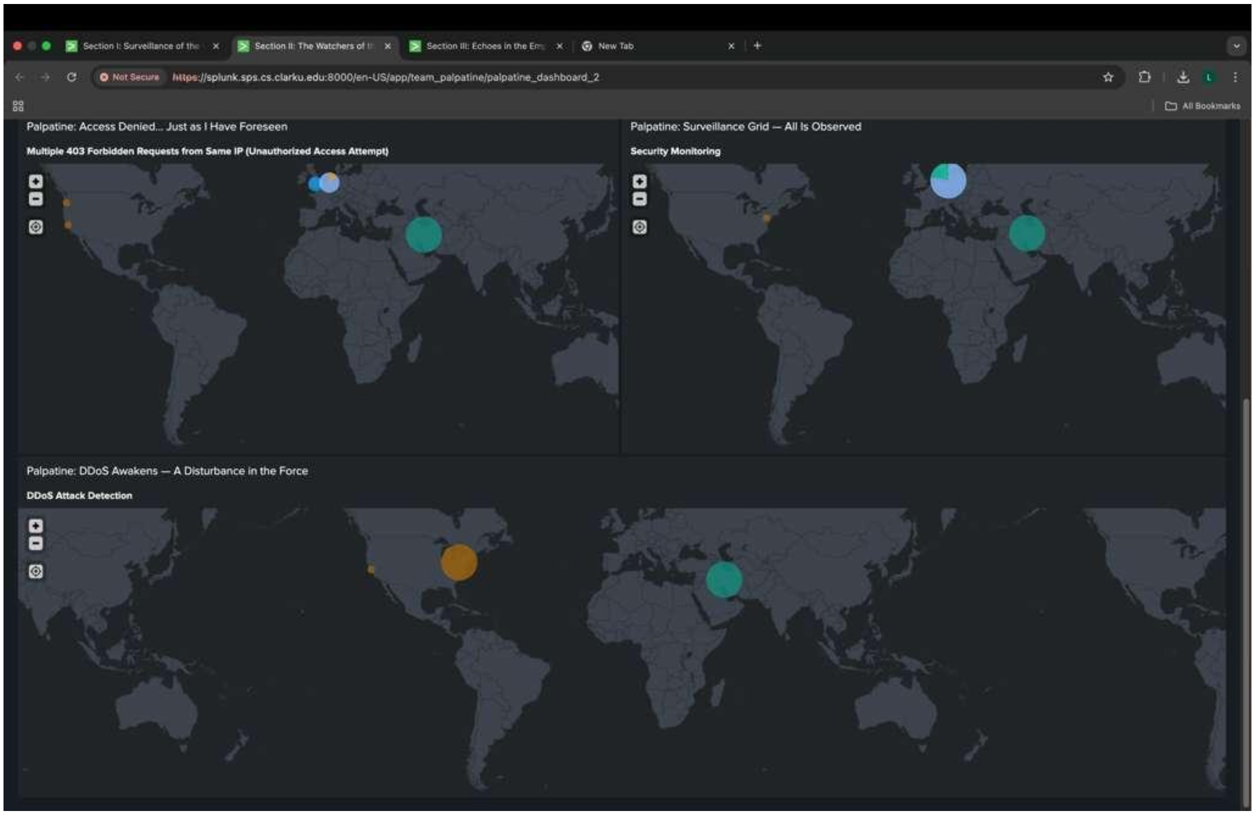
Time ⇕	Error Count ⇕	Average Error ⇕	Standard Deviation ⇕	Threshold ⇕
2019-01-26 10:00:00	7454	156.36082474226805	807.9931051888042	1772.3470351198764
2019-01-26 11:00:00	2786	156.36082474226805	807.9931051888042	1772.3470351198764

Palpatine: Droids in Disguise — OS Signature Breakdown

OS statistics for Access logs

Palpatine: Mapping the Empire — Reach Across the Systems

Geo Map of access log data.



Section I: Surveillance of the ×
Section II: The Watchers of th ×
Section III: Echoes in the Emp ×
New Tab ×
+
Not Secure
https://splunk.sps.cs.clarku.edu:8000/en-US/app/team_palpatine/palpatine_dashboard_2
All Bookmarks

Palpatine: Access Denied... Just as I Have Foreseen

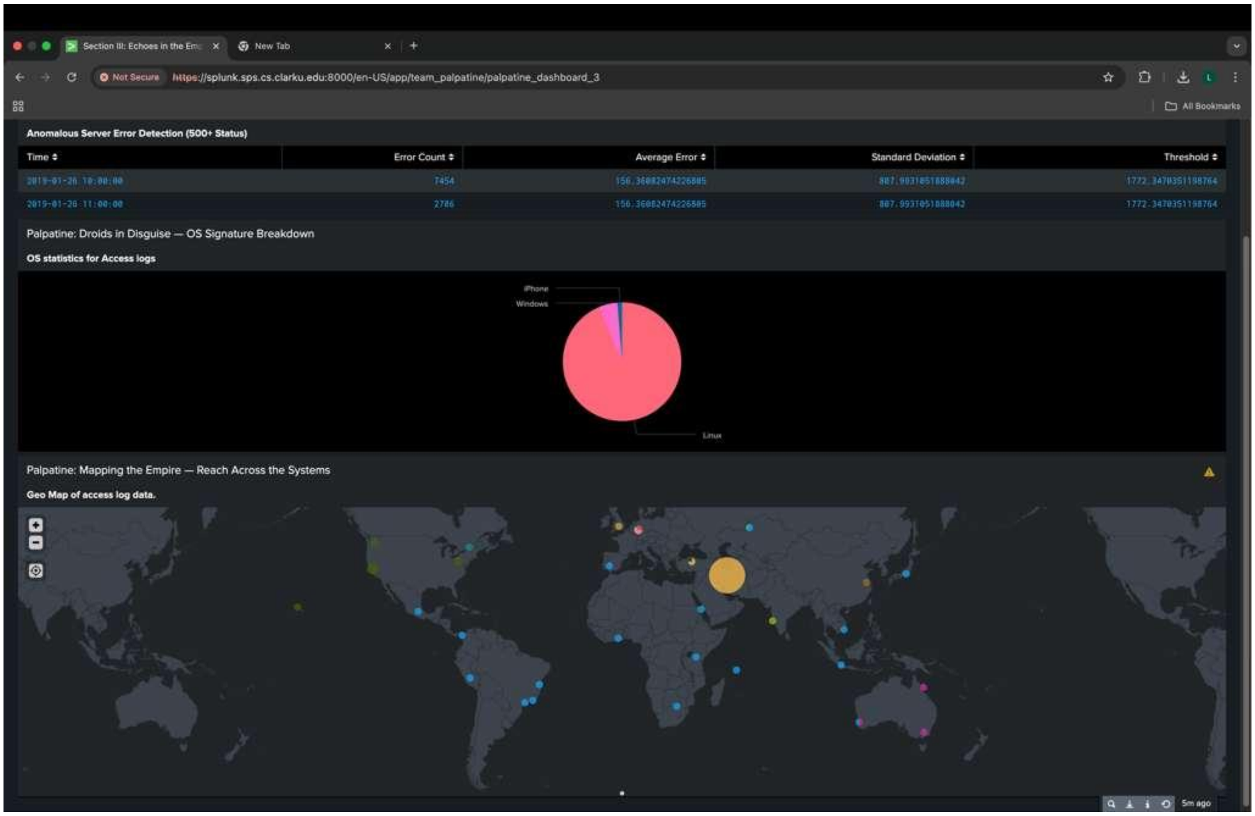
Multiple 403 Forbidden Requests from Same IP (Unauthorized Access Attempt)

Palpatine: Surveillance Grid — All Is Observed

Security Monitoring

Palpatine: DDoS Awakens — A Disturbance in the Force

DDoS Attack Detection


Section III: Echoes in the Em
New Tab
Not Secure
https://splunk.sps.cs.clarku.edu:8000/en-US/app/team_palpatine/palpatine_dashboard_3
All Bookmarks

Anomalous Server Error Detection (500+ Status)

Time ⬍	Error Count ⬍	Average Error ⬍	Standard Deviation ⬍	Threshold ⬍
2019-01-26 10:00:00	7454	156.36082474226805	807.9931051888042	1772.3470351198764
2019-01-26 11:00:00	2786	156.36082474226805	807.9931051888042	1772.3470351198764

Palpatine: Droids in Disguise — OS Signature Breakdown

OS statistics for Access logs

Palpatine: Mapping the Empire — Reach Across the Systems

Geo Map of access log data.