

April 27, 2021



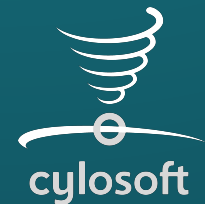
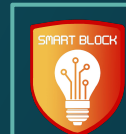
Smart Block:

Web Attack Tracking Software

Paul Degnan | Megan Hill | Andrew Marek
Jamie Sampson | Emily Young

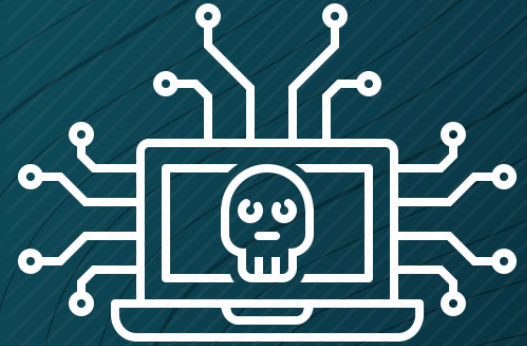
Andrew Dakin (Cylosoft)

Doug Jacobson



Problem Statement

- Malicious actors accessing Cylosoft's websites
- Wastes time and resources trying to block IPs manually
- Create a program to address these issues



Overview

File
Watcher

Security

Demo

Database

Website

Demo

Conclusion

Project Solution

- Web attack detection through visualization
- Modifiable configuration settings
- Easy to set up
- Extensible



Overview

File
Watcher

Security

Demo

Database

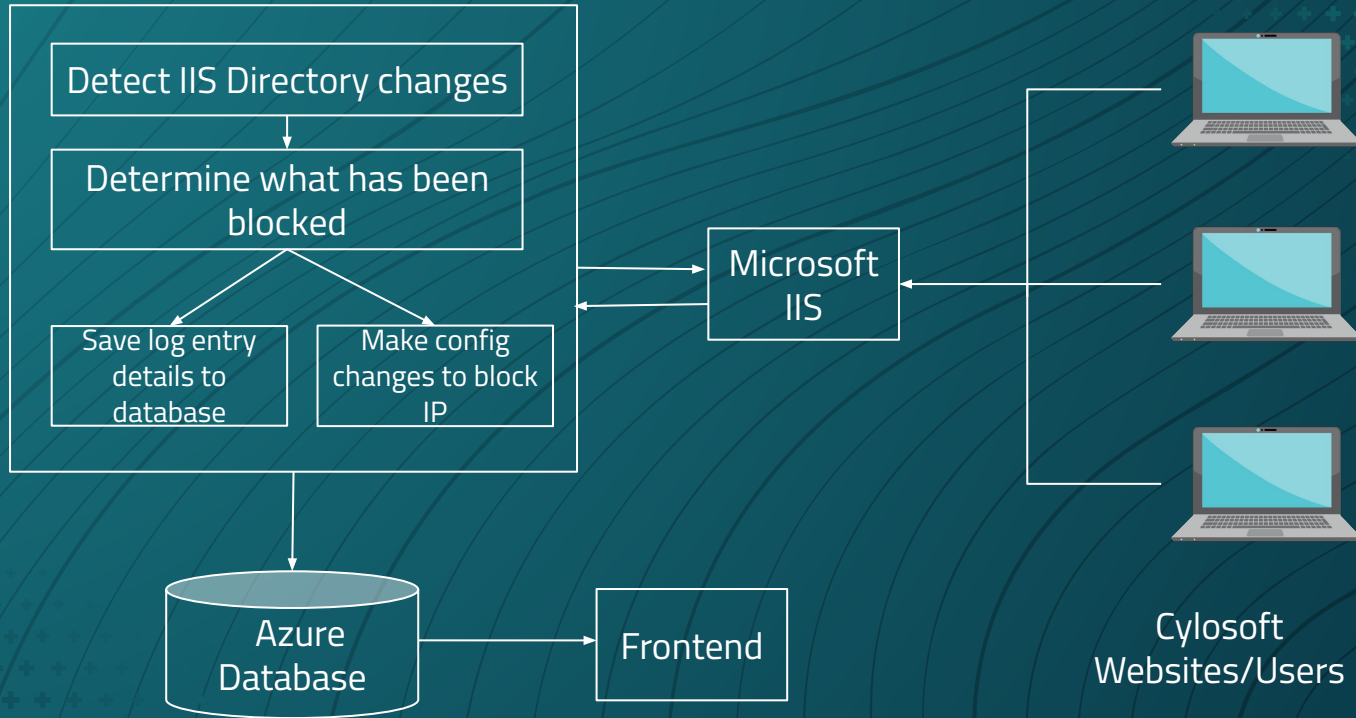
Website

Demo

Conclusion

System Diagram

Smart Block



Overview

File
Watcher

Security

Demo

Database

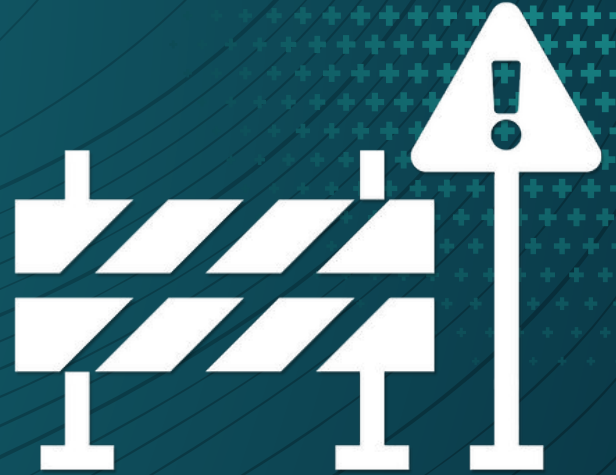
Website

Demo

Conclusion

Constraints

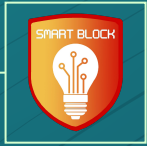
- Must use IIS
- Must use .NET Core App
- Connection to real IIS software
- Connection to Client's pre-existing database



Requirements

- Configuration to an IIS site ID
- Process multiple sites on a single server
- Web UI to display metrics
- Block and Unblock Addresses



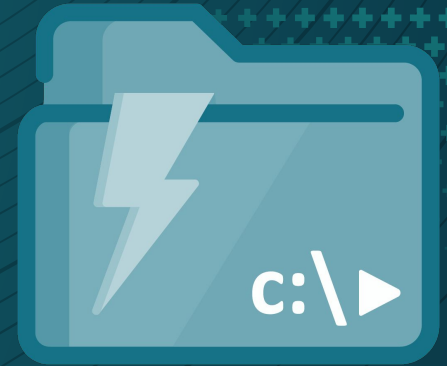


File Watcher

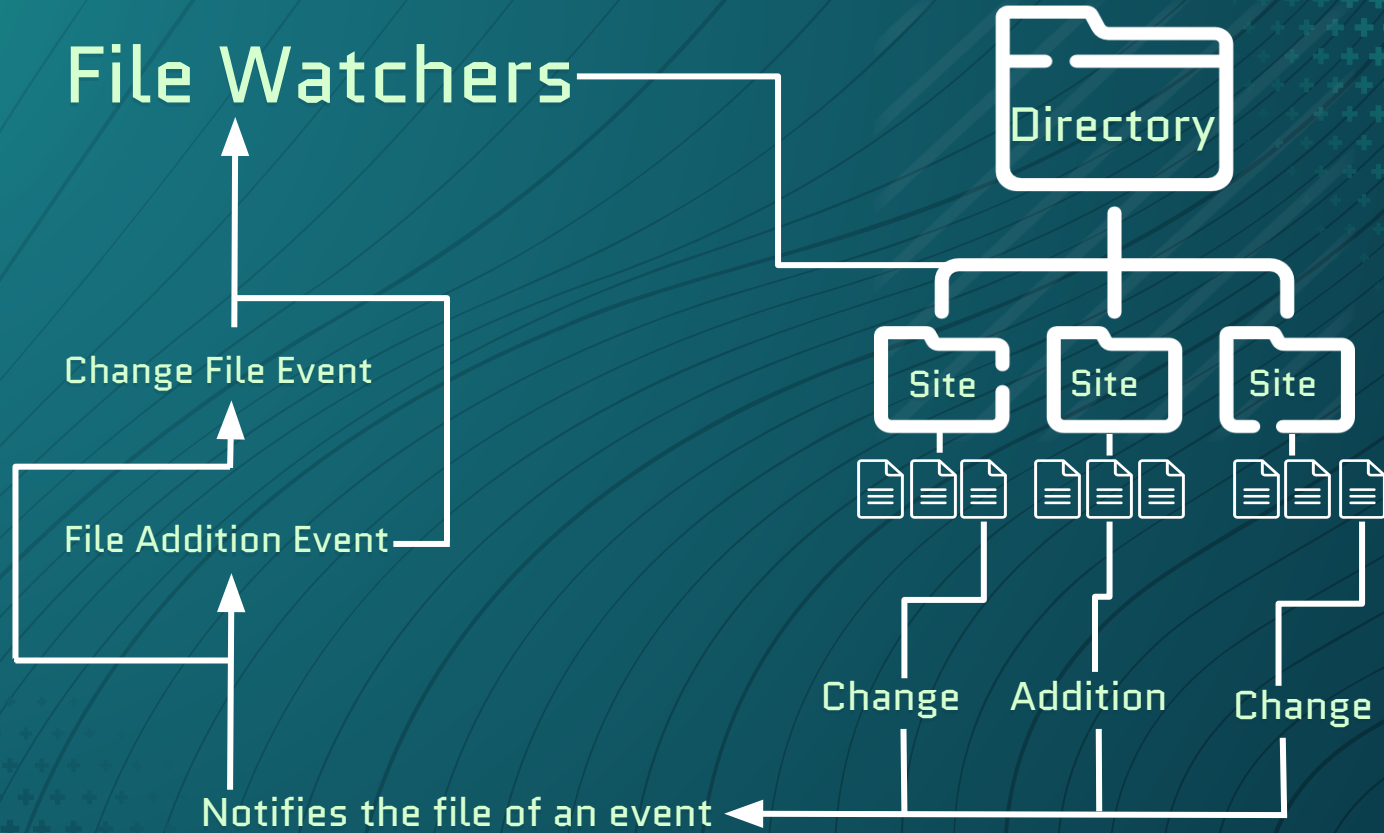
Paul Degnan

Background Information

- Assumptions
 - Parsing log/txt files.
 - IIS is providing correct, accurate content.
- Log Delivery
 - No control over what gets logged.
 - Updated in 15-20 second bursts.
 - Files located in a directory, with a subdirectory for each site.
 - New file for each day per site.
- Goal
 - To replace a human hand reading each and every file.



File Watchers



Overview

File
Watcher

Security

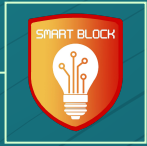
Demo

Database

Website

Demo

Conclusion



Security

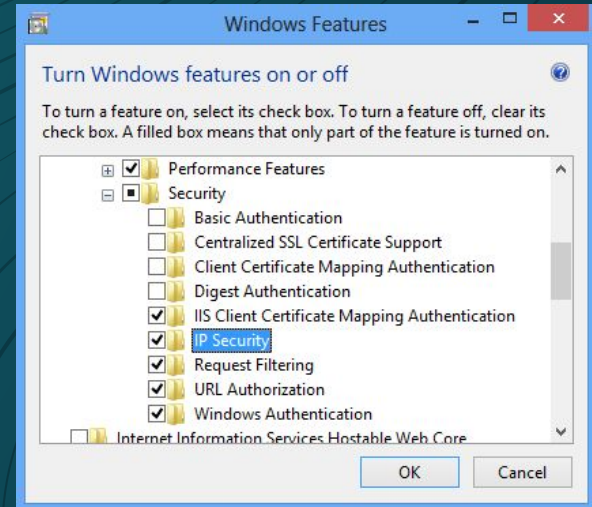
Jamie Sampson



Microsoft IIS

Microsoft IIS APIs

- Setup
- IP Address & Domain Restrictions
- Filtering Rules
- URL Sequences
- Dynamic IP Restrictions



Overview

File
Watcher

Security

Demo

Database

Website

Demo

Conclusion

File View Help

Connections

- DESKTOP-FKAGAS4 (DESKTOP)
 - Application Pools
 - Sites
 - Default Web Site
 - App_Data
 - aspnet_client

IP Address and Domain Restrictions

Use this feature to restrict or grant access to Web content based on IP addresses or domain names. Set the restrictions in order of priority.

Group by: No Grouping

Mode	Requestor	Entry Type
Deny	104.223.94.210	Inherited

File View Help

Connections

- DESKTOP-FKAGAS4 (DESKTOP)
 - Application Pools
 - Sites
 - Default Web Site

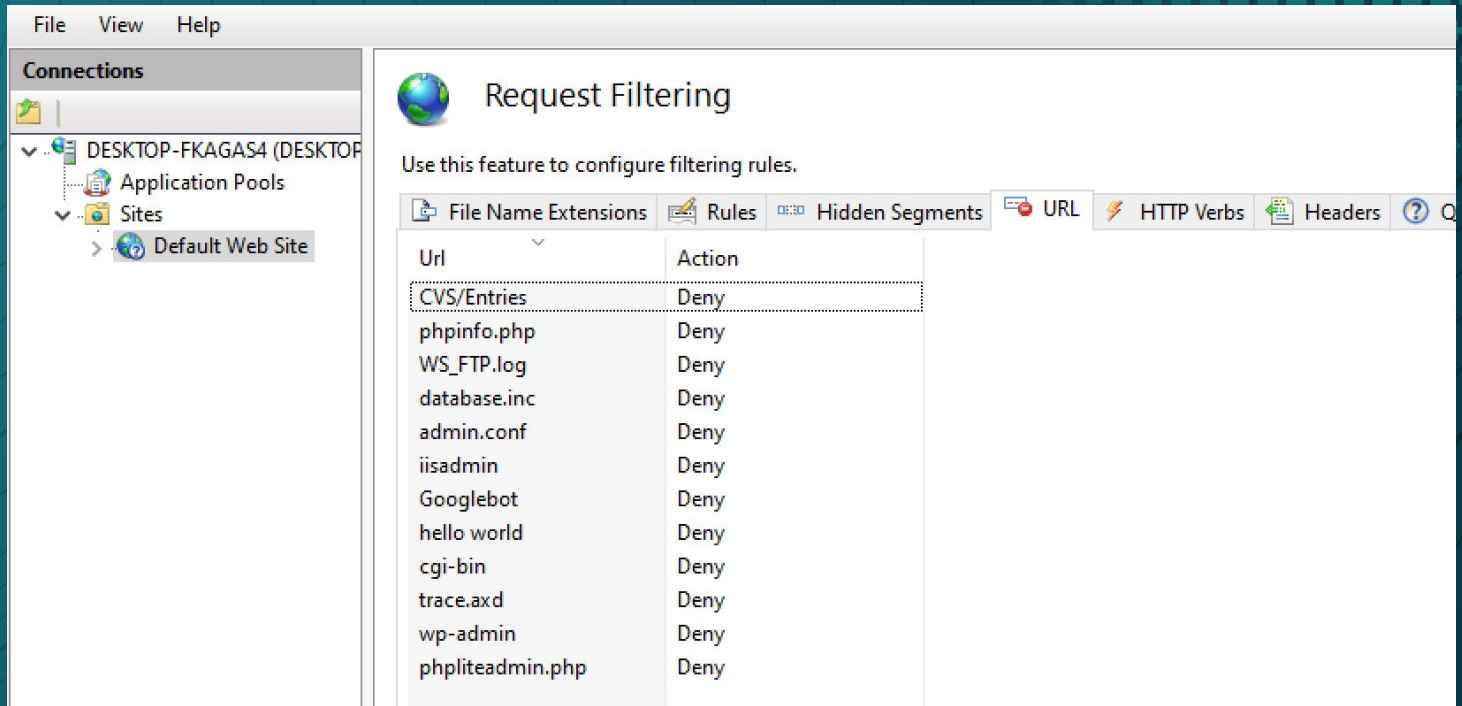
Request Filtering

Use this feature to configure filtering rules.

File Name Extensions Rules Hidden Segments URL HTTP Verbs Headers Query Strings

Name	Scan	Applies To	Deny Strings
testFilter	Query string, Url		wordpress, dino

IIS: Request Filtering - URL Sequences



The screenshot shows the IIS Request Filtering console. The left pane shows the server hierarchy: Desktop-FKAGAS4 (DESKTOP) > Sites > Default Web Site. The main pane is titled "Request Filtering" and contains a table of filtering rules. The "URL" tab is selected, showing a list of URL sequences and their corresponding actions, all of which are set to "Deny".

Url	Action
CVS/Entries	Deny
phpinfo.php	Deny
WS_FTP.log	Deny
database.inc	Deny
admin.conf	Deny
iisadmin	Deny
Googlebot	Deny
hello world	Deny
cgi-bin	Deny
trace.axd	Deny
wp-admin	Deny
phpliteadmin.php	Deny

Overview

File
Watcher

Security

Demo

Database

Website

Demo

Conclusion

IIS: Dynamic IP Restrictions

Dynamic IP Restriction Settings

Deny IP Address based on the number of concurrent requests

Maximum number of concurrent requests:

Deny IP Address based on the number of requests over a period of time

Maximum number of requests:

Time Period (in milliseconds):

Enable Logging Only Mode

Overview

File
Watcher

Security

Demo

Database

Website

Demo

Conclusion

JSON Site Settings

```
{  
  "SiteName": "Default Web Site",  
  "LogFolderName": "W01",  
  "SiteId": 1,  
  "SiteDynamicSecurity": {  
    "EnableProxyMode": true,  
    "LogOnlyMode": true,  
    "EnableDenyByConcurrentRequests": false,  
    "MaxConcurrentRequests": 20,  
    "EnableDenyByRequestRate": true,  
    "MaxRequests": 35,  
    "RequestInterval": 200  
  },  
}
```

```
{  
  "Names": [  
    "Test Web Site",  
    "Default Web Site",  
    "Default Values"  
  ]  
}
```

```
"SiteDenyUrl": {  
  "UrlSequences": [  
    "hello world",  
    "cgi-bin",  
    "CVS/Entries",  
    "phpinfo.php",  
    "WS_FTP.log",  
    "trace.axd",  
  ]  
}
```

```
"SiteRequestFiltering": {  
  "EnableScanUrl": true,  
  "EnableScanQueryString": true,  
  "FilterName": "testFilter",  
  "DenyStrings": [  
    "wordpress",  
    "dino"  
  ]  
},
```


Technical Challenges

- Handling duplicate entries
- Choosing which settings to include



```
2021-04-02 11:36:35.8872 SmartBlock.IpSecurity not adding, ip already exists: 104.223.94.210
2021-04-02 11:36:35.9224 SmartBlock.IpSecurity IpSecurityCollection
2021-04-02 11:36:35.9224 SmartBlock.IpSecurity 104.223.94.210
```

Overview

File
Watcher

Security

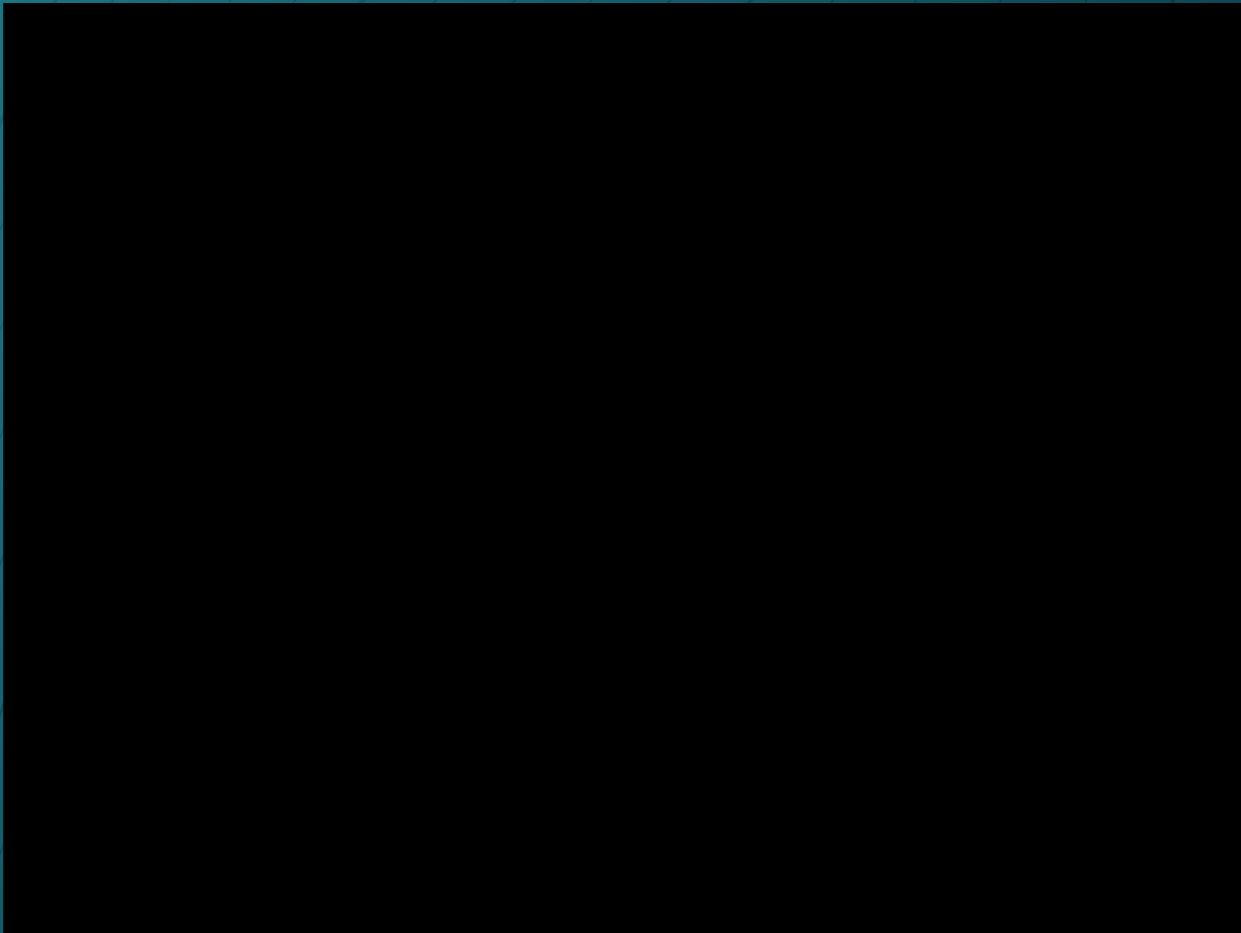
Demo

Database

Website

Demo

Conclusion



Overview

File
Watcher

Security

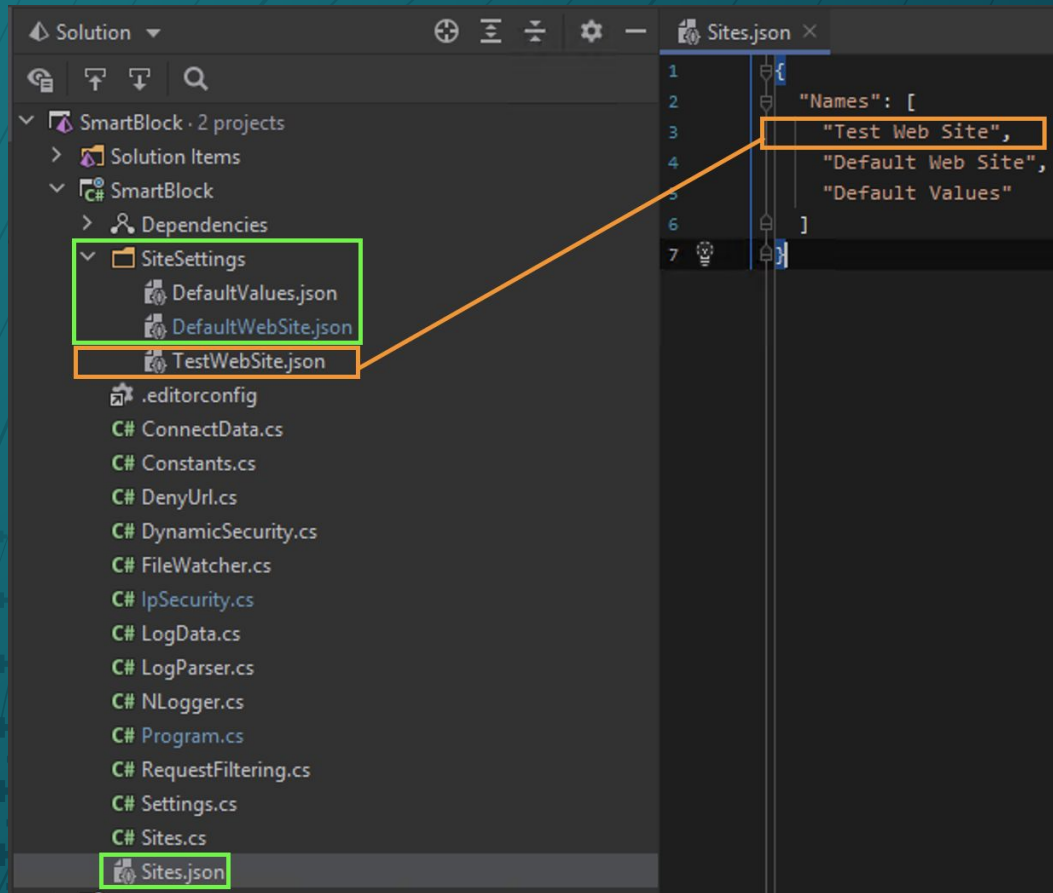
Demo

Database

Website

Demo

Conclusion



Overview

File
Watcher

Security

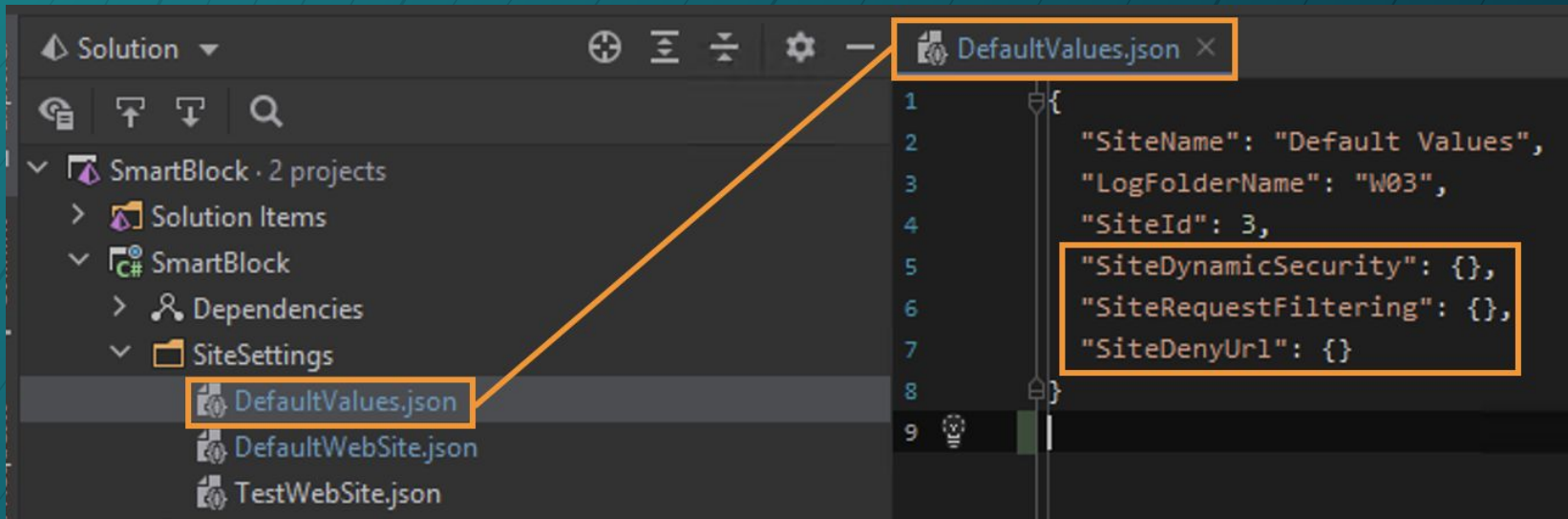
Demo

Database

Website

Demo

Conclusion



Overview

File
Watcher

Security

Demo

Database

Website

Demo

Conclusion

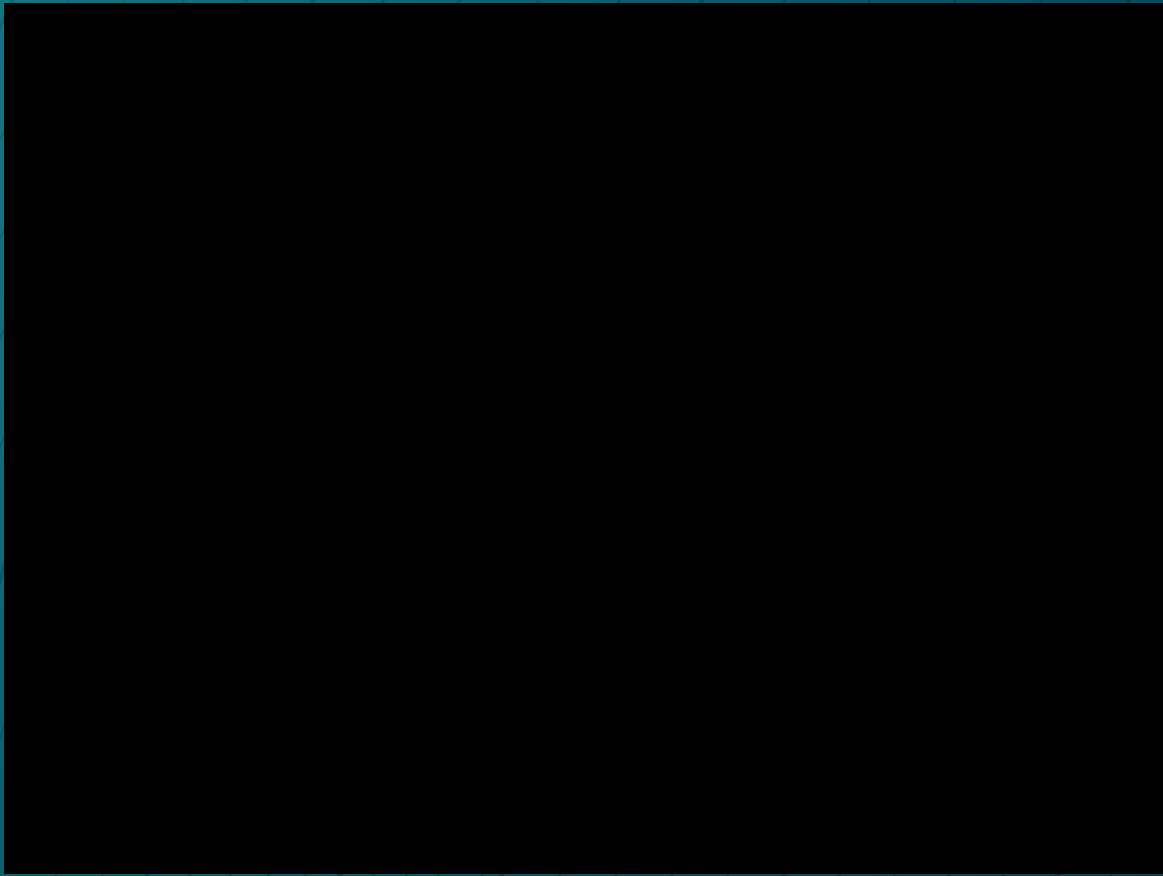
```
DefaultWebSite.json ×
1 {
2   "SiteName": "Default Web Site",
3   "LogFolderName": "W01",
4   "SiteId": 1,
5   "SiteDynamicSecurity": {
6     "EnableProxyMode": true,
7     "LogOnlyMode": true,
8     "EnableDenyByConcurrentRequests": false,
9     "MaxConcurrentRequests": 42,
10    "EnableDenyByRequestRate": true,
11    "MaxRequests": 35,
12    "RequestInterval": 500
13  },
14  "SiteRequestFiltering": {
15    "EnableScanUrl": true,
16    "EnableScanQueryString": true,
17    "FilterName": "testFilter",
18    "DenyStrings": [
19      "wordpress",
20      "dino"
21    ]
22  },
23  "SiteDenyUrl": {
24    "UrlSequences": [
25      "hello world",
26      "cgi-bin",
27      "CVS/Entries",
28      "phpinfo.php",
29      "MS_FTP.log",
30      "trace.axd",
31      "database.inc",
32      "admin.conf",
33      "wp-admin",
34      "iisadmin",
35      "phpliteadmin.php",
36      "Googlebot"
37    ]
38  }
39 }
40
```

```
DefaultWebSite.json ×
1 {
2   "SiteName": "Default Web Site",
3   "LogFolderName": "W01",
4   "SiteId": 1,
```

```
DefaultWebSite.json x
1 {
2   "SiteName": "Default Web Site",
3   "LogFolderName": "W01",
4   "SiteId": 1,
5   "SiteDynamicSecurity": {
6     "EnableProxyMode": true,
7     "LogOnlyMode": true,
8     "EnableDenyByConcurrentRequests": false,
9     "MaxConcurrentRequests": 42,
10    "EnableDenyByRequestRate": true,
11    "MaxRequests": 35,
12    "RequestInterval": 500
13  },
14  "SiteRequestFiltering": {
15    "EnableScanUrl": true,
16    "EnableScanQueryString": true,
17    "FilterName": "testFilter",
18    "DenyStrings": [
19      "wordpress",
20      "dino"
21    ],
22  },
23  "SiteDenyUrl": {
24    "UrlSequences": [
25      "hello world",
26      "cgi-bin",
27      "CVS/Entries",
28      "phpinfo.php",
29      "WS_FTP.log",
30      "trace.axd",
31      "database.inc",
32      "admin.conf",
33      "wp-admin",
34      "iisadmin",
35      "phpliteadmin.php",
36      "GoogLebot"
37    ]
38  }
39 }
40
```

```
"DenyStrings": [
  "wordpress",
  "dino"
]
```

```
"UrlSequences": [
  "hello world",
  "cgi-bin",
  "CVS/Entries",
  "phpinfo.php",
  "WS_FTP.log",
  "trace.axd",
  "database.inc",
  "admin.conf",
  "wp-admin",
  "iisadmin",
  "phpliteadmin.php",
  "GoogLebot"
]
```



Overview

File
Watcher

Security

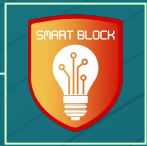
Demo

Database

Website

Demo

Conclusion



Database

Emily Young

Database

- Connecting to Database
 - VPN
 - VDI
 - Remote Desktop
- Using Database
- Database Migrations



Overview

File
Watcher

Security

Demo

Database

Website

Demo

Conclusion



```
2020-09-06 13:09:41 10.10.3.1 GET / - 443 - 18.212.7.196 Mozilla/5.0+(Macintosh;+Intel+Mac
+OS+X+10_15_4)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/83.0.4103.61+Safari/537.36 -
302 0 0 33
```

Overview

File
Watcher

Security

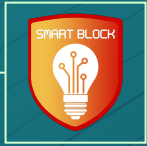
Demo

Database

Website

Demo

Conclusion



Website

Megan Hill

Backend



KNEX.JS



Overview

File
Watcher

Security

Demo

Database

Website

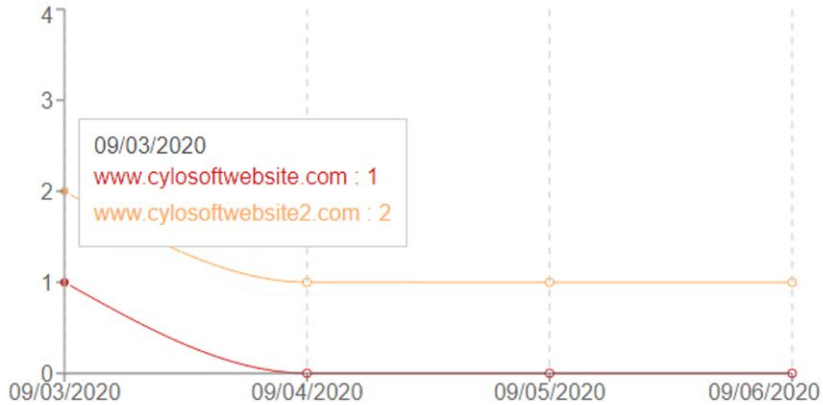
Demo

Conclusion

Frontend

sIP	cIP	Cloudfla...	csHost	csUriStem	Date and Time
10.10.2.1	162.158.15...	77.88.5.67	www.cylosoftwebsite.com	/BVMODULES/Themes/Foundation4+Responsive/ProductTemplates/B...	2020-09-03T01:40:34.000Z
10.10.2.1	300.132.15...	77.88.5.67	www.cylosoftwebsite2.com	/BVMODULES/Themes/Foundation4+Responsive/ProductTemplates/B...	2020-09-03T01:40:34.000Z
10.10.2.1	300.132.15...	77.88.5.67	www.cylosoftwebsite2.com	/BVMODULES/Themes/Foundation4+Responsive/ProductTemplates/B...	2020-09-03T12:40:34.000Z
10.10.2.1	300.132.15...	77.88.5.67	www.cylosoftwebsite2.com	/BVMODULES/Themes/Foundation4+Responsive/ProductTemplates/B...	2020-09-06T01:40:34.000Z
10.10.2.1	300.132.15...	77.88.5.67	www.cylosoftwebsite2.com	/BVMODULES/Themes/Foundation4+Responsive/ProductTemplates/B...	2020-09-05T01:40:34.000Z

Data



Overview

File
Watcher

Security

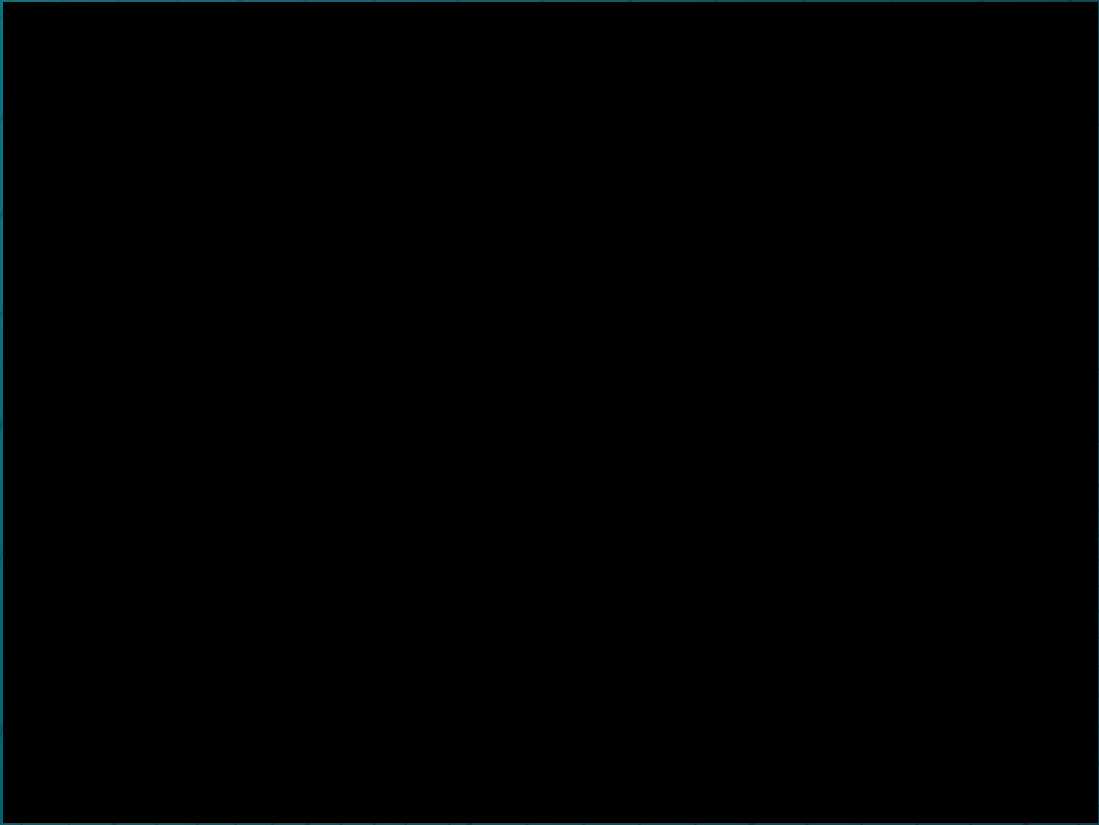
Demo

Database

Website

Demo

Conclusion



Overview

File
Watcher

Security

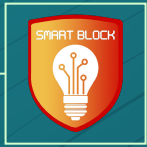
Demo

Database

Website

Demo

Conclusion



Conclusion

Lessons Learned

- New Technologies
- Being able to define requirements
- How to get reliable IP addresses



Overview

File
Watcher

Security

Demo

Database

Website

Demo

Conclusion

Future Development

- Deploy on Production Server
- Change default config file to meet needs
- Any future blocking rules



Overview

File
Watcher

Security

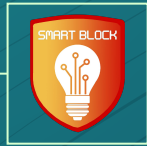
Demo

Database

Website

Demo

Conclusion



Thank You!

Questions?

Team Leader:
Andrew Marek
(sdmay21-17@iastate.edu)

Team: sdmay21-17