Week in the Life of a DFIR

Elizabeth Schweinsberg
@bethlogic

Motivation

What my friends think I do

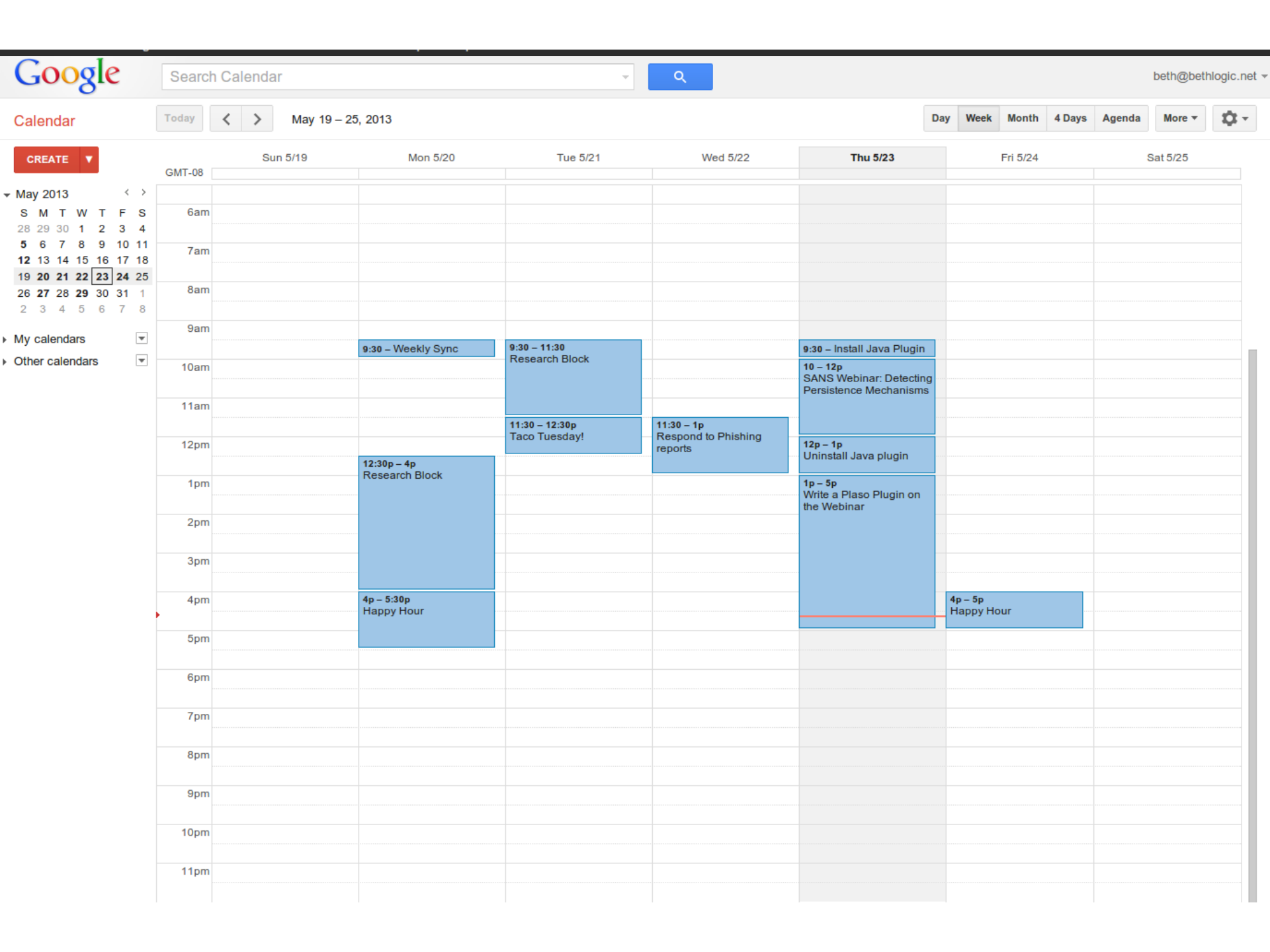
What my mom thinks I do

What IT thinks I do

What my cat thinks I do

What I think I do

What I really do


Google
Search Calendar
beth@bethlogic.net
Calendar
Today
May 19 – 25, 2013
Day
Week
Month
4 Days
Agenda
More
CREATE
May 2013
S M T W T F S
28 29 30 1 2 3 4
5 6 7 8 9 10 11
12 13 14 15 16 17 18
19 20 21 22 23 24 25
26 27 28 29 30 31 1
2 3 4 5 6 7 8
My calendars
Other calendars
GMT-08
Sun 5/19
Mon 5/20
Tue 5/21
Wed 5/22
Thu 5/23
Fri 5/24
Sat 5/25
6am
7am
8am
9am
10am
11am
12pm
1pm
2pm
3pm
4pm
5pm
6pm
7pm
8pm
9pm
10pm
11pm
9:30 – Weekly Sync
9:30 – 11:30
Research Block
11:30 – 12:30p
Taco Tuesday!
11:30 – 1p
Respond to Phishing reports
9:30 – Install Java Plugin
10 – 12p
SANS Webinar: Detecting Persistence Mechanisms
12p – 1p
Uninstall Java plugin
1p – 5p
Write a Plaso Plugin on the Webinar
12:30p – 4p
Research Block
4p – 5:30p
Happy Hour
4p – 5p
Happy Hour

Monday 9:30

Weekly Sync meeting with partner teams

It was a quiet weekend... too quiet...

Monday 10:23

Snort alert for a Java Exploit on a MacBook...

in Prague

- Have a local Tech remove drive from laptop and connect to your server for imaging
  - Calculate hashes
  - Copy drive to filer
  - Check hashes
- Start log2timeline massive processing on the image and have a beer with co-workers before heading home

Tuesday

- Read twitter and catch up on blogs - Research IDXs for today's case
  - A great blog tells you all you need to do!
  - http://computer-forensics.sans.org/blog/2013/02/16/idx-sample-file-malware
- Head to lunch for Taco Tuesday
- Investigate the image from yesterday
  - Get an IDX parser from your research -- Perl or Python?
  - Use the timeline, grep, and icat to extract the IDX files
  - Data reduction -- my timeline is 2GB! Where to begin?
    - Web history for that day
    - Process execution
    - Packet capture from the Snort alert
- Write a plaso plug in to make this easier next time

Tuesday, during NCIS:LA...

DNS Hijack Alert for your .fn cc TLD

Receive an alert from our 3rd party monitoring system that the DNS resolution our cc tld for Florin (.fn) has been redirected to a non-corporate site.

- Confirm that webfu.fn is not pointing to our page anymore
  - Grab a screenshot, check whois, and check dig to collect intel
- Get someone to redirect
- Work with your Domain Management company to contact the registry
- Give PR a heads up

Wednesday

- Bug the Domain Monitoring company to get a postmortem from the .fn registrar
- Respond to emails about reports of phishing
  - Get headers and look into the origins of the email
  - Search Google for reports
  - Reassure your coworkers that it’s standard spam and nothing targeted

Wednesday 13:43

Lost Laptop with Confidential Data

A financial analyst reports that her car was broken into while she was at dinner the night before and her work bag containing her work laptop, RSA token, and tablet with corporate data access were stolen.

- Get her to change her password, and revoke any other access like OAuth tokens
- Look at her account access for the last day -- no unusual locations
- Talk to her about confidential data and if she had any on her laptop
- Talk to the lawyers about what she reports

Thursday

- Install Java plugin for Firefox on Linux system
- Watch a SANS webcast -- Detecting Persistence Mechanisms
- Uninstall the Java plugin
- Write a plaso plugin inspired by SANS webcast

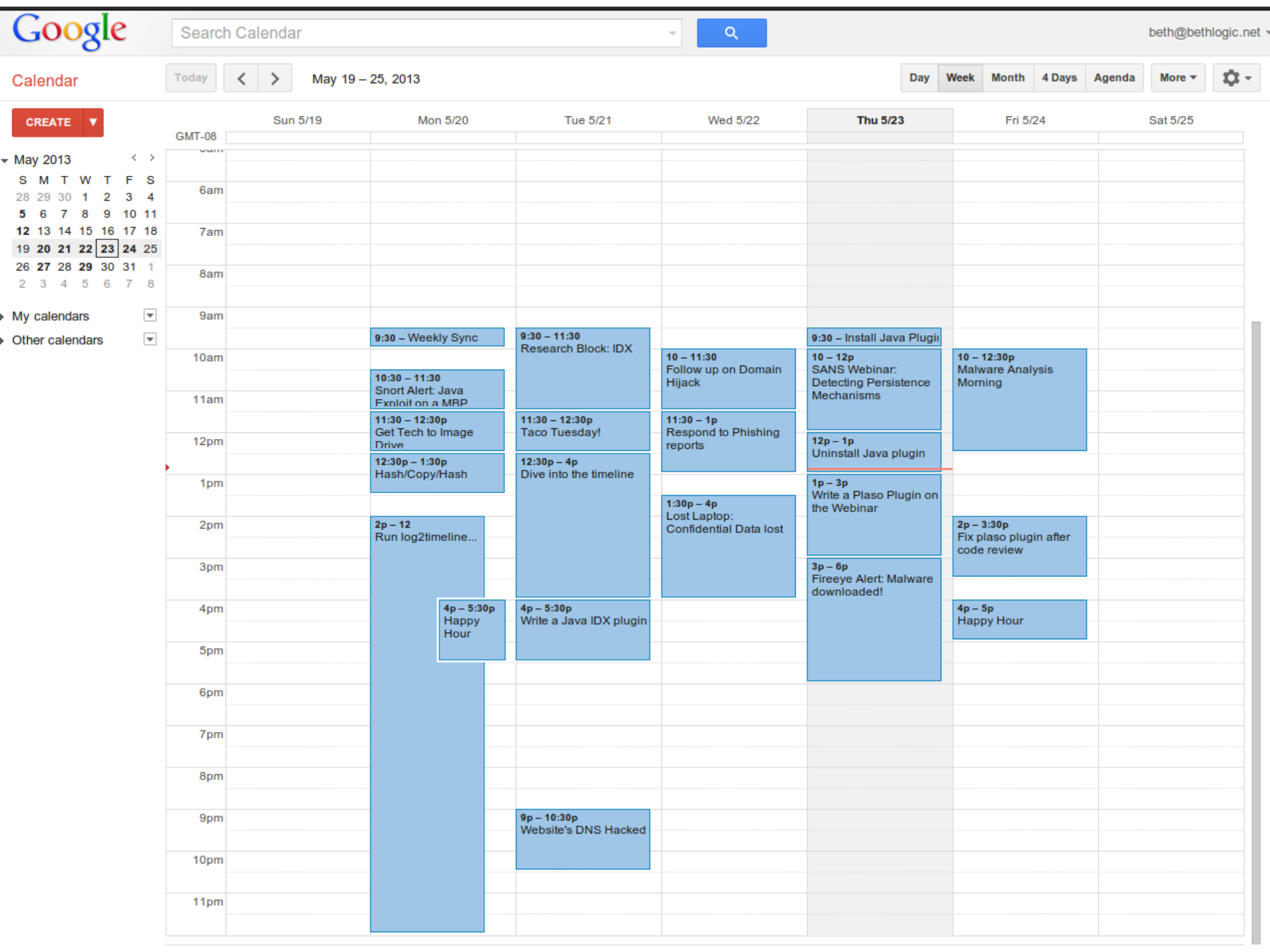
Thursday 15:07

Fireeye alert for a malicious file download

- Connect to GRR to investigate
- Run the Chrome History flow
- Find out there was more than one Chrome profile, so go back and run that flow on all the profiles
- Pull down Registry files and Windows Evtx files
- Run plaso on them for a timeline
- Catch the original website that redirected to the malicious one, see the file downloaded, and execution stopped by Bit9
- Feed the URLs to the Safe Browsing team, upload to VirusTotal

Friday

- Quick analysis of the binary -- it was just the dropper
  - Run the dropper in a sandbox and allow it to get the main file
  - Do some static and dynamic analysis to get the C2 info out
  - Write a Snort signature to detect the dropper and main file
- Finish the plaso plugin you started on Thursday...
- Have a beer with coworkers, and head out for a hopefully quiet weekend


Google
Search Calendar
beth@bethlogic.net
Calendar
Today
May 19 – 25, 2013
Day
Week
Month
4 Days
Agenda
More
CREATE
May 2013
S M T W T F S
28 29 30 1 2 3 4
5 6 7 8 9 10 11
12 13 14 15 16 17 18
19 20 21 22 23 24 25
26 27 28 29 30 31 1
2 3 4 5 6 7 8
My calendars
Other calendars
GMT-08
Sun 5/19
Mon 5/20
Tue 5/21
Wed 5/22
Thu 5/23
Fri 5/24
Sat 5/25
6am
7am
8am
9am
10am
11am
12pm
1pm
2pm
3pm
4pm
5pm
6pm
7pm
8pm
9pm
10pm
11pm
9:30 – Weekly Sync
10:30 – 11:30 Snort Alert: Java Exploit on a MBP
11:30 – 12:30p Get Tech to Image Drive
12:30p – 1:30p Hash/Copy/Hash
2p – 12 Run log2timeline...
4p – 5:30p Happy Hour
9:30 – 11:30 Research Block: IDX
11:30 – 12:30p Taco Tuesday!
12:30p – 4p Dive into the timeline
4p – 5:30p Write a Java IDX plugin
9p – 10:30p Website's DNS Hacked
10 – 11:30 Follow up on Domain Hijack
11:30 – 1p Respond to Phishing reports
1:30p – 4p Lost Laptop: Confidential Data lost
9:30 – Install Java Plugi
10 – 12p SANS Webinar: Detecting Persistence Mechanisms
12p – 1p Uninstall Java plugin
1p – 3p Write a Plaso Plugin on the Webinar
3p – 6p Fireeye Alert: Malware downloaded!
10 – 12:30p Malware Analysis Morning
2p – 3:30p Fix plaso plugin after code review
4p – 5p Happy Hour