Incident Response at Scale
Building a next generation SOC

Omer Cohen
@omercnet
Who?

- 15+ years Information Security experience
- Sr. Paranoid, Global IR Lead, Yahoo!
- Co-Founder, VP IR, IL-CERT
- ISACA CSX Task Force
- Licensed Skydiver, 996 jumps
Security Operations Center?
Security Operations Center in real life

http://securityreactions.tumblr.com/
205 days before detecting a security breach

Mandiant M-Trends® 2015
DATA BREACHES

DATA RECORDS LOST OR STOLEN IN FIRST SIX MONTHS OF 2015

245,919,393

ONLY 4% of breaches were "Secure Breaches" where encryption was used and the stolen data was rendered useless.

1,358,671 records lost or stolen every day
56,611 records every hour
943 records every minute
16 records every second

© BreachLevelIndex.com
Majority of any given SOC shift

http://securityreactions.tumblr.com/
Why?
Triaging a malware event

SIEM Alert
Triaging a malware event

SIEM Alert ->

Analyst collects information
20:33:29 [omer@sl흘 slow-lm:~] host contoso.com
contoso.com has address 64.4.6.100
contoso.com has address 65.55.39.10
contoso.com mail is handled by 10 mail.global.frontbridge.com.
20:33:33 [omer@sl꼼 slow-lm:~]
host contoso.com
contoso.com has address 64.4.6.100
contoso.com has address 65.55.39.10
contoso.com mail is handled by mail.global.frontbridge.com.
20:33:29 [omerc@sisterslow-lm:~] host contoso.com
Contoso.com has address 64.4.6.100
Contoso.com has address 65.55.39.10
Contoso.com mail is handled by 10 mail.global.frontbridge.com.
20:33:33 [omerc@sisterslow-lm:~]

D:\>ping -a 76.96.54.12
Pinging www4.comcast.net [76.96.54.12] with 32 bytes of data:
Reply from 76.96.54.12: bytes=32 time=93ms TTL=51
Reply from 76.96.54.12: bytes=32 time=7ms TTL=51
Reply from 76.96.54.12: bytes=32 time=7ms TTL=51
Reply from 76.96.54.12: bytes=32 time=7ms TTL=51
Ping statistics for 76.96.54.12:
   Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
   Minimum = 7ms, Maximum = 93ms, Average = 28ms
D:\>
Triaging a malware event

SIEM Alert ->

Analyst collects information ->

Analyst understands context
Triaging a malware event

SIEM Alert ->

   Analyst collects information ->

   Analyst understands context ->

   Analyst classifies incident
Figure 1—Intelligent Workflow

FIRE ALARM:
View alarm location on map.

Analyze P/TZ
camera #52 and
look for signs of
smoke and fire.

Are there signs of
smoke and fire?

Yes

No

Start ventilation
systems.

Are there signs of
smoke and fire?

Yes

No

Call FIRE
Department
(905-320-9569)
Notify them to come
in from the SOUTH
ENTRANCE and park
at 145 Bay Street.

Are there signs of
smoke and fire from
other cameras?

Yes

No

Launch map
to view other
cameras near
the alarm area.

Call SECURITY
(905-320-9510)
Tell them
to paint section C30 to C40.
If there are no clues,
security will have to stop
Fire Alarm manually from
control panel.

Are people in area?

Yes

No

Monitor spread of fire
from video cameras
around the area.
Determine which route is
safe for evacuation.

Call SECURITY
(905-320-9510) to
assist in evacuation.

Activate emergency
lighting, exit
safe route.

Activate alarm
area.

Monitor spread of
fire, and assist Fire
Department until
area is clear.

Step alarm
area.

Step ventilation
system.

Dove ESIF
lighting.

File full report for
investigative purposes.
Protect all recorded
video in system.

Are people in area?

Yes

No
**Figure 1—Intelligent Workflow**

1. **Fire Alarm:**
   - View alarm location on map.
   - Ask comms if smoke and fire.
   - Monitor spread of fire from video cameras around the area.
   - Determine which route is safe for evacuation.
   - Call Security Guard (605-555-1234) to assist in evacuation.
   - Activate emergency exit lighting, exit safe routes.
   - Activate alarm system.

2. **PTZ Camera:**
   - Ask comms signs of smoke and fire.
   - Are there signs of smoke and fire from other cameras?
   - Launch view cameras from all angles.

3. **Fire Suppression:**
   - Fire Suppression (FSD) leaves fire suppression system.
   - Notify them to come in from the SOUTH ENTRANCE and park at 145 Bay Street.
   - Call FIRE Department (111-222-3333). Notify them to come in from the SOUTH ENTRANCE and park at 145 Bay Street.
   - Monitor spread of fire from video cameras around the area.
   - Determine which route is safe for evacuation.
   - Call Security Guard (605-555-1234) to assist in evacuation.
   - Activate emergency exit lighting, exit safe routes.
   - Activate alarm system.

4. **First Responder Data:**
   - Confiscate Hardware
   - Investigate
   - Notify Management Team

5. **Data Breach:**
   - Data Breach Confirmed
   - Potential
   - Investigate
   - Notify Management Team
Triaging a malware event

SIEM Alert ->

  Analyst collects information ->

  Analyst understands context ->

  Analyst classifies incident ->

  Analyst opens ITSM re-image ticket
<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Request ID</td>
<td>REQ000000012394</td>
</tr>
<tr>
<td>Summary</td>
<td>ABC</td>
</tr>
<tr>
<td>Request Type</td>
<td>Standard</td>
</tr>
<tr>
<td>Notes</td>
<td></td>
</tr>
<tr>
<td>Impact</td>
<td>A-Minor/Localized</td>
</tr>
<tr>
<td>Urgency</td>
<td>B-Medium</td>
</tr>
<tr>
<td>Status*</td>
<td>Initiated</td>
</tr>
<tr>
<td>Category 1*</td>
<td>Lifecycle Services</td>
</tr>
<tr>
<td>Category 2</td>
<td>REAC</td>
</tr>
<tr>
<td>Category 3</td>
<td>Information Security</td>
</tr>
<tr>
<td>Requested By</td>
<td></td>
</tr>
<tr>
<td>Company</td>
<td>ABC</td>
</tr>
<tr>
<td>First Name</td>
<td>Sreenker</td>
</tr>
<tr>
<td>Middle Name</td>
<td></td>
</tr>
<tr>
<td>Last Name</td>
<td>Masekar</td>
</tr>
<tr>
<td>Phone Number</td>
<td>###</td>
</tr>
<tr>
<td>Email</td>
<td></td>
</tr>
<tr>
<td>Organization</td>
<td>Commercial Sector</td>
</tr>
<tr>
<td>Department</td>
<td></td>
</tr>
<tr>
<td>Requested For</td>
<td></td>
</tr>
<tr>
<td>Company</td>
<td>ABC</td>
</tr>
<tr>
<td>First Name</td>
<td>Sreenker</td>
</tr>
<tr>
<td>Middle Name</td>
<td></td>
</tr>
<tr>
<td>Last Name</td>
<td>Masekar</td>
</tr>
<tr>
<td>Phone Number</td>
<td>###</td>
</tr>
<tr>
<td>Email</td>
<td></td>
</tr>
<tr>
<td>Organization</td>
<td>Commercial Sector</td>
</tr>
<tr>
<td>Department</td>
<td></td>
</tr>
<tr>
<td>Location Information</td>
<td></td>
</tr>
<tr>
<td>Location Company*</td>
<td>ABC</td>
</tr>
<tr>
<td>Region</td>
<td>XXX</td>
</tr>
<tr>
<td>Site Group</td>
<td>XXX</td>
</tr>
<tr>
<td>Site</td>
<td>XXXXXX</td>
</tr>
<tr>
<td>Address</td>
<td>Pune, India</td>
</tr>
</tbody>
</table>
Triaging a malware event

SIEM Alert ->

Analyst collects information ->

Analyst understands context ->

Analyst classifies incident ->

Analyst opens ITSM re-image ticket ->

System re-image
Triaging a malware event

SIEM Alert ->

Analyst collects information ->

Analyst understands context ->

Analyst classifies incident ->

Analyst opens ITSM re-image ticket ->

System re-image ->

Incident closed
Forensics at Scale?
How?
Incident Response on a tight budget

http://securityreactions.tumblr.com/
Better junior analysts

- Junior Analysts have a steep learning curve
- Company specific play-books
- Senior analysts focus on investigations
Let's automate

OH: I don't have time to automate things because I'm too busy doing things that should be automated..
Automation overkill

http://securityreactions.tumblr.com/
Triaging a malware event

SIEM Alert
Triaging a malware event

SIEM Alert ->

Automagically collect endpoint information
Triaging a malware event

SIEM Alert ->

Automagically collect endpoint information ->

Automagically make a decision based on BU
Triaging a malware event

SIEM Alert ->

Automagically collect endpoint information ->

Automagically make a decision based on BU ->

Automagically classify incident
Triaging a malware event

SIEM Alert ->

Automagically collect endpoint information ->

Automagically make a decision based on BU ->

Automagically classify incident ->

Automagically open ITSM re-image ticket
How your team *SHOULD* respond to incidents

http://securityreactions.tumblr.com/
Triaging a malware event

SIEM Alert ->

Automagically collect endpoint information ->

Automagically make a decision based on BU ->

Automagically classify incident ->

Automagically open ITSM re-image ticket ->

System re-imaged
Triaging a malware event

SIEM Alert ->

Automagically collect endpoint information ->

Automagically make a decision based on BU ->

Automagically classify incident ->

Automagically open ITSM re-image ticket ->

System re-imaged ->

Incident closed
APIS
EVERYWHERE
Integrate APIs into Incident Response

- Endpoint information
  - Host Asset Management
  - HR Systems
Integrate APIs into Incident Response

Endpoint information
   - Host Asset Management
   - HR Systems

IOC Lookups
   - Threat Exchange
   - Virus Total
   - IOC Management Systems
ThreatExchange

Learn about threats. Share threat information back. Everybody becomes more secure.

Apply for the Beta

https://facebook.com/threatexchange
from pytx import ThreatIndicator
from pytx.vocabulary import ThreatType as tt
from pytx.vocabulary import Types as t

print ThreatIndicator.objects(threat_type=tt.COMPROMISED_CREDENTIAL,
type_=t.EMAIL_ADDRESS, fields=['indicator', 'passwords'])
Automatic e-Crime detection?

```json
{ 
  data: [ 
    { 
      indicator: "asalas881@gmail.com", 
      added_on: "2015-06-30T06:03:21+0000", 
      id: "911123668926498" 
    }, 
    { 
      indicator: "bergmanjonathan@gmail.com", 
      added_on: "2015-06-30T06:03:21+0000", 
      id: "7459282858867220" 
    }, 
    { 
      indicator: "bizwam@gmail.com", 
      added_on: "2015-06-30T06:03:21+0000", 
      id: "838301019552941" 
    }, 
    { 
      indicator: "apurv.jamaiyar@gmail.com", 
      added_on: "2015-06-30T06:03:21+0000", 
      id: "97156128906025" 
    }, 
    { 
      indicator: "axilrod@gmail.com", 
      added_on: "2015-06-30T06:03:21+0000", 
      id: "931651286899781" 
    }, 
  ] 
}
```
Automatic e-Crime detection?

```json
1 { 
2   data: [ 
3     
4       indicator: "asalas881@gmail.com",
5       added_on: "2015-06-30T06:03:21+0000",
6       id: "911123668926498"
7     },
8     
9       indicator: "bergmanjonathan@gmail.com",
10      added_on: "2015-06-30T06:03:21+0000",
11      id: "745922858867220"
12     },
13     
14       indicator: "bizwam@gmail.com",
15      added_on: "2015-06-30T06:03:21+0000",
16      id: "838301019552941"
17     },
18     
19       indicator: "apurv.jamaiyar@gmail.com",
20      added_on: "2015-06-30T06:03:21+0000",
21      id: "971561682906025"
22     },
23     
24       indicator: "axilrod@gmail.com",
25      added_on: "2015-06-30T06:03:21+0000",
26      id: "931651286899781"
27   ]
28 }
```
VirusTotal is a free service that analyzes suspicious files and URLs and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware.

By clicking 'Scan it!', you consent to our Terms of Service and allow VirusTotal to share this file with the security community. See our Privacy Policy for details.
```python
>>> import json
>>> import urllib
>>> url = 'https://www.virustotal.com/vapi/v2/ip-address/report'
>>> parameters = {'ip': '90.156.201.27', 'apikey': '-- YOUR API KEY --'}
>>> response = urllib.urlopen('%s%s' % (url, urllib.urlencode(parameters))).read()
>>> response_dict = json.loads(response)
>>> print response_dict
{u'response_code': 1,
 u'verbose_msg': u'IP address found in dataset',
 u'resolutions': [
   {u'last_resolved': u'2013-04-08 00:00:00', u'hostname': u'027.ru'},
   {u'last_resolved': u'2013-04-08 00:00:00', u'hostname': u'auto.rema-tiptop.ru'},
   {u'last_resolved': u'2013-04-08 00:00:00', u'hostname': u'catalog24de.ru'},
   {u'last_resolved': u'2013-04-08 00:00:00', u'hostname': u'club.velhod.ru'},
   {u'last_resolved': u'2013-04-08 00:00:00', u'hostname': u'danilova.pro'},
   ... continues ...
],
 u'detected_urls': [
   {u'url': u'http://027.ru/', u'positives': 2, u'total': 37, u'scan_date': u'2013-04-07 07:18:09'},
   ... continues ...
]}
```
Integrate APIs into Incident Response

- Communications
  - STOP USING EMAIL (least for full reports)
  - Incident Management Systems (not your SIEM)
  - Alerts on messaging systems (IM/hipchat/slack/whatsapp/etc.)
Integrate APIs into Incident Response

- **Communications**
  - STOP USING EMAIL (least for full reports)
  - Incident Management Systems (not your SIEM)
  - Alerts on messaging systems (IM/hipchat/slack/whatsapp/etc.)

- **Automate the response**
  - Open reimage tickets in ITSM
  - Send out incident digest reports
Benefits of automation
Benefits of automation
Benefits of automation

- Reduce triage time
- Reduce response time
- Ensure all tasks are completed
Thank you

omer@cohen.io

@omercnet