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.

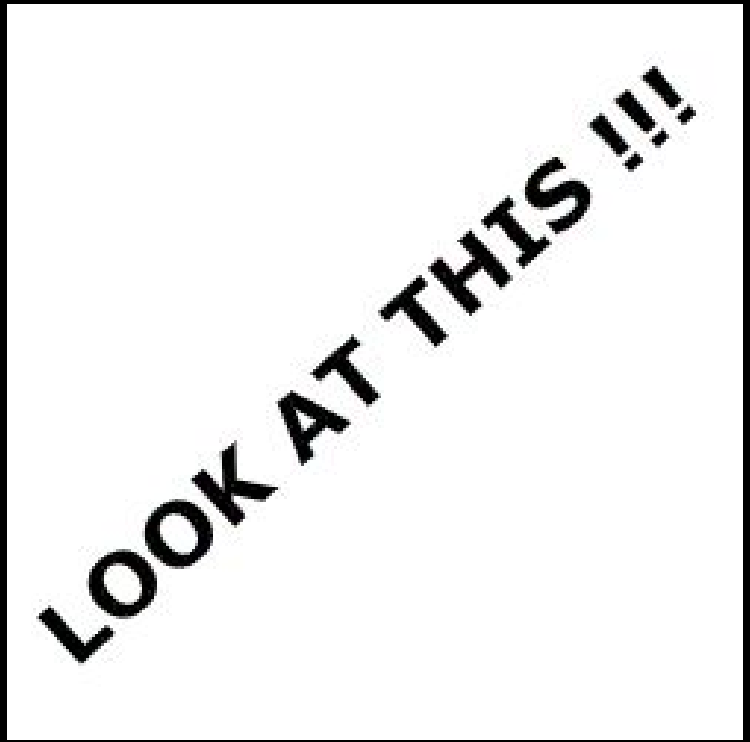
1,358,671 records lost or stolen **every day**

56,611 records **every hour**

943 records **every minute**

16 records **every second**

Majority of any given SOC shift



http://securityreactions.tumblr.com/

Why?


ArcSight Console 5.0.2.6904.3
Navigator
Viewer
Inspect/Edit
Audit Flag by User Snapshot
Object Activity Snapshot
LOGbinder SP Rule Firings
NITROVIEW
QRadar - Dashboard
Offenses - New Offense Count
Most Severe Offenses
Server Applications - Inbound Bytes
Events - Average Events Per Second
Most Recent Offenses
Server Applications - Outbound Bytes
System Summary
Logger Events
Threat Level
SIEM: Top 10 Events by Product
Unresolved Alarms vs Open Tickets
SIEM: Top 10 Event Categories

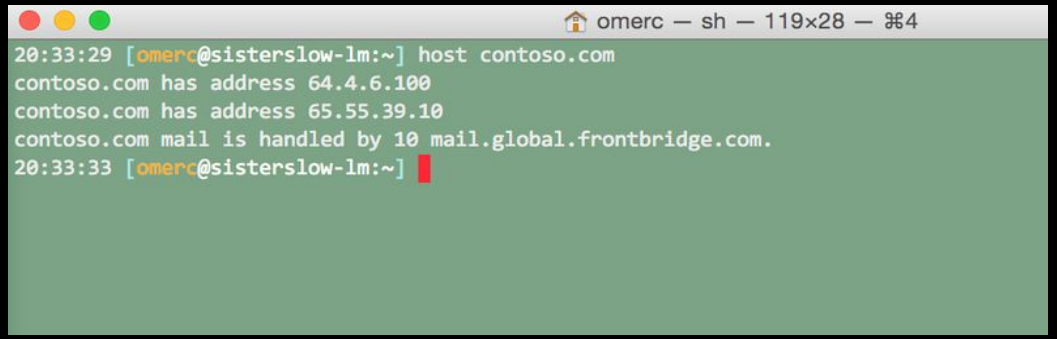
Triaging a malware event

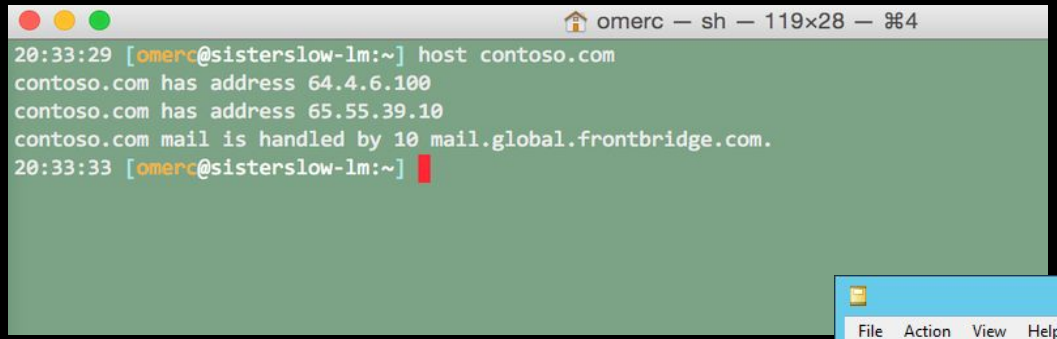
SIEM Alert

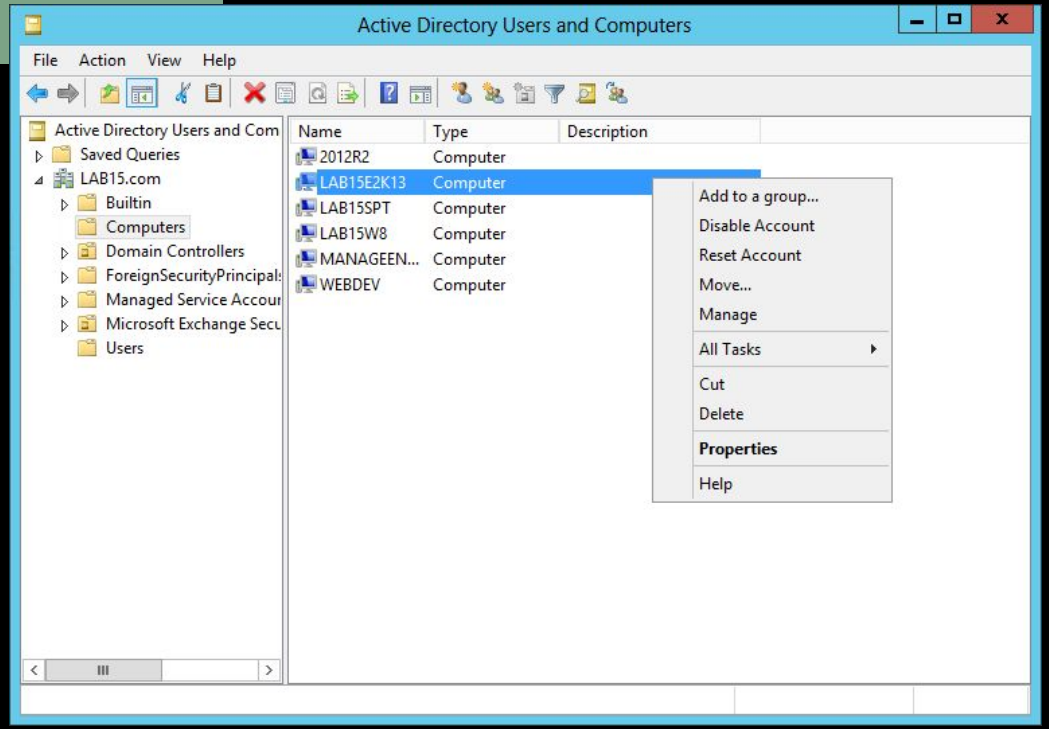
Triaging a malware event

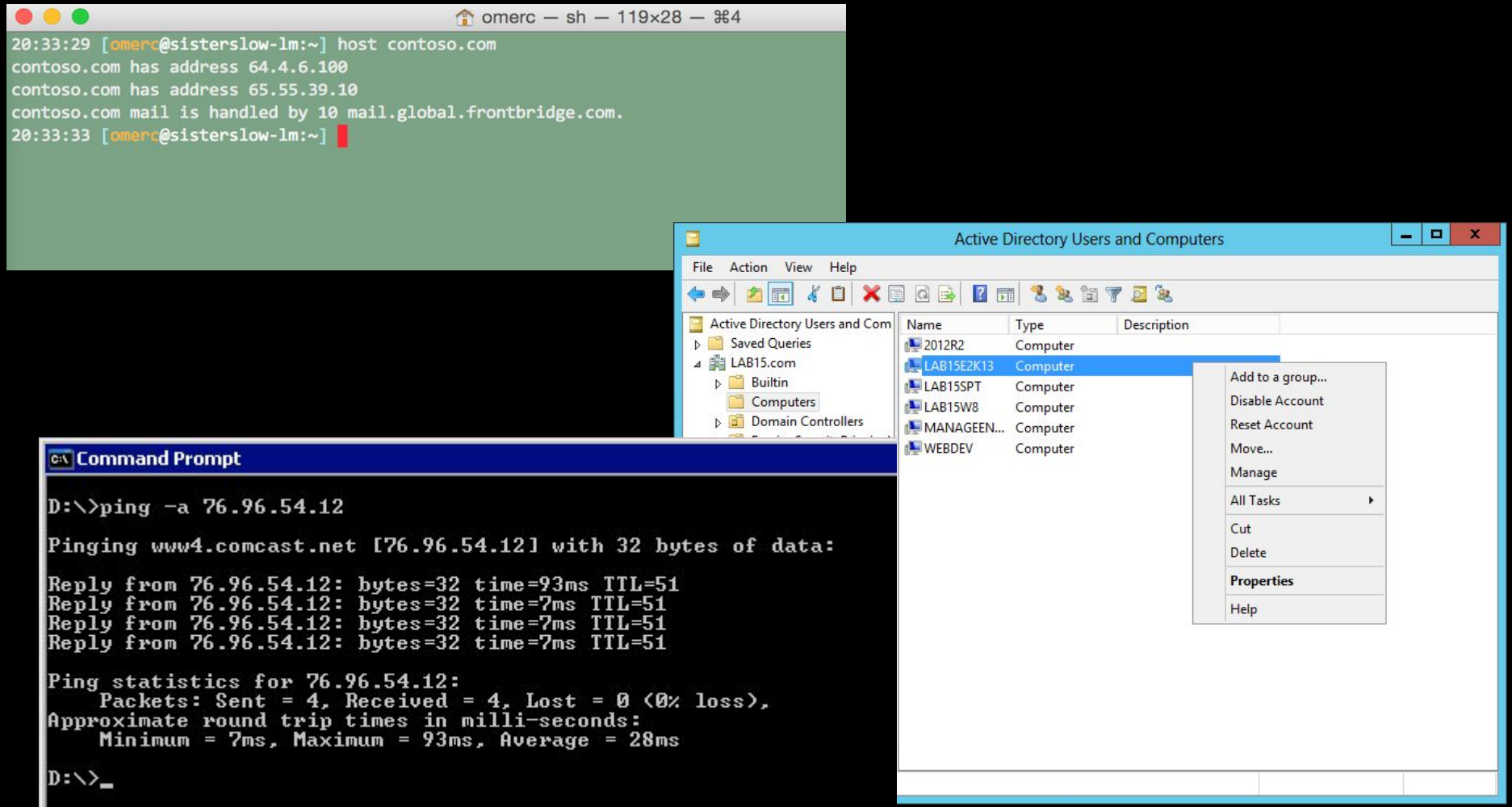
SIEM Alert ->

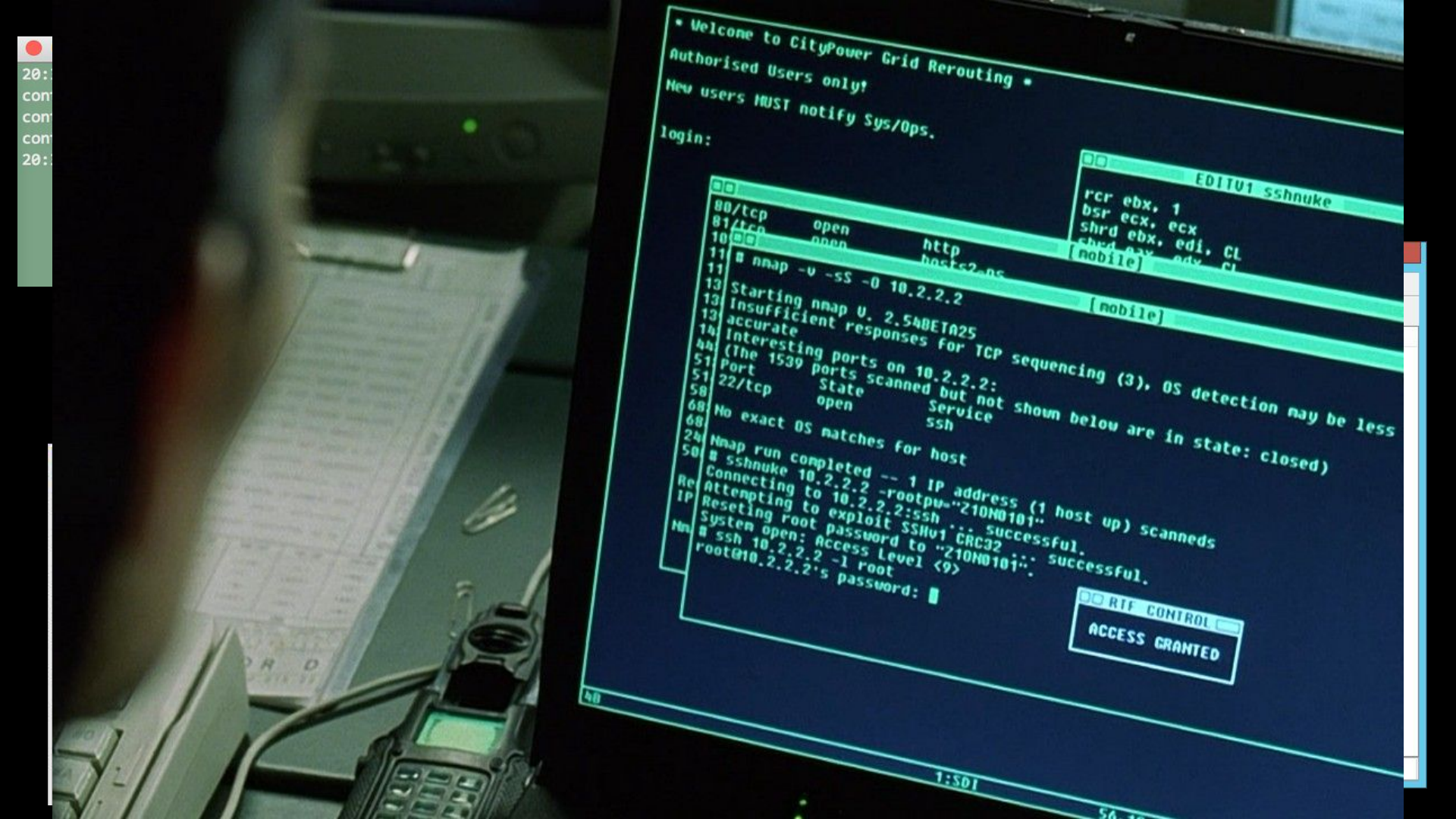
Analyst collects information


omerc — sh — 119×28 — ⌘4
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:~]


omerc — sh — 119×28 — ⌘4
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:~]


Active Directory Users and Computers
File
Action
View
Help
Active Directory Users and Com
Saved Queries
LAB15.com
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipal:
Managed Service Accour
Microsoft Exchange Secu
Users
Name
Type
Description
2012R2
Computer
LAB15E2K13
Computer
LAB15SPT
Computer
LAB15W8
Computer
MANAGEEN...
Computer
WEBDEV
Computer
Add to a group...
Disable Account
Reset Account
Move...
Manage
All Tasks
Cut
Delete
Properties
Help


omerc — sh — 119×28 — ⌘4
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:~]
Active Directory Users and Computers
File Action View Help
Active Directory Users and Com
Saved Queries
LAB15.com
Builtin
Computers
Domain Controllers
Name Type Description
2012R2 Computer
LAB15E2K13 Computer
LAB15SPT Computer
LAB15W8 Computer
MANAGEEN... Computer
WEBDEV Computer
Add to a group...
Disable Account
Reset Account
Move...
Manage
All Tasks
Cut
Delete
Properties
Help
Command Prompt
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:\>


* Welcome to CityPower Grid Rerouting *
Authorised Users only!
New users MUST notify Sys/Ops.
login:
EDIT V1 sshnuke
rcr ebx, 1
bsr ecx, ecx
shrd ebx, edi, CL
[mobile]
80/tcp open http
81/tcp open
10
11
13
14
44
51
58
68
24
50
nmap -v -sS -O 10.2.2.2
Starting nmap V. 2.54BETA25
Insufficient responses for TCP sequencing (3), OS detection may be less accurate
Interesting ports on 10.2.2.2:
(The 1539 ports scanned but not shown below are in state: closed)
Port State Service
22/tcp open ssh
No exact OS matches for host
Nmap run completed -- 1 IP address (1 host up) scanned
sshnuke 10.2.2.2 -rootpw="Z1ON0101"
Connecting to 10.2.2.2:ssh ... successful.
Attempting to exploit SSHv1 CRC32 ... successful.
Resetting root password to "Z1ON0101".
System open: Access Level <9>
ssh 10.2.2.2 -l root
root@10.2.2.2's password:
RIF CONTROL
ACCESS GRANTED
1:SDI

Triaging a malware event

SIEM Alert ->

Analyst collects information ->

Analyst understands context

Triaging a malware event

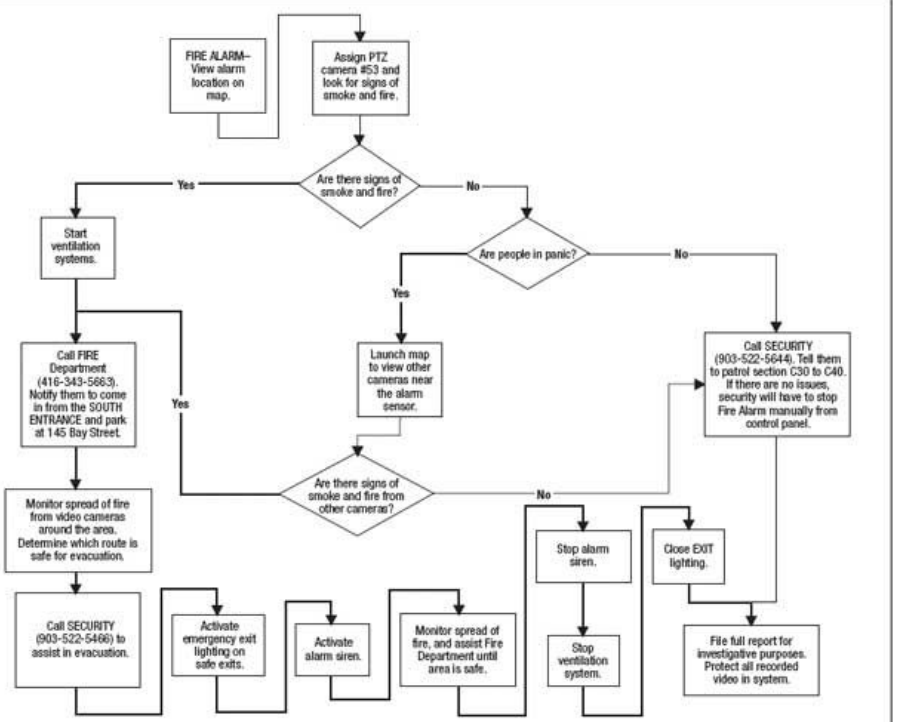
SIEM Alert ->

Analyst collects information ->

Analyst understands context ->

Analyst classifies incident

Figure 1—Intelligent Workflow



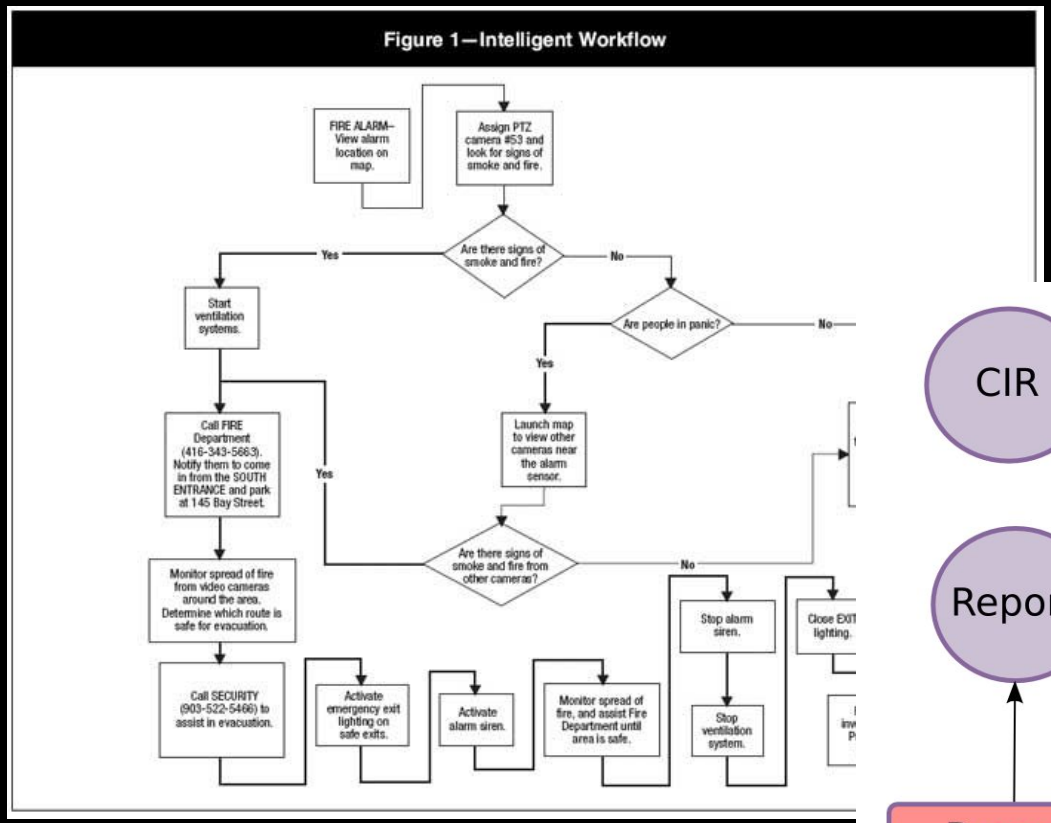
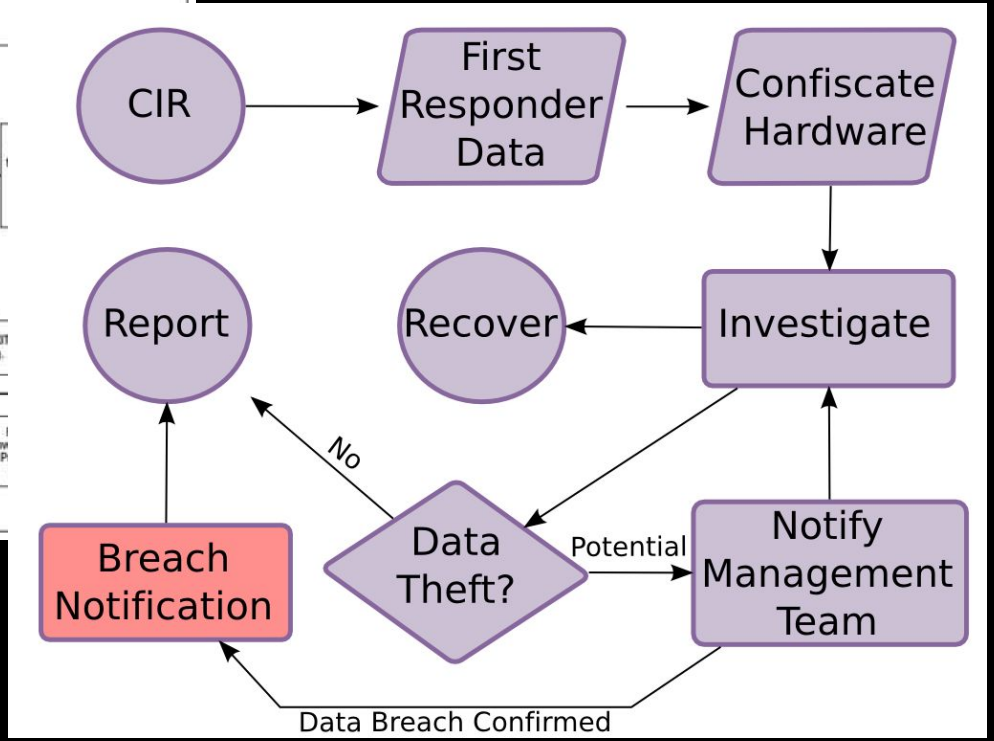


Figure 1—Intelligent Workflow
FIRE ALARM– View alarm location on map.
Assign PTZ camera #53 and look for signs of smoke and fire.
Are there signs of smoke and fire?
Yes
No
Start ventilation systems.
Are people in panic?
No
Yes
Call FIRE Department (416-343-5663). Notify them to come in from the SOUTH ENTRANCE and park at 145 Bay Street.
Launch map to view other cameras near the alarm sensor.
Yes
Are there signs of smoke and fire from other cameras?
No
Monitor spread of fire from video cameras around the area. Determine which route is safe for evacuation.
Stop alarm siren.
Call SECURITY (903-522-5466) to assist in evacuation.
Activate emergency exit lighting on safe exits.
Activate alarm siren.
Monitor spread of fire, and assist Fire Department until area is safe.
Stop ventilation system.


CIR
First Responder Data
Confiscate Hardware
Report
Recover
Investigate
No
Data Theft?
Potential
Notify Management Team
Breach Notification
Data Breach Confirmed

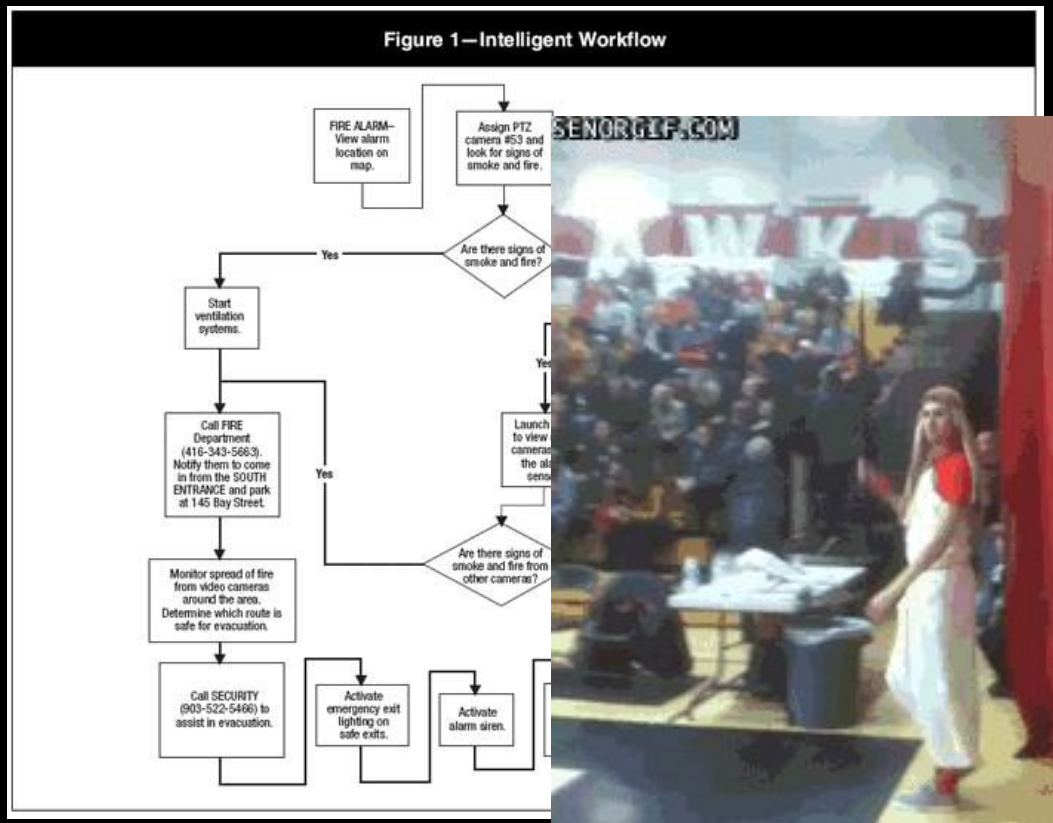
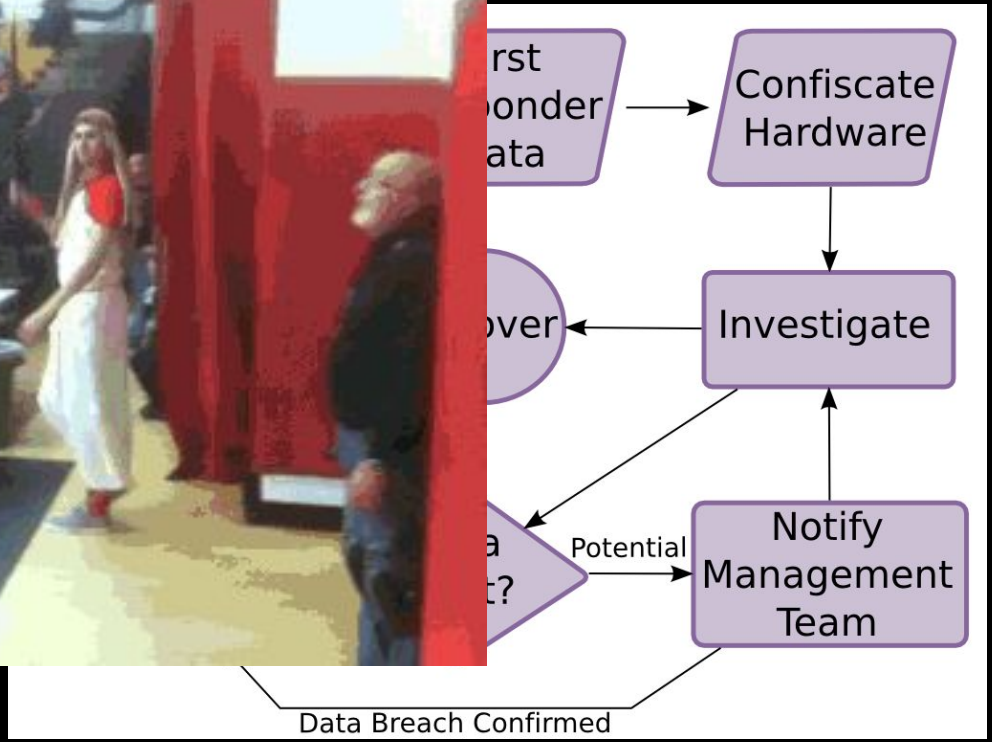


Figure 1—Intelligent Workflow
FIRE ALARM– View alarm location on map.
Assign PTZ camera #53 and look for signs of smoke and fire.
Are there signs of smoke and fire?
Yes
Start ventilation systems.
Call FIRE Department (416-343-5663). Notify them to come in from the SOUTH ENTRANCE and park at 145 Bay Street.
Yes
Monitor spread of fire from video cameras around the area. Determine which route is safe for evacuation.
Are there signs of smoke and fire from other cameras?
Call SECURITY (903-522-5466) to assist in evacuation.
Activate emergency exit lighting on safe exits.
Activate alarm siren.

SENORGIF.COM


rst
onder
ata
Confiscate Hardware
Investigate
over
a
t?
Potential
Notify Management Team
Data Breach Confirmed

Triaging a malware event

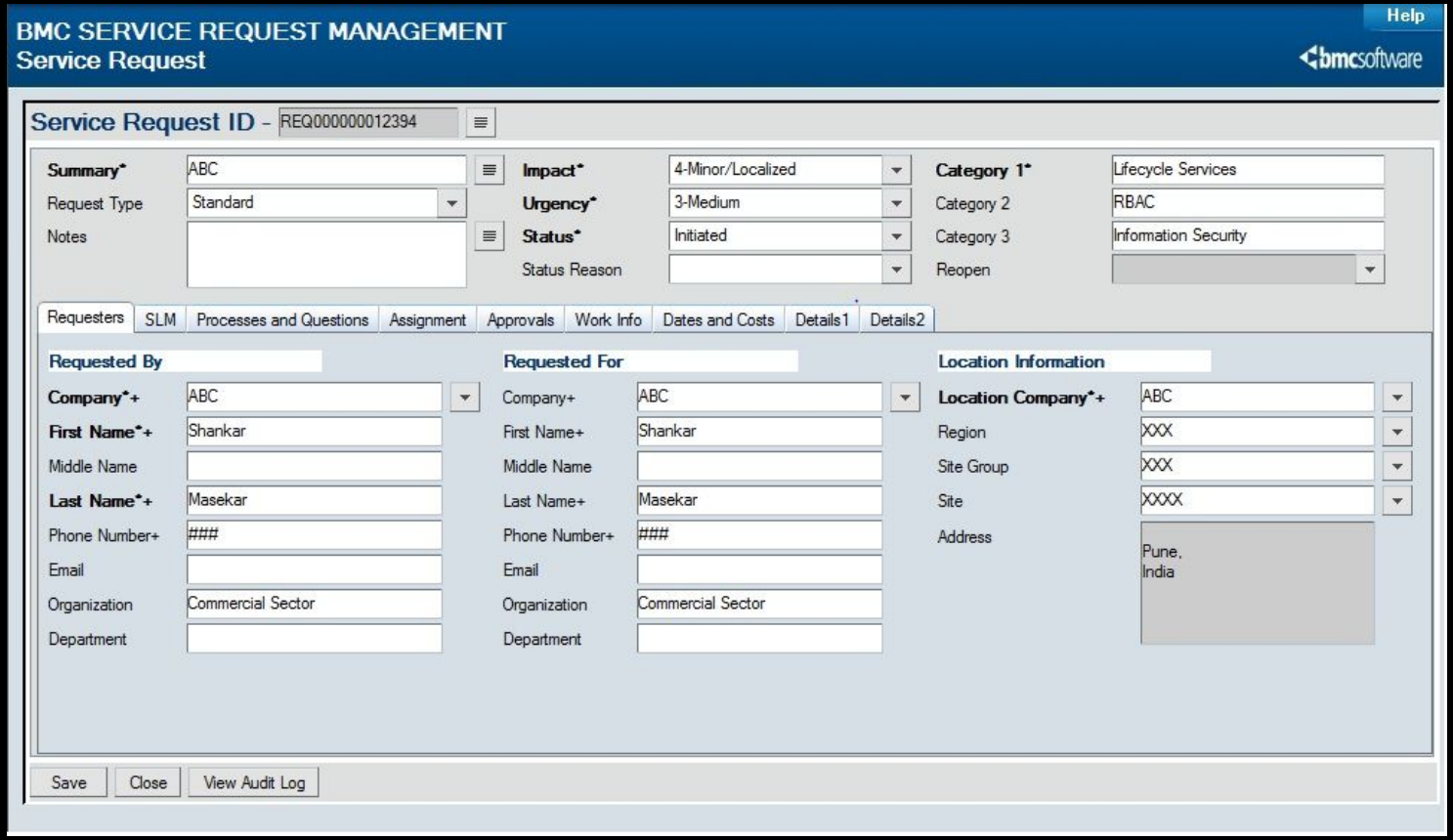
SIEM Alert ->

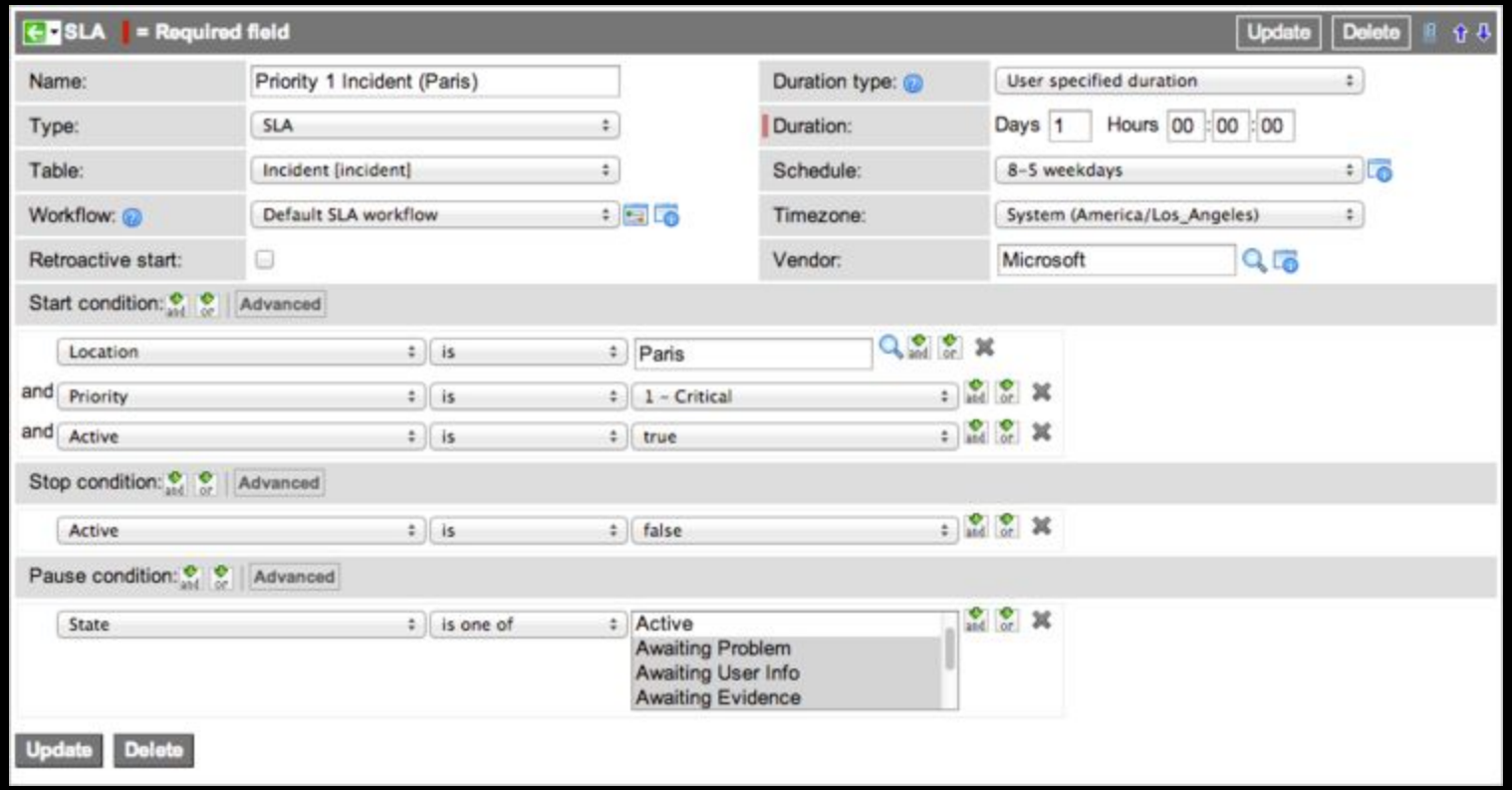
Analyst collects information ->

Analyst understands context ->

Analyst classifies incident ->

Analyst opens ITSM re-image ticket


BMC SERVICE REQUEST MANAGEMENT
Service Request
Help
bmcsoftware
Service Request ID - REQ000000012394
Summary* ABC
Request Type Standard
Notes
Impact* 4-Minor/Localized
Urgency* 3-Medium
Status* Initiated
Status Reason
Category 1* Lifecycle Services
Category 2 RBAC
Category 3 Information Security
Reopen
Requesters SLM Processes and Questions Assignment Approvals Work Info Dates and Costs Details1 Details2
Requested By
Company*+ ABC
First Name*+ Shankar
Middle Name
Last Name*+ Masekar
Phone Number+ ###
Email
Organization Commercial Sector
Department
Requested For
Company+ ABC
First Name+ Shankar
Middle Name
Last Name+ Masekar
Phone Number+ ###
Email
Organization Commercial Sector
Department
Location Information
Location Company*+ ABC
Region XXX
Site Group XXX
Site XXXX
Address Pune, India
Save
Close
View Audit Log


SLA
= Required field
Update
Delete
Name:
Priority 1 Incident (Paris)
Type:
SLA
Table:
Incident [incident]
Workflow:
Default SLA workflow
Retroactive start:
Duration type:
User specified duration
Duration:
Days 1 Hours 00 00 00
Schedule:
8-5 weekdays
Timezone:
System (America/Los_Angeles)
Vendor:
Microsoft
Start condition:
Advanced
Location is Paris
and Priority is 1 - Critical
and Active is true
Stop condition:
Advanced
Active is false
Pause condition:
Advanced
State is one of
Active
Awaiting Problem
Awaiting User Info
Awaiting Evidence
Update
Delete

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?

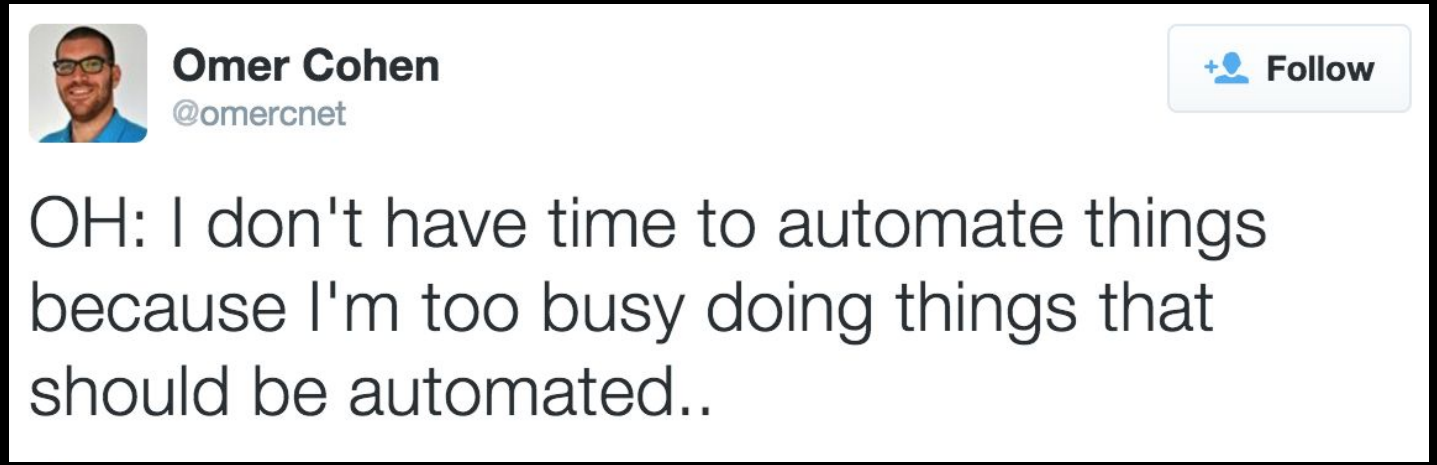
Incident Response on a tight budget

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



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 ->

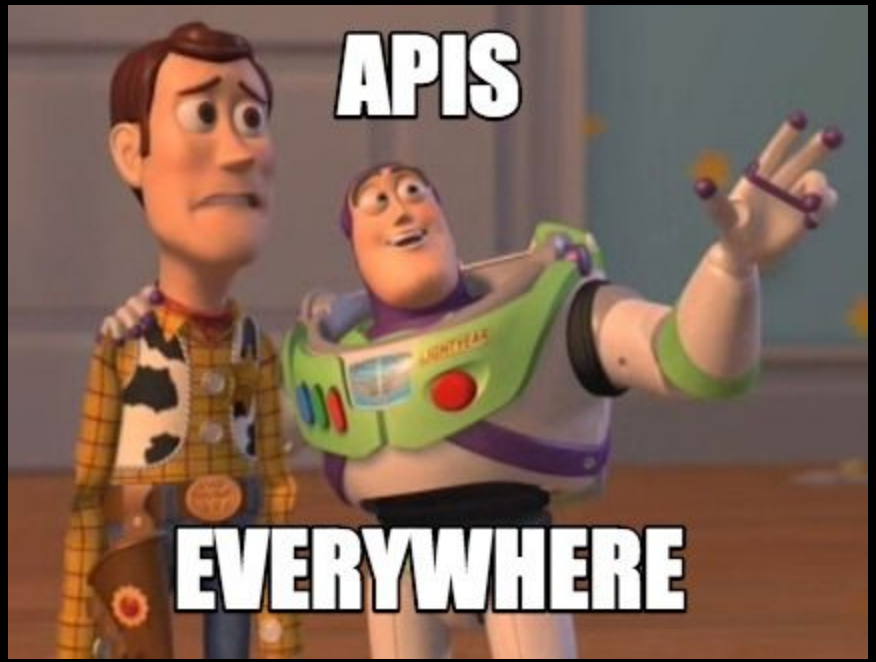
Automagically make a decision based on BU ->

Automagically classify incident ->

Automagically open ITSM re-image ticket ->

System re-imaged ->

Incident closed


APIS
EVERYWHERE

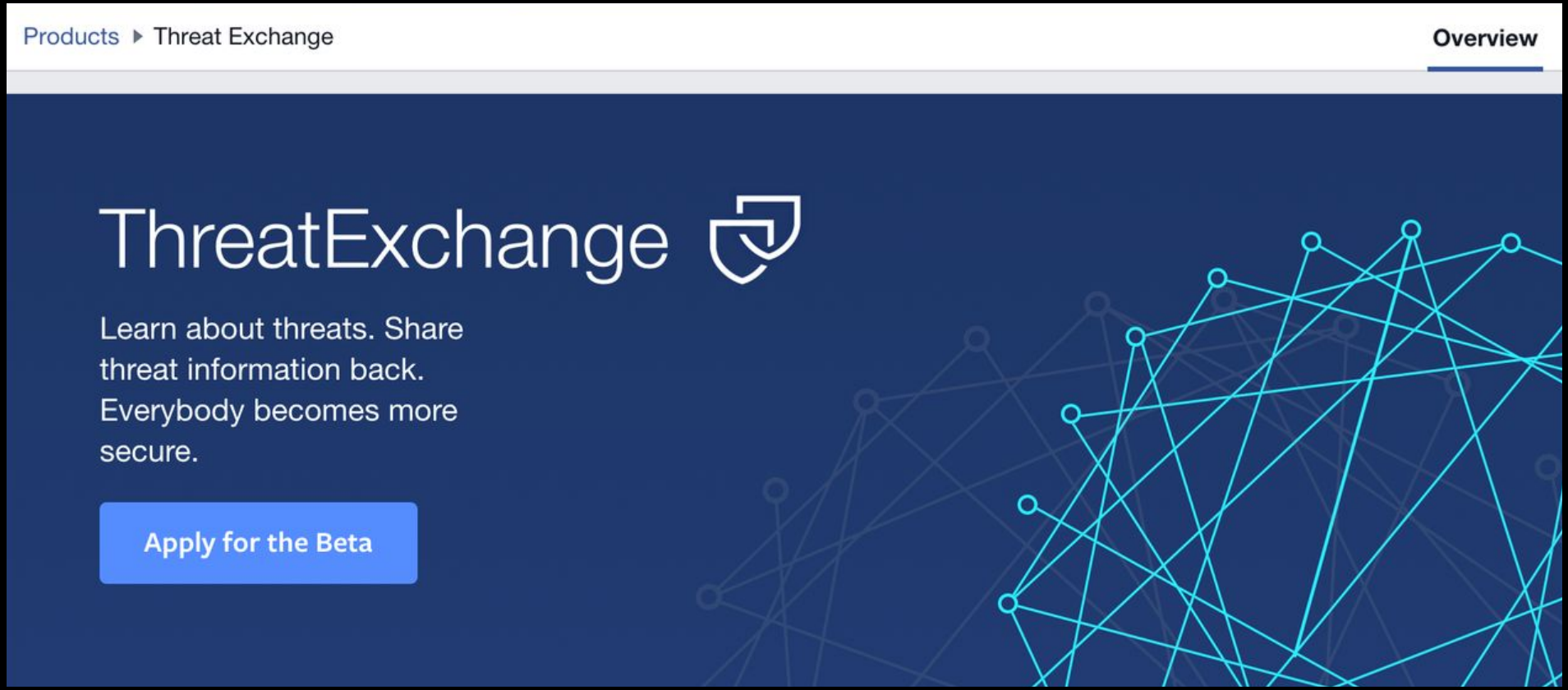
Integrate APIs into Incident Response

- 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



https://facebook.com/threatexchange

```
1  from pytx import ThreatIndicator
2  from pytx.vocabulary import ThreatType as tt
3  from pytx.vocabulary import Types as t
4
5  print ThreatIndicator.objects(threat_type=tt.COMPROMISED_CREDENTIAL,
6                  type_=t.EMAIL_ADDRESS, fields=['indicator', 'passwords'])
```

https://github.com/facebook/ThreatExchange/

Automatic e-Crime detection?


```
{
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: "745922858867220"
},
{
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: "971561682906025"
},
{
indicator: "axilrod@gmail.com",
added_on: "2015-06-30T06:03:21+0000",
id: "931651286899781"
},
```

Automatic e-Crime detection?

```
{
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: "745922858867220"
},
{
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: "971561682906025"
},
{
indicator: "axilrod@gmail.com",
added_on: "2015-06-30T06:03:21+0000",
id: "931651286899781"
},
```

```
{
data: [
{
indicator: "asalas881@yahoo.com",
added_on: "2015-06-30T06:03:21+0000",
id: "911123668926498"
},
{
indicator: "bergmanjonathan@yahoo.com",
added_on: "2015-06-30T06:03:21+0000",
id: "745922858867220"
},
{
indicator: "bizwam@yahoo.com",
added_on: "2015-06-30T06:03:21+0000",
id: "838301019552941"
},
{
indicator: "apurv.jamaiyar@yahoo.com",
added_on: "2015-06-30T06:03:21+0000",
id: "971561682906025"
},
{
indicator: "axilrod@yahoo.com",
added_on: "2015-06-30T06:03:21+0000",
id: "931651286899781"
},
```

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.

File URL Search

No file selected Choose File

Maximum file size: 128MB

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.

Scan it!

```
>>> import json
>>> import urllib
>>> url = 'https://www.virustotal.com/vtapi/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': [
    {"url": "http://027.ru/", "positives": 2, "total": 37, "scan_date": "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


JIRA Service Desk


JIRA Service Desk


bmc


JIRA Service Desk


bmc


servicenow


JIRA Service Desk


bmc


LANDESK


servicenow

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