Pulse

IBM SolutionsConnect 2013

Using Security Intelligence to Stay out of the Headlines

Matthew Prince, CISSP, Sr. IT Specialist, IBM Australia

12/06/2013

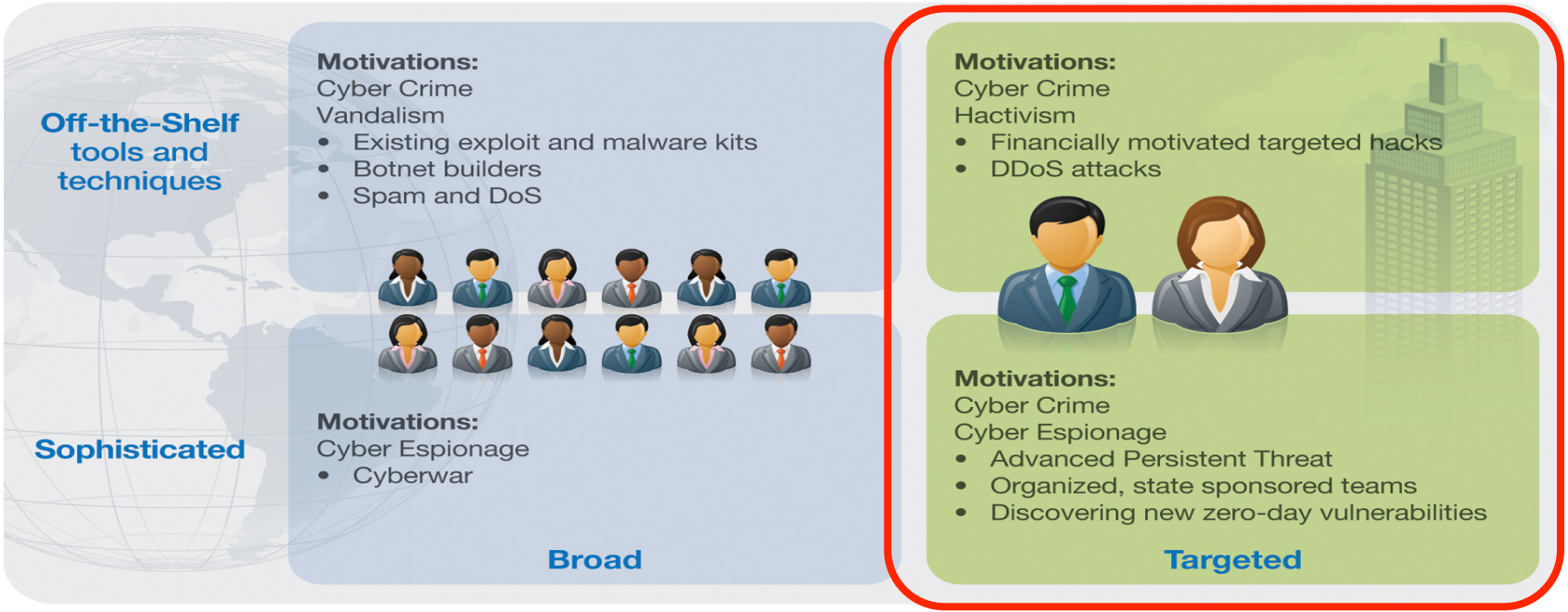
IBM

Agenda

- Changing threat landscape
- Analysis of three highly publicized incidents
- Applying Security Intelligence
- Real world scenarios

The Game has Changed ...

Different adversaries, motivations, and techniques



Source: IBM X-Force® Research and Development

Targets of Choice

- Transition from “Targets of Opportunity” to “Targets of Choice”
  - Actions of a decade ago were different both in motivation and result than today. Vandalism/ego vs:

    Organized internet crime: monetary gain

    Cyber warfare: Nation state driven

    Political: hacktivism
  - In most cases, actors are now **highly disciplined and have significant resources at their disposal**
  - In all cases, the actor has engaged in sophisticated **evasion techniques**
  - Unlike in the previous era, actors place huge emphasis on **concealing their presence**, rather than broadcasting it to the world
  - These techniques defeated traditional detection capabilities (1st generation SIEM, DLP, AntiVirus)

In the News

- **WikiLeaks/Bradley Manning** is one of the most public examples of a persistent threat that enterprises constantly face
- **Stuxnet** – Industrial espionage / sabotage
- **RSA** attacked, SecureID tokens targeted
- Other recent examples:
  - ASIO HQ plans leaked?
  - F-35 Joint Strike Fighter and other military systems plans stolen by Chinese hackers
  - So on, so forth …

Funny, they look alike…

The WikiLeaks Insider

- PFC Bradley Manning had been an intelligence analyst (MOS 35F) and was in process for early discharge at COS Hammer (10th Mountain Division) Iraq
- Using his classified workstations, he allegedly accessed data on SIPRNET and JWICS and **transferred it to his personal laptop**.
- Using a combination of Winzip, Tor, Torsocks, Privoxy and OpenSSH, Manning allegedly **uploaded content to the WikiLeaks website using his personal laptop**.
- In online chats, Manning took credit for uploading a video of an airstrike at Granai and a video of an incident resulting in the death of Reuters photographer Namir Noor-Eldeen
- In July 2010, WikiLeaks published **77,000 documents** relating to the war in Afghanistan
- In December, the same site published more than **150,000** classified State Department cables

PFC Manning, in his own words…

Source: http://www.wired.com/threatlevel/2010/06/wikileaks-chat/

(01:52:30 PM) Manning: funny thing is… we transffered so much data on unmarked CDs…
(01:52:42 PM) Manning: everyone did… videos… movies… music
(01:53:05 PM) Manning: all out in the open
(01:53:53 PM) Manning: **bringing CDs too and from the networks was/is a common phenomeon**
(01:54:14 PM) Lamo: is that how you got the cables out?
(01:54:28 PM) Manning: perhaps
(01:54:42 PM) Manning: i would come in with music on a CD-RW
(01:55:21 PM) Manning: labelled with something like "Lady Gaga"… erase the music… then write a compressed split file
(01:55:46 PM) Manning: no-one suspected a thing

(02:00:12 PM) Manning: everyone just sat at their workstations… watching music videos / car chases / buildings exploding… and writing more stuff to CD/DVD… **the culture fed opportunities**
(02:01:44 PM) Manning: hardest part is arguably internet access… uploading any sensitive data over the open internet is a bad idea… since networks are monitored for any insurgent/terrorist/militia/criminal types
(02:01:52 PM) Lamo: tor?
(02:02:13 PM) Manning: tor + ssl + sftp
(02:02:33 PM) Lamo: *nod*
(02:03:05 PM) Lamo: not quite how i might do it, but good
(02:03:22 PM) Manning: **i even asked the NSA guy if he could find any suspicious activity coming out of local networks… he shrugged and said… "its not a priority"**
(02:03:53 PM) Manning: went back to watching "Eagle's Eye"

(02:12:23 PM) Manning: so… it was a massive data spillage… facilitated by numerous factors… both physically, technically, and culturally
(02:13:02 PM) Manning:: perfect example of **how not to do INFOSEC**
(02:14:21 PM) Manning: listened and lip-synced to Lady Gaga's Telephone while exfiltratrating possibly the largest data spillage in american history
(02:15:03 PM) Manning: pretty simple, and unglamorous
(02:16:37 PM) Manning: *exfiltrating
(02:17:56 PM) Manning: weak servers, **weak logging**, weak physical security, weak counter-intelligence, inattentive signal analysis… a perfect storm
(02:43:33 PM) Manning: also, theres **god awful accountability of IP addresses**…
(02:44:47 PM) Manning: the network was upgraded, and patched up so many times… and systems would go down, **logs would be lost**… and when moved or upgraded… hard drives were zeroed
(02:45:12 PM) Manning: its impossible to trace much on these field networks…
(02:46:10 PM) Manning: and who would honestly expect so much information to be exfiltrated from a field network?

WikiLeaks Scenario—Insider Threat

- WikiLeaks and other insider breaches are a combination of:
  - Legitimate but **excessive** access to information, and
  - Ill considered or nefarious actions with that information
- Isolated network—no internet access
- Appropriate access controls on local workstation for role
- Windows object auditing and endpoint security
- Evasion & Exfiltration:
  - Browsed through, then copied significant data to workstation
  - Disconnect workstation from network
  - Burn information to CD
  - Erase log activity
  - Reconnect to network
  - Total time: 8 minutes
- How would you detect and stop this?

Stuxnet: Cyberweapon

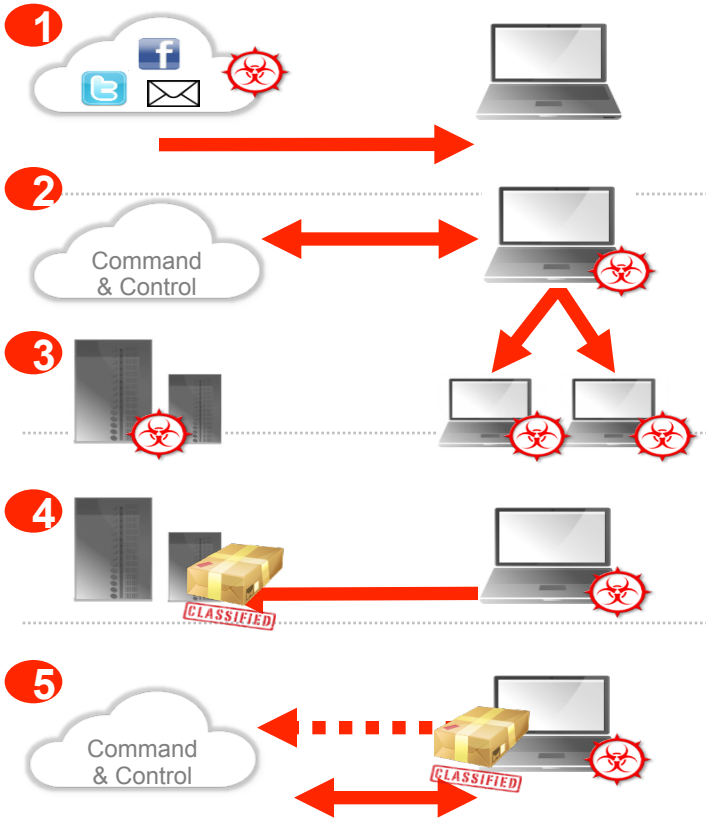
- Virus/worm designed to specifically target Iran's uranium enrichment program.
- Stuxnet is known to propagate itself through removable drives, and relies upon Windows vulnerabilities to exploit network shares, remote machines, database servers, LANs.
- Has functionality to bypass certain security telemetry it encounters, and contains a binary screening mechanism to hide its code.
- Its reported there have been 12K+ incidents globally; 100K+ computers infected worldwide; 60K+ machines in Iran.
- Believed to be the first piece of malware targeted specifically at industrial control systems
- Represents a dangerous tool, or "cyberweapon" that can be launched by a malicious insider – and all it takes is one!
- The threat of Stuxnet is that it extends beyond the virtual to attack the physical, impacting government, industry, consumers and citizens

2011 RSA Attack

- Targeted phishing attack (aka spear-phishing) to a small group of employees
  - Attachment titled “2011 Recruitment Plan.xls”
- At least one employee succumbed to curiosity, their system and credentials were compromised
- Those credentials were then used to expand the attacker’s beachhead and pursue the primary target
- Data exfiltrated using FTP from internally compromised staging servers to external hosts owned by the attacker
- Attacker’s target was SecureID, however no public disclosure on what was ultimately stolen
  - Possibly because they don’t know?
- Still feel good about your SecureID deployment?

Further reading at http://blogs.rsa.com/anatomy-of-an-attack/

2011 RSA Attack



Spear phishing and 0-day attacks	User behaves in risky manner. Receives enterprise email from personal social network
Backdoor or malware is installed	Anomalous device and network behavior; DNS query to known malicious hosts; abnormal traffic patterns
Lateral movement	User behavior is anomalous; Device is contacting new hosts; Network pattern anomalous
Data acquisition and aggregation	User behavior is anomalous; Data access patterns abnormal; Data rapidly aggregating

How Are these Incidents Similar?

- Despite the stark differences in these high-profile cases, the common element is the **user**, whether a rogue employee or a compromised account.
  - WikiLeaks – PFC Manning.
  - Stuxnet – Who brought it in? Why did they have access to the SCADA network?
  - RSA – Lateral movement through compromised account
- All represent the confluence of excessive access to highly sensitive systems with nefarious intent, whether on the part of the user themselves or someone else with access to their credentials
- These scenarios illustrate a paradigm shift in the threat landscape with far-reaching impacts across nuclear programs, the global energy industry, Federal systems, espionage, sensitive intellectual property, etc.

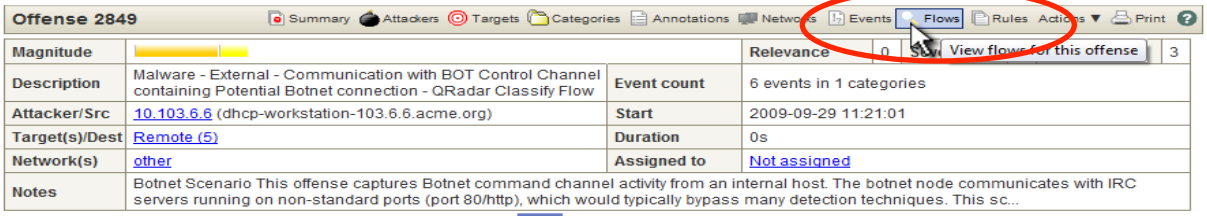
The Wrong Answer…

- The problem isn't that users are accessing data they aren't authorized to
- DLP–while useful–isn't going to solve the specific problem
- Focusing on writing to CDs/DVDs isn't the answer
- Focusing on detecting and stopping Tor/Privoxy etc isn't the answer
- The TSA model is a game of catch-up:
  - Shoe bomber, take off your shoes
  - Underwear bomber, well…you get the idea

Monitoring Requirements for an APT World

- Start with risk assessment and audit
  - Classify assets and objects, in all types of organizations
- Clearly define roles and privileges
  - Identification
  - Security clearance
  - Need to know
- It's all about **behavior**:
  - Tracking users
  - Who does what, when, how often, and how much
    - Baseline application use and identify anomalies
    - Baseline file/database access and identify anomalies
    - Baseline network activity and identify anomalies
    - Ad infinitum / ad nauseum, whichever comes first
  - This requires broad telemetry and instrumentation

Botnet Phone Home?



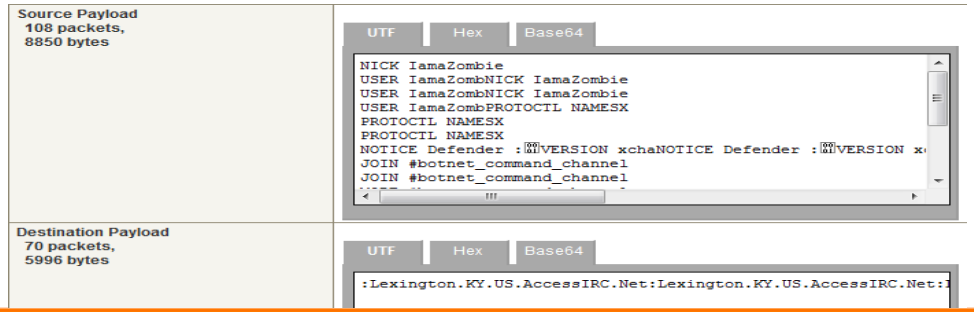
Magnitude		Relevance	0
Description	Malware - External - Communication with BOT Control Channel containing Potential Botnet connection - QRadar Classify Flow	Event count	6 events in 1 categories
Attacker/Src	10.103.6.6 (dhcp-workstation-103.6.6.acme.org)	Start	2009-09-29 11:21:01
Target(s)/Dest	Remote (5)	Duration	0s
Network(s)	other	Assigned to	Not assigned
Notes	Botnet Scenario This offense captures Botnet command channel activity from an internal host. The botnet node communicates with IRC servers running on non-standard ports (port 80/http), which would typically bypass many detection techniques. This sc...		

Botnet Detected?

First Packet Time	Protocol	Source IP	Source Port	Destination IP	Destination Port	Application	ICMP Type/Cod	Source Flags	Destinat Flags	Source QoS	Destinat QoS	Flow Sourc
11:19	tcp_ip	10.103.6.6	48667	62.64.54.11	80	IRC	N/A	S,P,A	F,S,P,A	Best Effor	Class 1	qradar
11:19	tcp_ip	10.103.6.6	50296	192.106.224.13	80	IRC	N/A	S,P,A	S,A	Best Effor	Class 1	qradar
11:19	tcp_ip	10.103.6.6	51451	62.181.209.201	80	IRC	N/A	S,P,A	F,S,P,A	Best Effor	Class 1	qradar
11:19	tcp_ip	10.103.6.6	47961	62.211.73.232	80	IRC	N/A	F,S,P,A	F,S,P,A	Best Effor	Class 1	qradar

IRC on port 80?

Flow analytics enables detection of a covert channel.



Irrefutable

Layer 7 data contains botnet command and control instructions.

Complex Threat Detection

Offense 3063 Summary | Attackers | Targets | Categories | Annotations | Networks | Events

Magnitude		**Relevance**	3
Description	Target Vulnerable to Detected Exploit preceded by Exploit Attempt Proceeded by Recon preceded by Exploit/Malware Events Across Multiple Targets preceded by Recon - External - Potential Network Scan	**Event count**	1428 events in 3 cate
Attacker/Src	202.153.48.66	**Start**	2009-09-29 16:05:01
Target(s)/Dest	Local (717)	**Duration**	1m 32s
Network(s)	Multiple (3)	**Assigned to**	Not assigned
Notes	Vulnerability Correlation Use Case Illustrates a scenario involving correlation of vulnerability data with I China (202.153.48.66) sweeps a subnet using the Conficker worm exploit (CVE 2008-4250). The first s		

Sounds Nasty…

But how do we know this?

The evidence is a single click away.

Network Scan

Detected by Layer 7 analysis

Buffer Overflow

Exploit attempt seen by IDS

	Event Name	Source IP	Destination IP	Destination Port	Log Source	Low Level Category
	Network Sweep - QRadar Classify Flow	202.153.48.66	Multiple (716)	445	Flow Classification E	Network Sweep
	NETBIOS-DG SMB v4 srvsvc NetrpPathConon	202.153.48.66	Multiple (8)	445	Snort @ 10.1.1.5	Buffer Overflow

Port	Service	OSVDB ID	Name	Description	Risk / Severity
445	unknown	49243	Microsoft Windows Server Service Crafted RPC Request Handling Unspecified Remote Code Execution	Microsoft Windows Server Service contains a flaw that may allow a malicious user to remotely execute arbitrary code. The issue is triggered when a crafted RPC request is handled. It is possible that the flaw may allow remote code execution resulting in a loss of integrity.	3

Targeted Host Vulnerable

Detected by vulnerability scanner

Total Visibility

Convergence of Network, Event and Vulnerability data.

Fraud & Data Loss Detection

Problem Statement

- Malicious activity against ‘targets of choice’
- Privileged or knowledgeable users internal to the network
- Fraud patterns that are ‘low and slow’ by nature
- Associating suspicious patterns across network, security, application and host layers in the infrastructure

Required Intelligence

- Ability to take and normalize telemetry across many diverse sources
- Correlation of host and asset profiles with IAM infrastructure
- Integration of 3rd party intelligence sources

Fraud & Data Loss Detection

Potential Data Loss?

Who? What? Where?

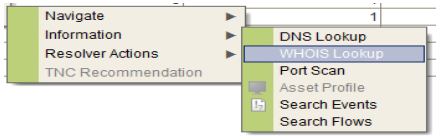
Magnitude	
Description	Potential Data Loss/Theft Detected
Attacker/Src	10.103.14.139 (dhcp-workstation-103.14.139.acme.org)
Target(s)/Dest	Local (2) Remote (1)
Network(s)	Multiple (3)
Notes	Data Loss Prevention Use Case. Demonstrates QRadar DL authentication ...

Attacker Summary	Details		
Magnitude		User	scott
Description	10.103.14.139	Asset Name	dhcp-workstation-103.14.139.acme.org
Vulnerabilities	0	MAC	Unknown
Location	NorthAmerica.all	Asset Weight	0

Who?
An internal user

	Event Name	Source IP (Unique Count)	Log Source (Unique Count)	Username (Unique Count)	Category (Unique Count)
	Authentication Failed	10.103.14.139	OracleDbAudit @ 10.101.145.198	Multiple (2)	Misc Login Failed
	Misc Login Succeeded	10.103.14.139	OracleDbAudit @ 10.101.145.198	scott	Misc Login Succeeded
	DELETE failed	10.103.14.139	OracleDbAudit @ 10.101.145.198	scott	System Action Deny
	SELECT succeeded	10.103.14.139	OracleDbAudit @ 10.101.145.198	scott	System Action Allow
	Misc Logout	10.103.14.139	OracleDbAudit @ 10.101.145.198	scott	Misc Logout
	Suspicious Pattern Detec	10.103.14.139	Custom Rule Engine-8 :: qradar-vn	N/A	Suspicious Pattern Detected
	Remote Access Login Fa	10.103.14.139	Custom Rule Engine-8 :: qradar-vn	N/A	Remote Access Login Failed

What?
Oracle data



QRadar Has Completed Your Request

Go to APNIC results

[Querying whois.arin.net]
[whois.arin.net]

OrgName: Google Inc.
OrgID: GOGL
Address: 1600 Amphitheatre Parkway
City: Mountain View

Where?
Gmail

Compliance Violations and Data Loss

Tale of Two (North American) Universities

- University A: long time SIEM customer w/network visibility
- University B: no SIEM/NBAD capabilities

University A

- Host is compromised and detected by SIEM.
- Host is identified as a critical system in accounting with student personally identifiable information (PII).
- Analysis of flow data to/from compromised host shows that the only data transferred was copyrighted material, and **not** student PII.
- Compromised host was cleaned and no one outside was ever notified

University B

- Host is compromised and detected at some point after the attack
- Host is found to carry PII.
- Without content & flow analysis, it cannot be determined which (if any) data was stolen.
- The university is then required to notify ALL students of the **potential** loss of privacy and setup a call center to answer questions … lots of $$$, bad PR.

Complex Threats - Detecting the Undetectable

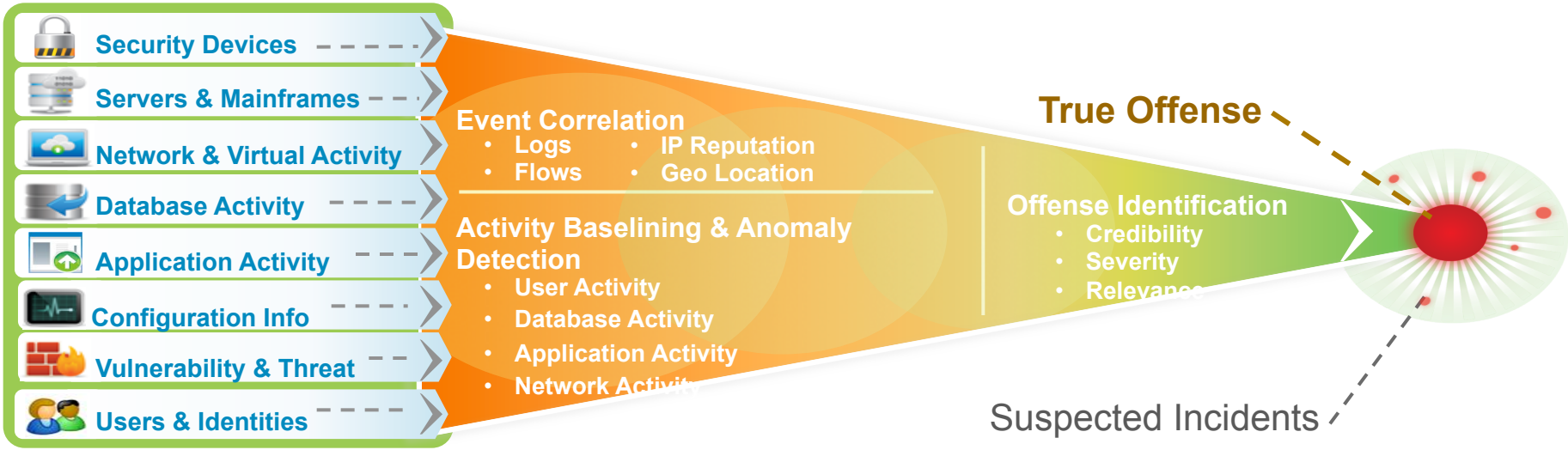
Quite often, despite numerous security measures organizations put in place, a host gets quietly compromised and remains undetected…

During a Customer POC:

- In a network of 80,000 hosts, 3 make a web request to the same address and transfer a 112 byte .gif image several times a day.
- Those hosts make no other related requests to the .gif-serving host
- These machines often don't appear to be in use at the time of the suspicious requests.
- The 3 systems all have Anti-Virus/Anti-Malware which claim they are clean
- The machine hosting the .gif image in question is a known botnet command & control server (identified through external Security Intelligence sources)
- POC customer is aggressive and re-images the 3 hosts identified…

Activity goes away….

Security Intelligence: Context and Correlation Drive Deep Insight



Extensive Data Sources + Deep Intelligence = Exceptionally Accurate and Actionable Insight

Questions?

Thank you !