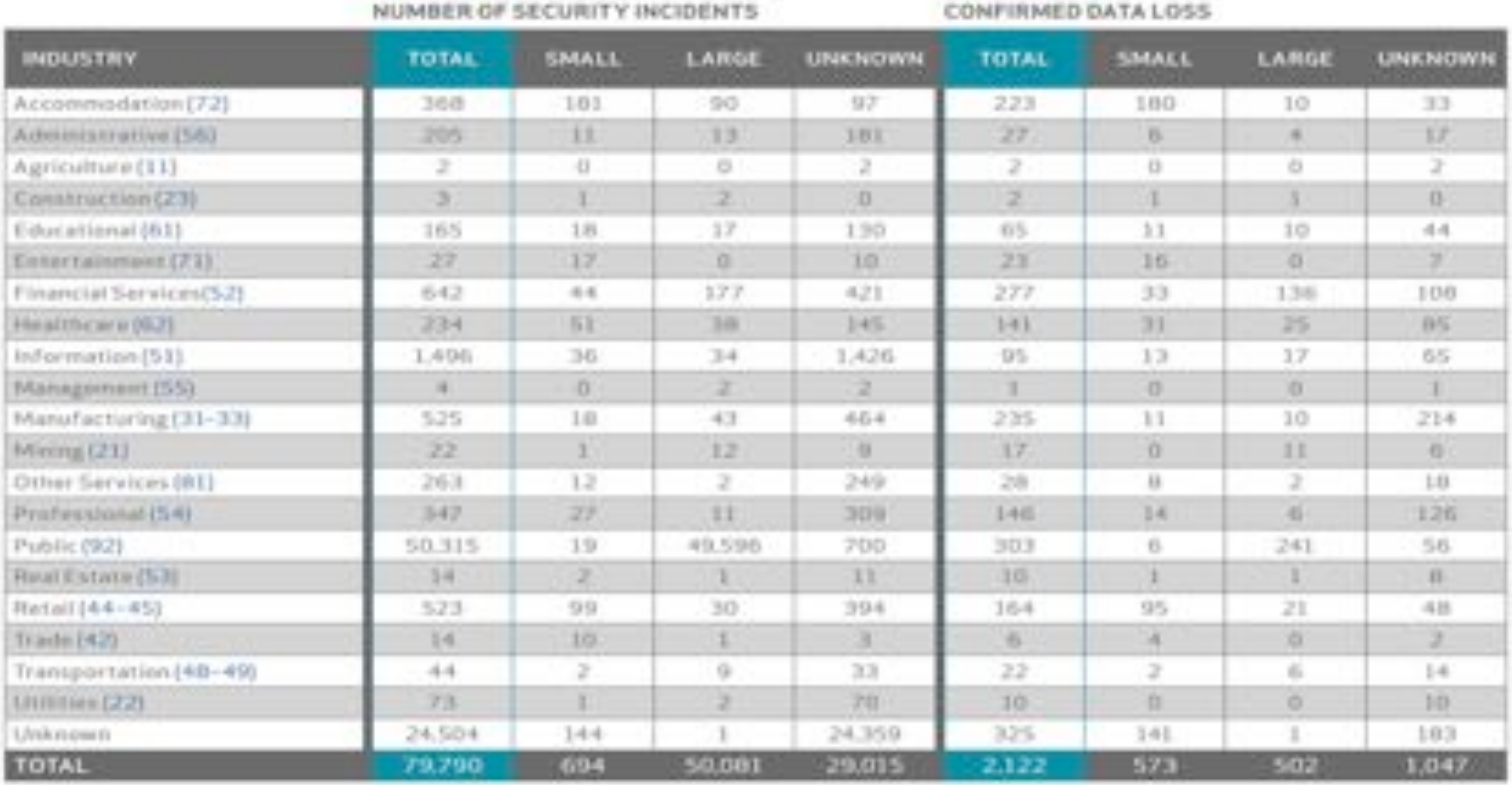
BLUE COAT Network + Security + Cloud

Cyber Threats and Risks

Maturing Your Incident Response Capabilities

Chong Kwek Wee (CISSP)
Snr Systems Engineer – ASEAN

WE LIVE IN A POST PREVENTION WORLD



	NUMBER OF SECURITY INCIDENTS				CONFIRMED DATA LOSS			
INDUSTRY	TOTAL	SMALL	LARGE	UNKNOWN	TOTAL	SMALL	LARGE	UNKNOWN
Accommodation (72)	368	181	90	97	223	180	10	33
Administrative (56)	205	11	13	181	27	6	4	17
Agriculture (11)	2	0	0	2	2	0	0	2
Construction (23)	3	1	2	0	2	1	1	0
Educational (61)	165	18	17	130	65	11	10	44
Entertainment (71)	27	17	0	10	23	16	0	7
Financial Services (52)	642	44	177	421	277	33	136	108
Healthcare (62)	234	51	38	145	141	31	25	85
Information (51)	1,496	36	34	1,426	95	13	17	65
Management (55)	4	0	2	2	1	0	0	1
Manufacturing (31-33)	525	18	43	464	235	11	10	214
Mining (21)	22	1	12	9	17	0	11	6
Other Services (81)	263	12	2	249	28	8	2	18
Professional (54)	347	27	11	309	146	14	6	126
Public (92)	50,315	19	49,596	700	303	6	241	56
Real Estate (53)	14	2	1	11	10	1	1	8
Retail (44-45)	523	99	30	394	164	95	21	48
Trade (42)	14	10	1	3	6	4	0	2
Transportation (48-49)	44	2	9	33	22	2	6	14
Utilities (22)	73	1	2	70	10	0	0	10
Unknown	24,504	144	1	24,359	325	141	1	183
TOTAL	79,790	694	50,081	29,015	2,122	573	502	1,047

THE INVISIBLE MAN…OR MALWARE

Threats we can’t see…

30-60% of Traffic is Encrypted

THE INVISIBLE MAN…OR MALWARE

SECURITYWEEK
INTERNET AND ENTERPRISE SECURITY NEWS, INSIGHTS & ANALYSIS

New Zeus Variant Uses Sophisticated Control Panel: Researchers ***"Date: Jan 29, 2015"***

"The new Zeus variant has been used to target major Canadian banks, including the National Bank of Canada, the Royal Bank of Canada, and the Bank of Montreal."

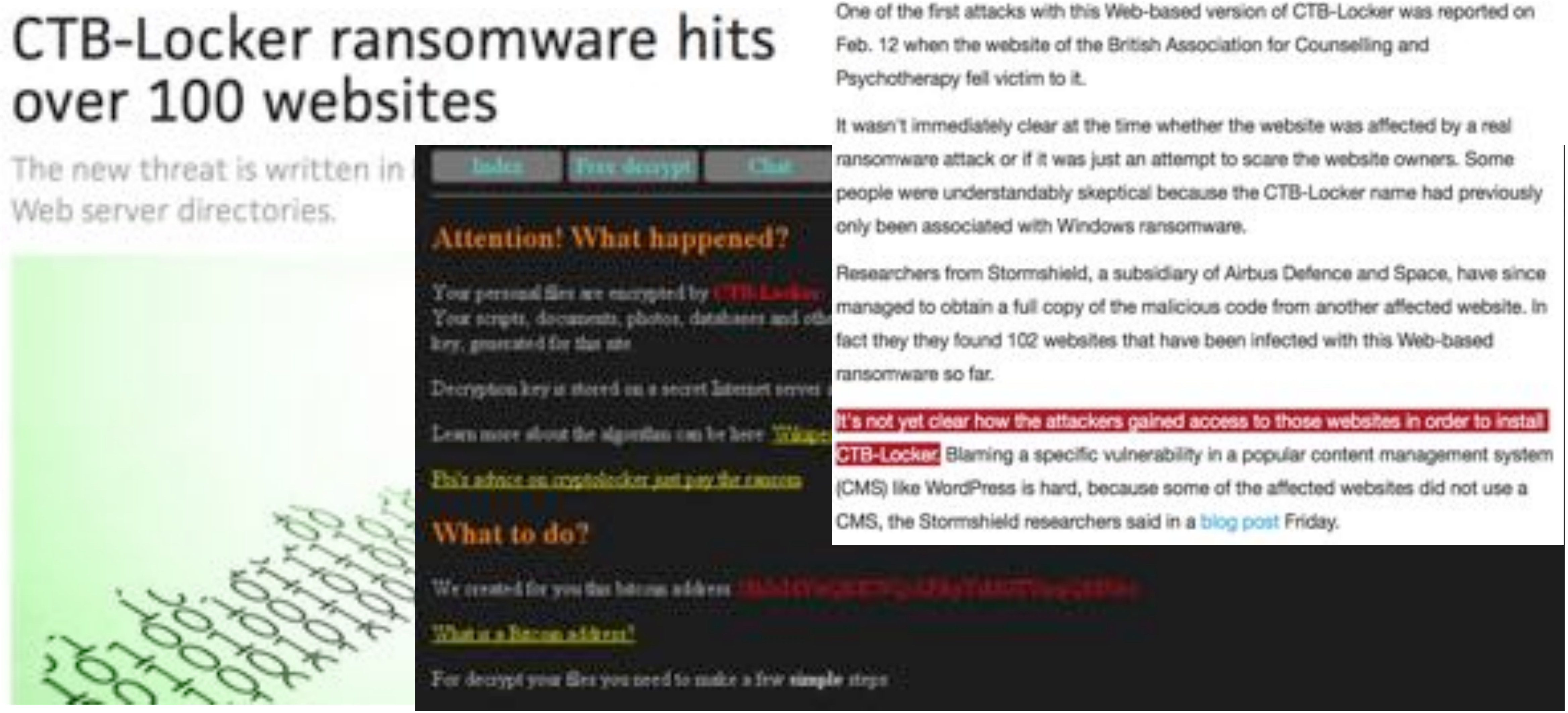
"Furthermore, the threat doesn't raise too much suspicion since browser security is bypassed and no SSL warnings are generated."

SC
MAGAZINE
FOR IT SECURITY PROFESSIONALS

GameOver Trojan hides activities in SSL connections to defraud victims ***"Date: Oct 7, 2013"***

"Instead of receiving instructions from an attacker-operated command-and-control server, the Upatre downloader uses an encrypted SSL connection to download malware directly from compromised web servers."

TERMINAYOR – RISE OF RANSOMWARES



CTB-Locker ransomware hits over 100 websites

The new threat is written in
Web server directories.

Attention! What happened?

Your personal files are encrypted by CTB-Locker.
Your scripts, documents, photos, databases and oth
key, generated for this site

Decryption key is stored on a secret Internet server

Learn more about the algorithm can be here: Wikipe

Phi's advice on cryptolocker just pay the ransom

What to do?

We created for you this bitcoin address: [illegible]

What is a Bitcoin address?

For decrypt your files you need to make a few **simple** steps

One of the first attacks with this Web-based version of CTB-Locker was reported on Feb. 12 when the website of the British Association for Counselling and Psychotherapy fell victim to it.

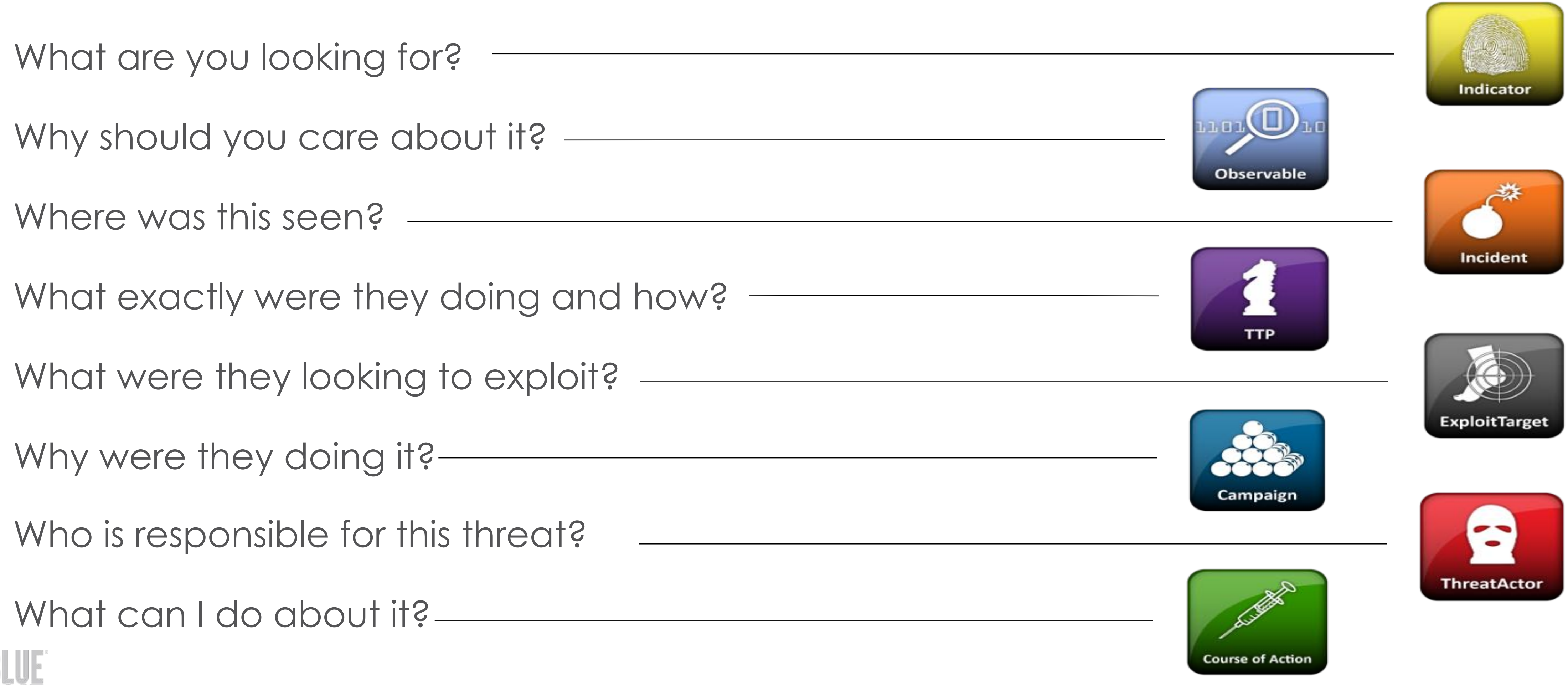
It wasn't immediately clear at the time whether the website was affected by a real ransomware attack or if it was just an attempt to scare the website owners. Some people were understandably skeptical because the CTB-Locker name had previously only been associated with Windows ransomware.

Researchers from Stormshield, a subsidiary of Airbus Defence and Space, have since managed to obtain a full copy of the malicious code from another affected website. In fact they they found 102 websites that have been infected with this Web-based ransomware so far.

It's not yet clear how the attackers gained access to those websites in order to install CTB-Locker. Blaming a specific vulnerability in a popular content management system (CMS) like WordPress is hard, because some of the affected websites did not use a CMS, the Stormshield researchers said in a blog post Friday.

THE QUESTIONS TO ASK

- Incident Response should answer the following:



What are you looking for?

Why should you care about it?

Where was this seen?

What exactly were they doing and how?

What were they looking to exploit?

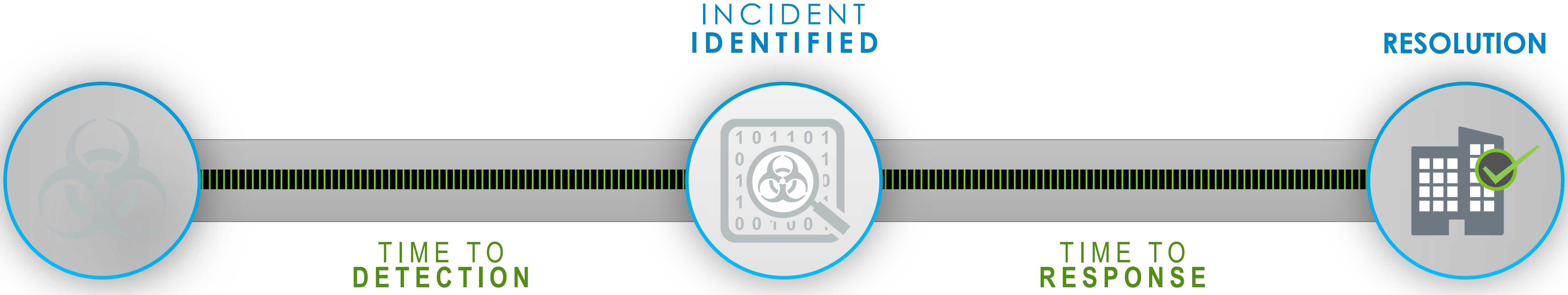
Why were they doing it?

Who is responsible for this threat?

What can I do about it?

THE EXPANDING WINDOW OF EXPOSURE

TODAY'S REALITY



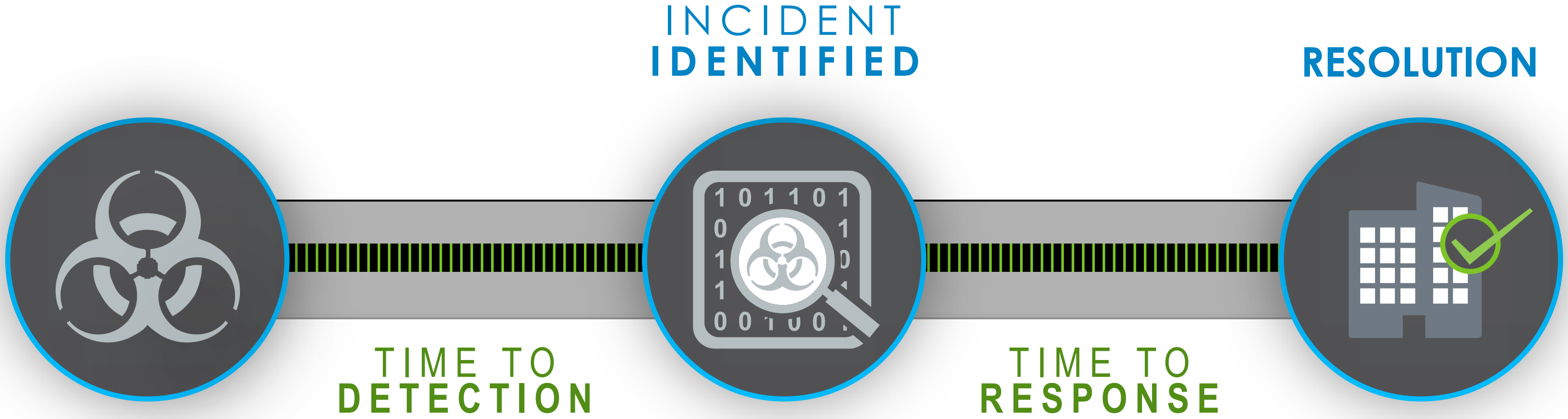
206 DAYS
to Detection*

21-35 DAYS
Average Breach Resolution

*Verizon 2014 Data Breach Investigations Report

SHRINKING THE WINDOW OF EXPOSURE

OUR MISSION



INCIDENT **IDENTIFIED**

RESOLUTION

TIME TO **DETECTION**

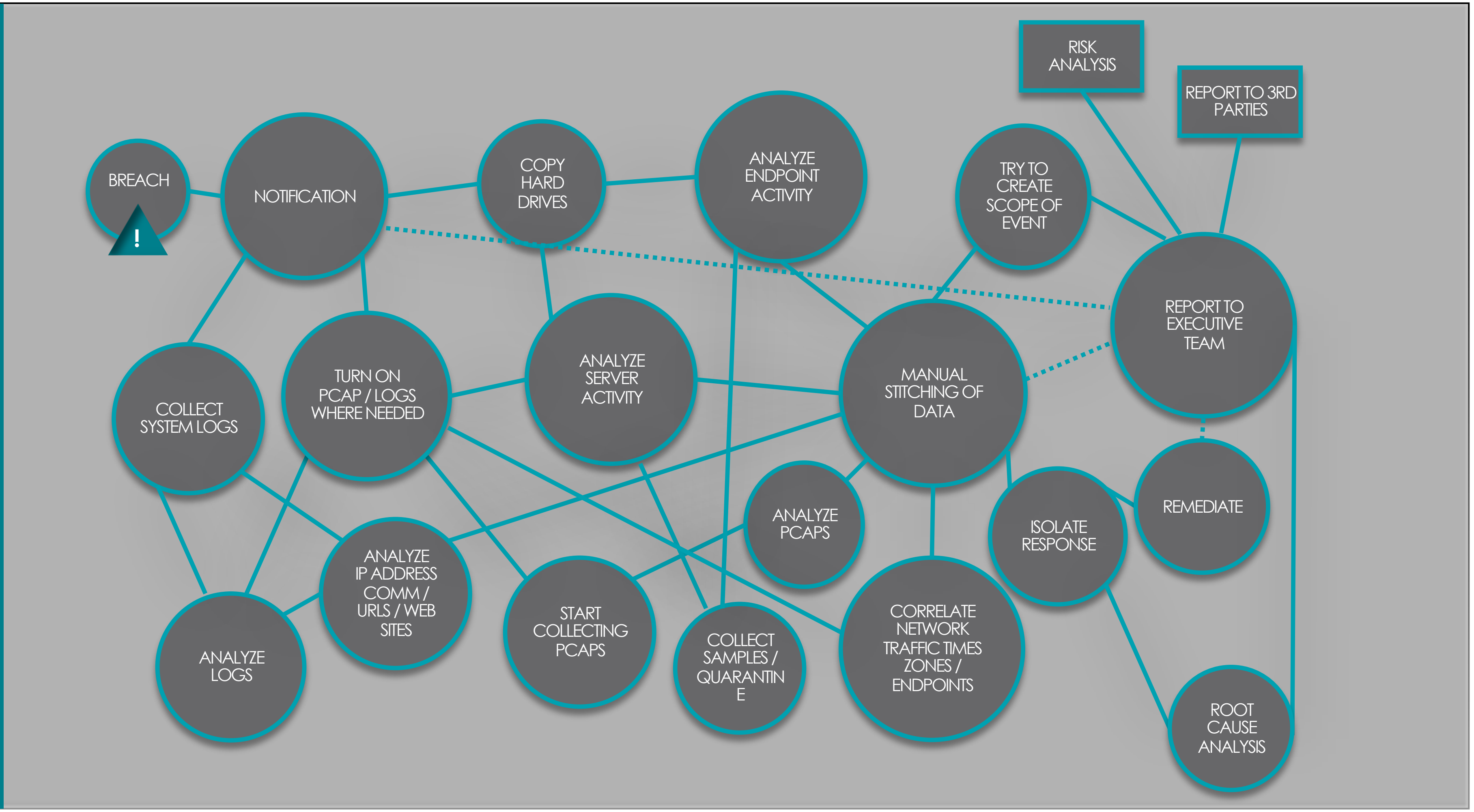
TIME TO **RESPONSE**

NET RESULT = LOWER COST

manpower, time, exposure to business and mitigated risk

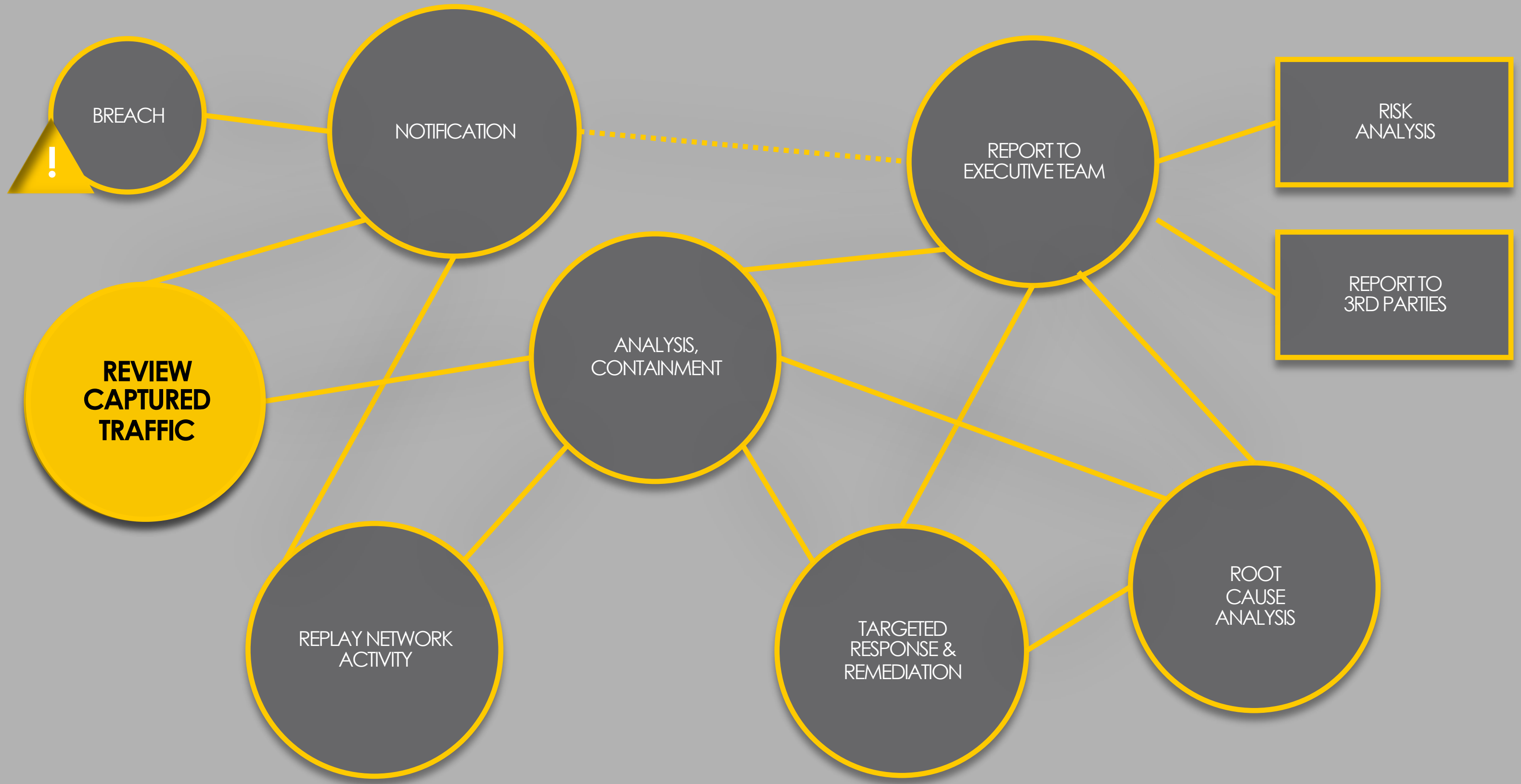
MANUAL FORENSICS

CLEANUP TAKES MONTHS WITH RANDOM PACKET ANALYSIS **WITHOUT COMPLETE RESOLUTION**



BASIC Forensics

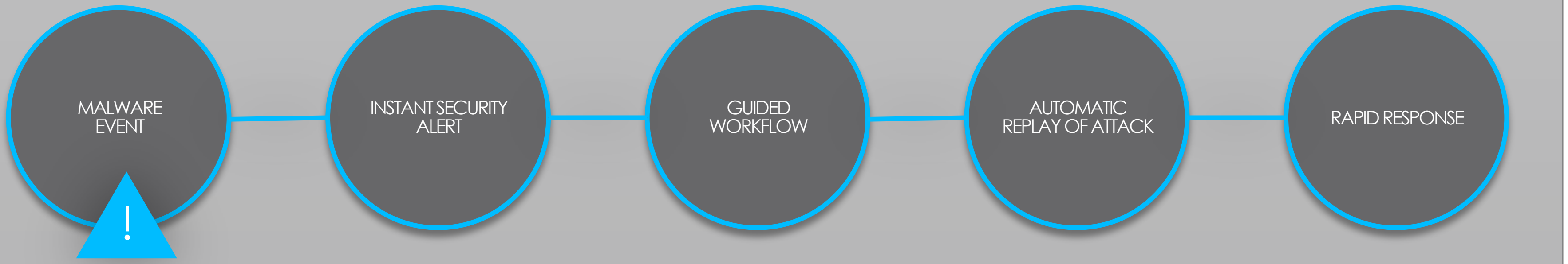
HISTORICAL CAPTURE AND REPLAY ACCELERATES RESPONSE AND MINIMIZES COSTS DRAMATICALLY



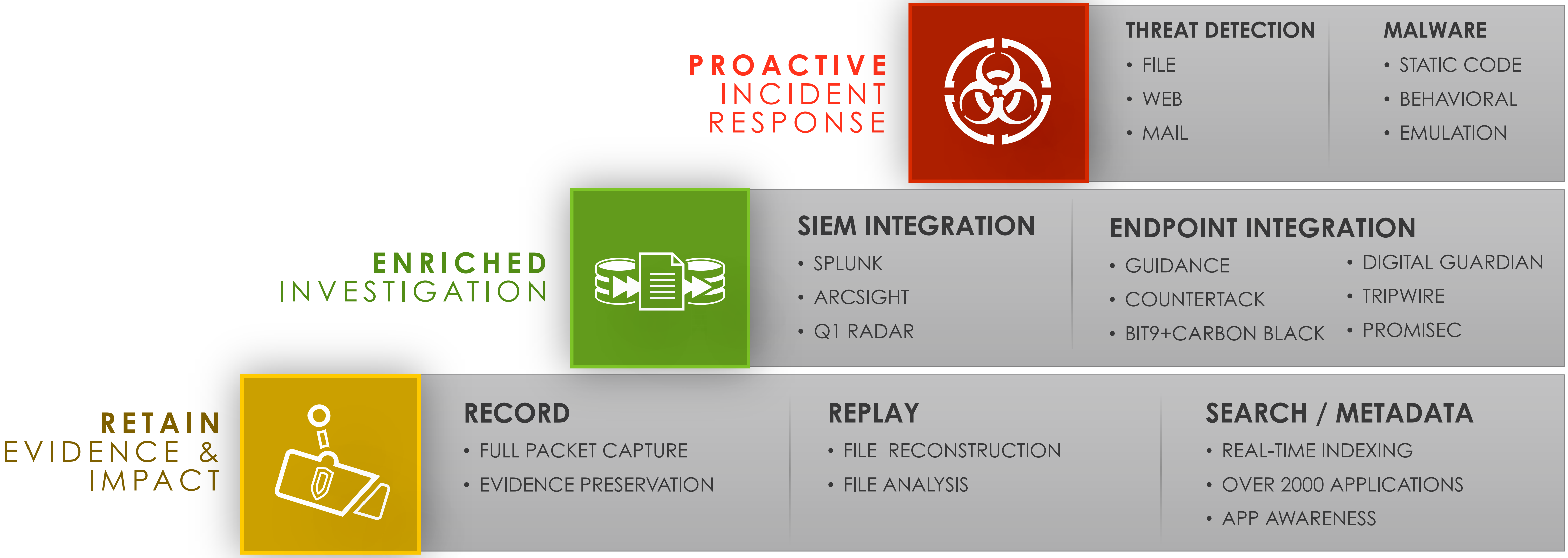
PROACTIVE INCIDENT RESPONSE

FAST DETECTION OF MALWARE **WITH RAPID RESPONSE**

MINIMIZES COSTS RESULTING FROM **BREACH**



MATURING INCIDENT RESPONSE CAPABILITIES



PROACTIVE INCIDENT RESPONSE

THREAT DETECTION

- FILE
- WEB
- MAIL

MALWARE

- STATIC CODE
- BEHAVIORAL
- EMULATION

ENRICHED INVESTIGATION

SIEM INTEGRATION

- SPLUNK
- ARCSIGHT
- Q1 RADAR

ENDPOINT INTEGRATION

- GUIDANCE
- COUNTERTACK
- BIT9+CARBON BLACK
- DIGITAL GUARDIAN
- TRIPWIRE
- PROMISEC

RETAIN EVIDENCE & IMPACT

RECORD

- FULL PACKET CAPTURE
- EVIDENCE PRESERVATION

REPLAY

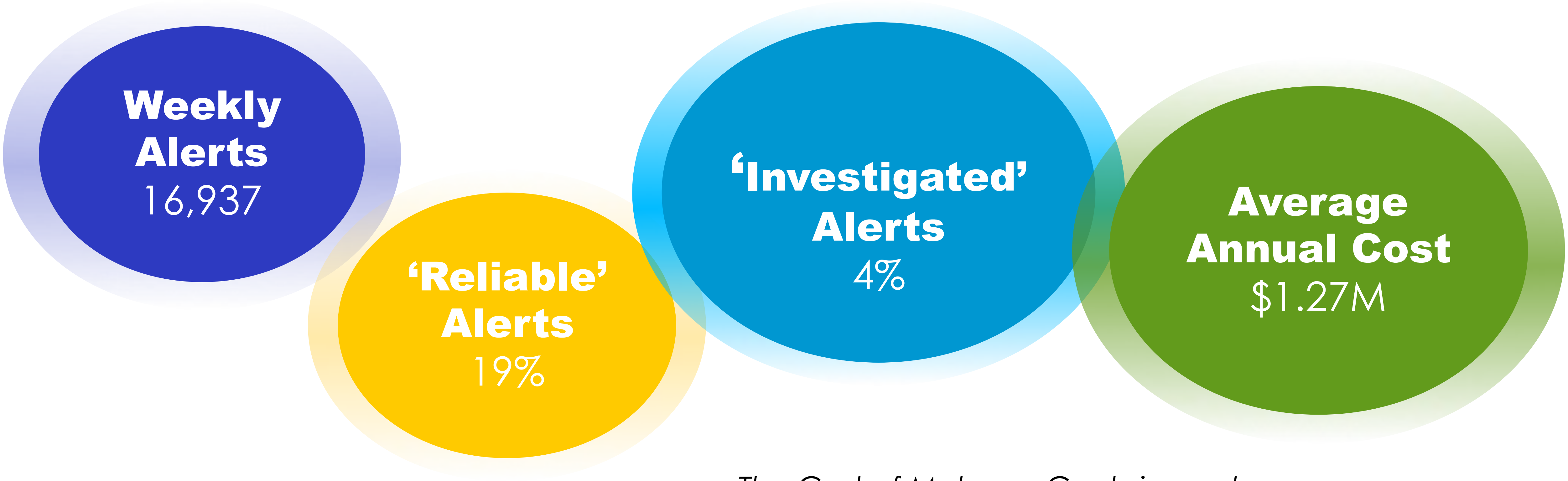
- FILE RECONSTRUCTION
- FILE ANALYSIS

SEARCH / METADATA

- REAL-TIME INDEXING
- OVER 2000 APPLICATIONS
- APP AWARENESS

THE HIGH PRICE OF TOO MANY ALERTS

“Two-thirds of the time spent by security staff responding to malware alerts is *wasted* because of faulty intelligence.”



Weekly Alerts
16,937

‘Reliable’ Alerts
19%

‘Investigated’ Alerts
4%

Average Annual Cost
$1.27M

The Cost of Malware Containment
Ponemon Institute, January 2015

CAR ALARM SYNDROME

"…in the case of each large breach over the past few years, **the alarms and alerts went off but no one paid attention to them.**"

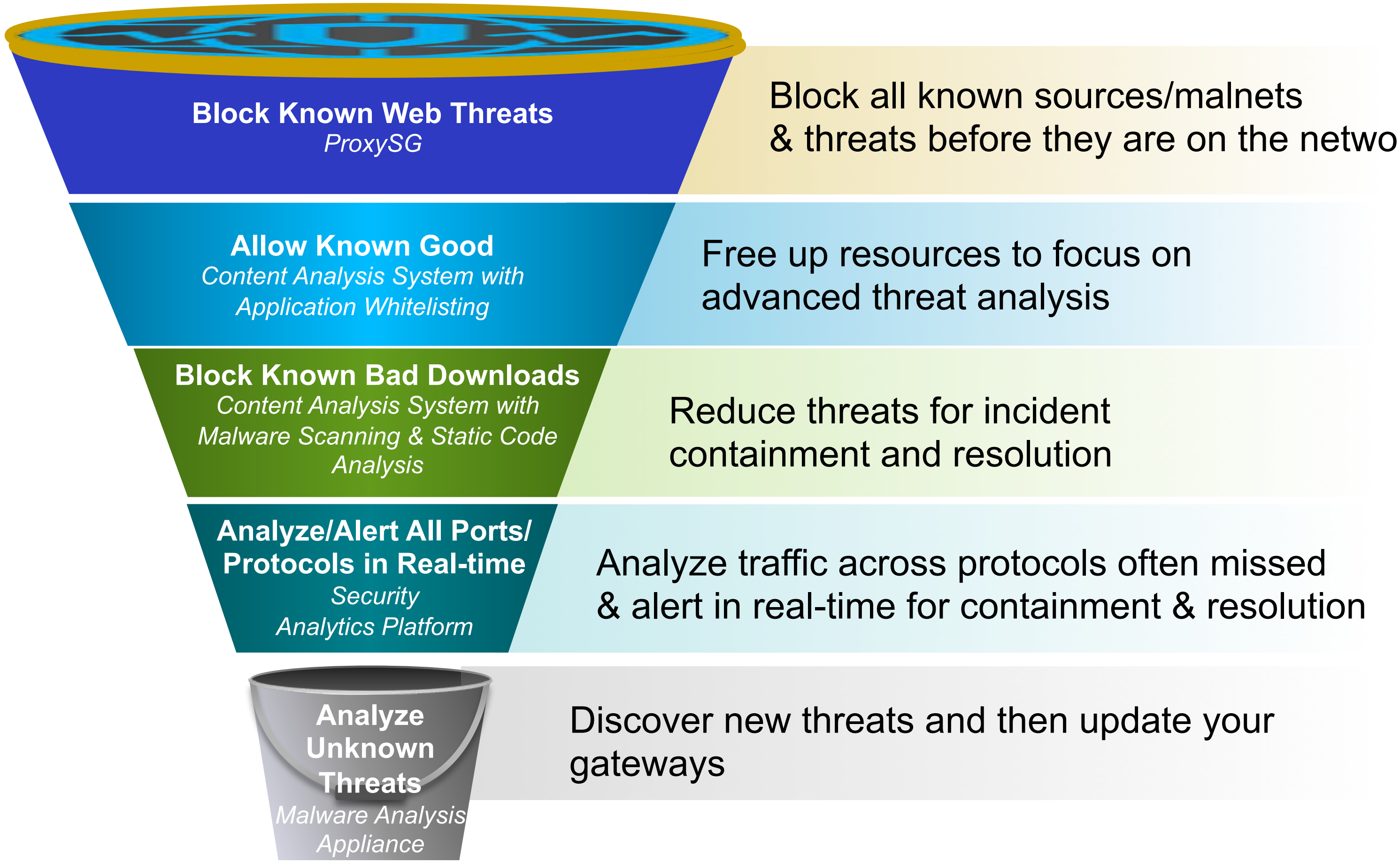
—Gartner Analyst Avivah Litan
Computerworld, 3/14/14

"….the Security software sent an alert with the generic name **"malware.binary".** It is possible that the staff could have viewed this alert as a false positive if the system was frequently alarming."

– US Senate Commerce Committee Report. 3/26/14

FOCUSING YOUR EFFORTS

Avoid the Car Alarm Syndrome



Block Known Web Threats
ProxySG

Block all known sources/malnets & threats before they are on the network

Allow Known Good
Content Analysis System with Application Whitelisting

Free up resources to focus on advanced threat analysis

Block Known Bad Downloads
Content Analysis System with Malware Scanning & Static Code Analysis

Reduce threats for incident containment and resolution

Analyze/Alert All Ports/ Protocols in Real-time
Security Analytics Platform

Analyze traffic across protocols often missed & alert in real-time for containment & resolution

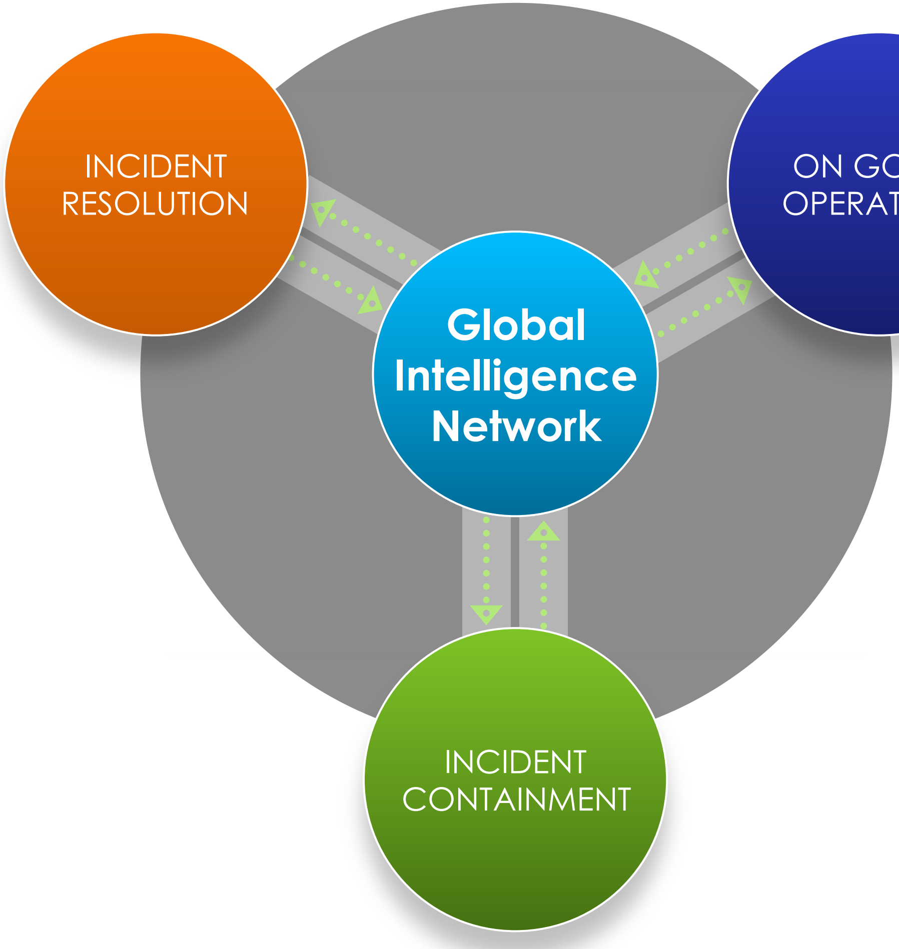
Analyze Unknown Threats
Malware Analysis Appliance

Discover new threats and then update your gateways

ADVANCE THREAT DEFENSE LIFECYCLE

INCIDENT RESOLUTION

- Investigate and Remediate Breach
- Threat Profiling and Eradication
- Retrospective Escalation



ON GOING OPERATIONS

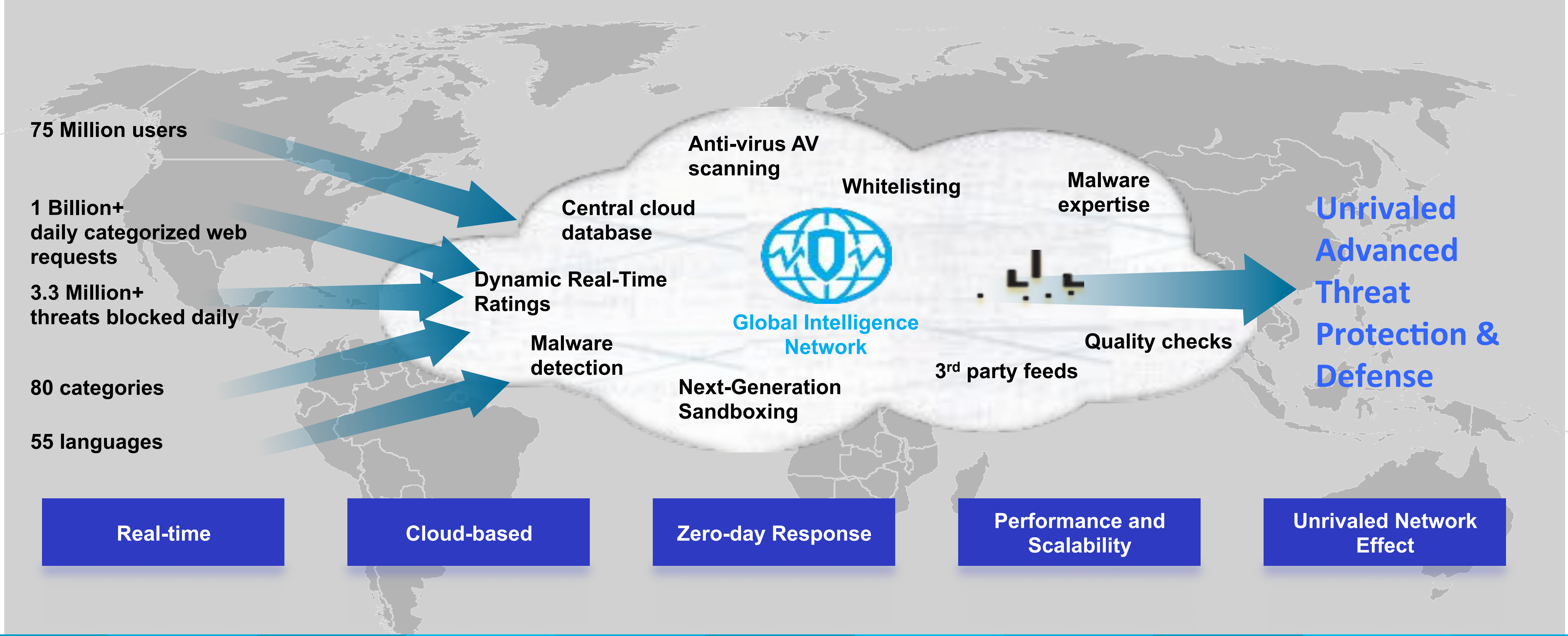
- Detect and Protect
- Block ALL Known Threats
- Fortify and Operationalize

INCIDENT CONTAINMENT

- Analyze and Mitigate
- Novel Threat Interpretation
- Unknown Event Escalation

BLUE COAT

BLUE COAT GLOBAL INTELLIGENCE NETWORK



75 Million users

1 Billion+ daily categorized web requests

3.3 Million+ threats blocked daily

80 categories

55 languages

Anti-virus AV scanning

Whitelisting

Malware expertise

Central cloud database

Dynamic Real-Time Ratings

Global Intelligence Network

Malware detection

Next-Generation Sandboxing

3rd party feeds

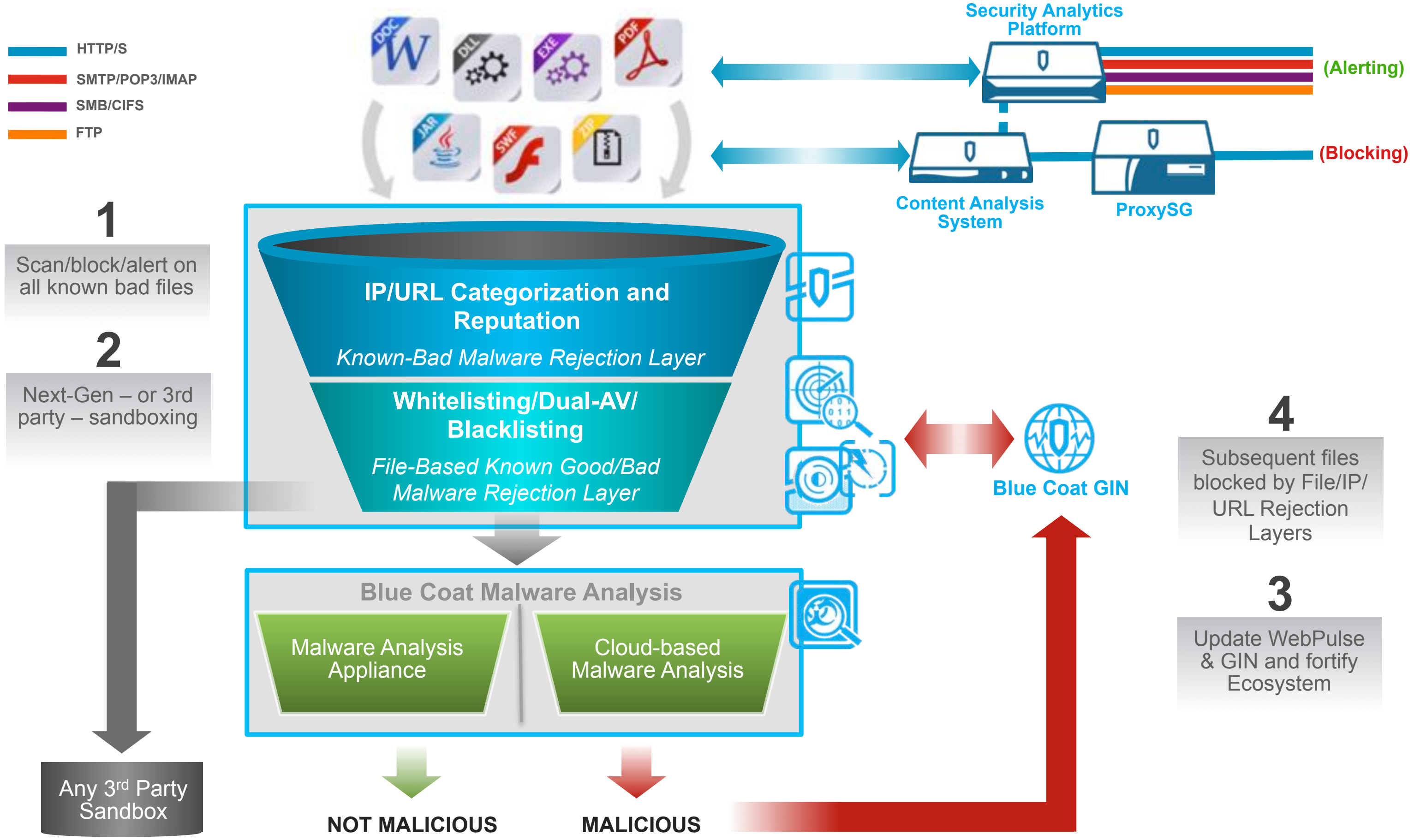
Quality checks

Unrivaled Advanced Threat Protection & Defense

- Real-time
- Cloud-based
- Zero-day Response
- Performance and Scalability
- Unrivaled Network Effect

Blocks 3.3 million threats per day

ADVANCE THREAT PROTECTION BY BLUE COAT



HTTP/S

SMTP/POP3/IMAP

SMB/CIFS

FTP

1

Scan/block/alert on all known bad files

2

Next-Gen – or 3rd party – sandboxing

IP/URL Categorization and Reputation

Known-Bad Malware Rejection Layer

Whitelisting/Dual-AV/ Blacklisting

File-Based Known Good/Bad Malware Rejection Layer

Blue Coat Malware Analysis

Malware Analysis Appliance

Cloud-based Malware Analysis

Any 3rd Party Sandbox

NOT MALICIOUS

MALICIOUS

Security Analytics Platform

(Alerting)

Content Analysis System

ProxySG

(Blocking)

Blue Coat GIN

4

Subsequent files blocked by File/IP/ URL Rejection Layers

3

Update WebPulse & GIN and fortify Ecosystem

> “Fixed fortifications are monuments to man’s stupidity.”
>
> — General George S. Patton

BLUE COAT

Network + Security + Cloud