



Enabling Effective & Efficient Investigations

Symantec Incident Response and Security Analytics

Keith Ferguson
Senior Systems Engineer
Network Forensics Team
Symantec Corporation



Quickly Closing the Window of Exposure



OUR MISSION



NET RESULT = LOWER COST

manpower, time, exposure to business and mitigated risk

Symantec Security Analytics



THE SECURITY CAMERA & DVR FOR YOUR NETWORK

Turning Complexity into Context



Providing
real-time analysis
and full visibility
of **everything**
going in and out
of your network

Records, classifies and indexes all packets and flows on high-speed networks

DPI classification of over 3,000 applications and thousands of meta attributes

On the wire, **real-time** visibility and analysis of data exfiltration & infiltration

Security Context – including reputation, user and social personas, artifacts

The 'Black Box' for incident response, forensics, root cause and impact analysis

SEE ALL. KNOW MORE. RESPOND FASTER.

Real-time Threat Analysis & Threat Reputation to Full Packet Capture



Intelligence Services

Tap the vast threat data from Symantec Global Intelligence Network to inspect all web, mail and file protocols for malicious activity and files

URL Reputation and
Content Categorization

File
Reputation

Other Indicators
of Compromise



Content/
Malware
Analysis

Suspicious files are delivered to sandbox
for inspection

Reputation Services from Multiple Sources



Global
Intelligence
Network

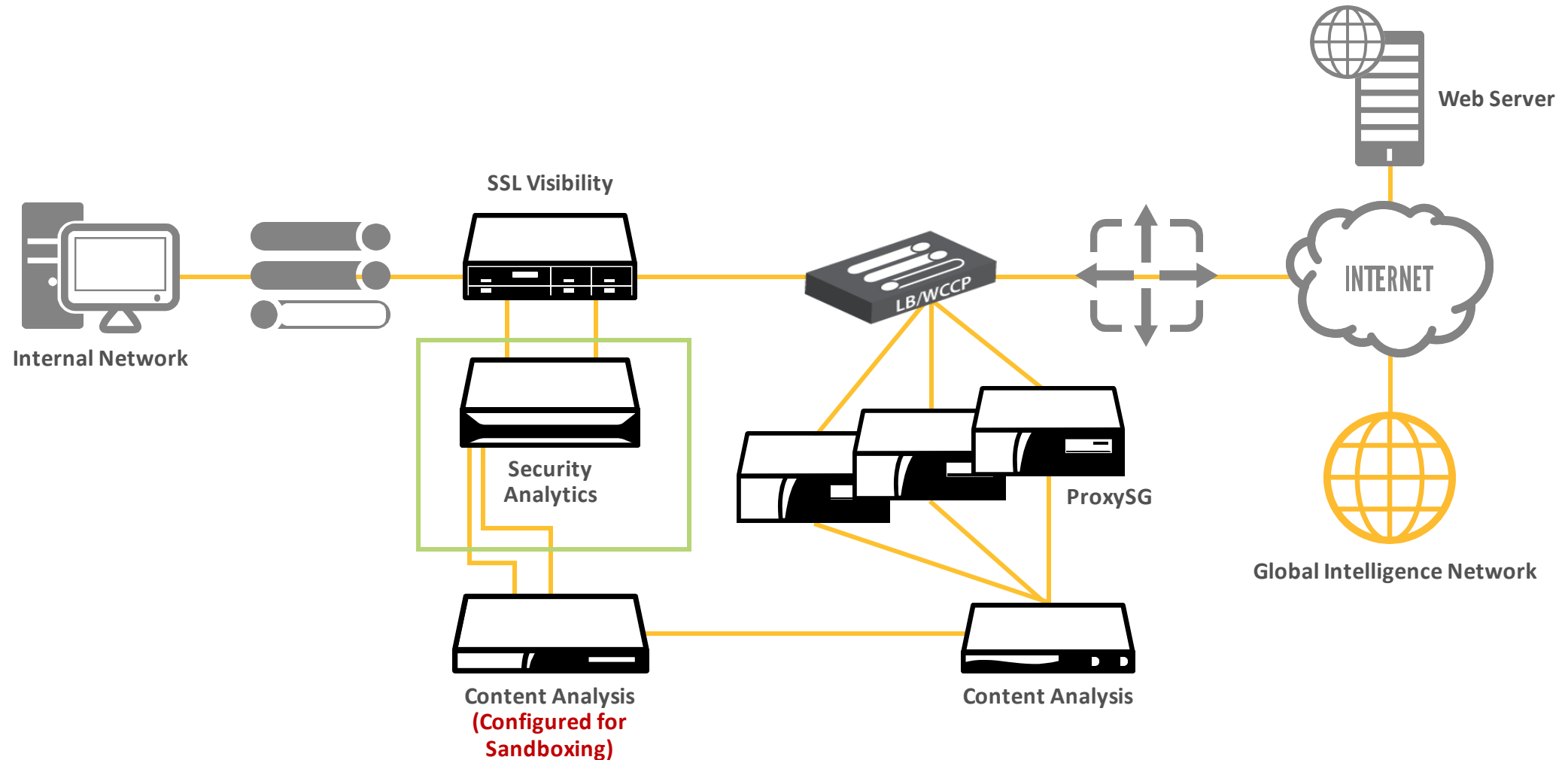


Malware
Analysis

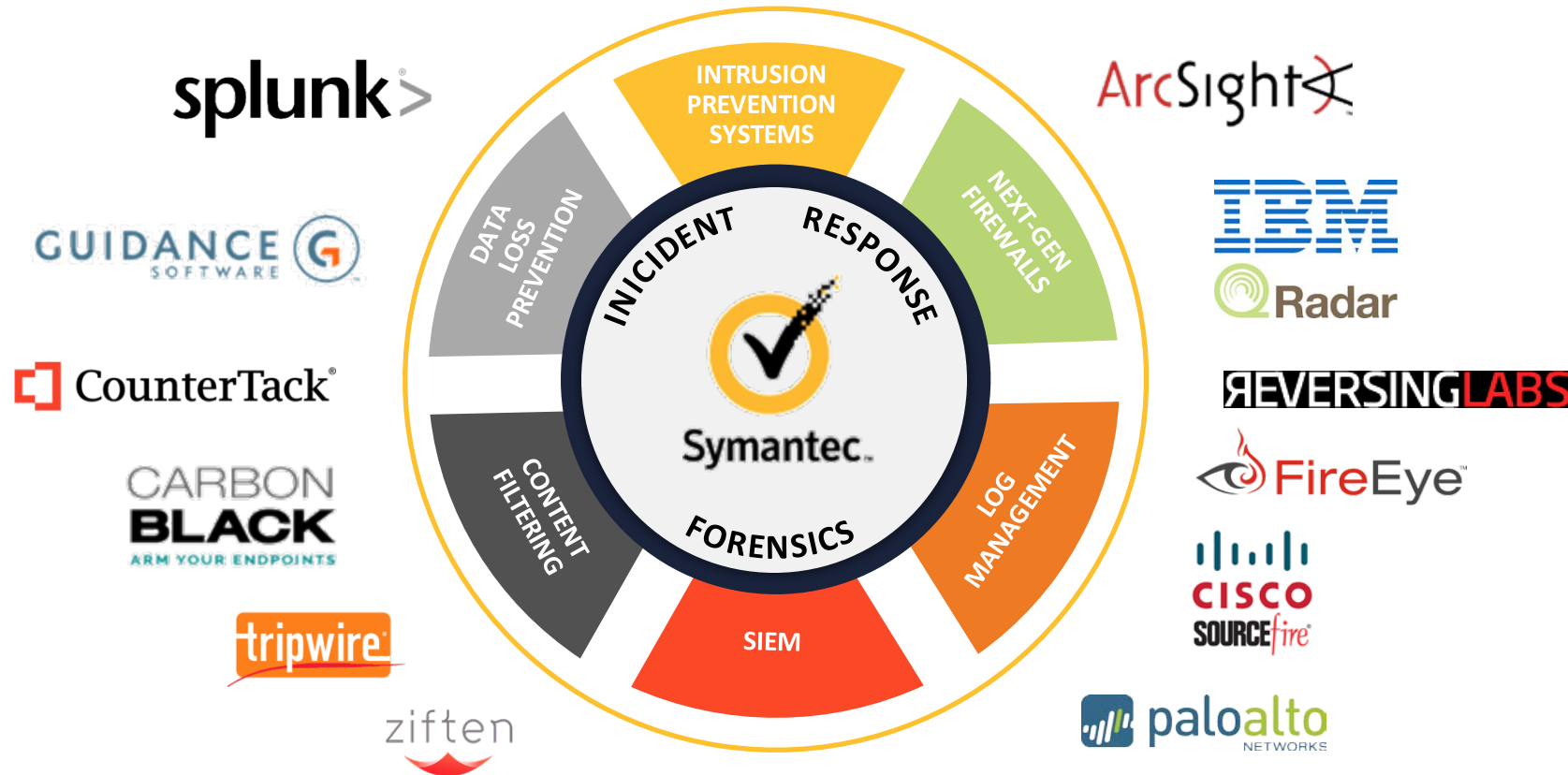


PE Scanner
jSUNPACK
Geolocation
More...

Advanced Threat Protection Architecture Including Security Analytics



Open Integration: Solid Partnerships



SECURITY ANALYTICS SUPPORTS BEST-OF-BREED INTEGRATIONS
Work Smarter & Faster – Make Better Decision

Security Analytics Components

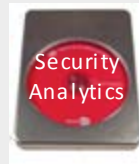


Security Analytics *Appliances*



Comprehensive, pre-configured
appliances (2G and 10G)

Security Analytics *Software*



Flexible and easy-to-deploy
on leading platforms

Security Analytics *Virtual Appliance*



Total network visibility
Absolute flexibility

Security Analytics *Central Manager*



Manage multiple
appliances/VMs

Security Analytics *Storage Modules* *Direct-attached and SAN*



Scale to any retention requirement with high-density storage options

How it Works

Security Analytics High-density storage:

- Security Analytics 1U 10G-HD Appliance
 - Same capabilities as the 10G Appliance but with Fibre Channel connectivity
 - 10G-HD Appliance # SA-S500-30-FA
- 300TB Storage Array
 - Storage Array # SA-E5660-ISA-300T (includes storage expansion license)



300TB of Usable Storage

Supported Configurations

- Up to 2 storage arrays can be directly attached.
- 3-5 arrays can be attached to a 10G-HD when deployed with a pair of Brocade 6500 series switches.

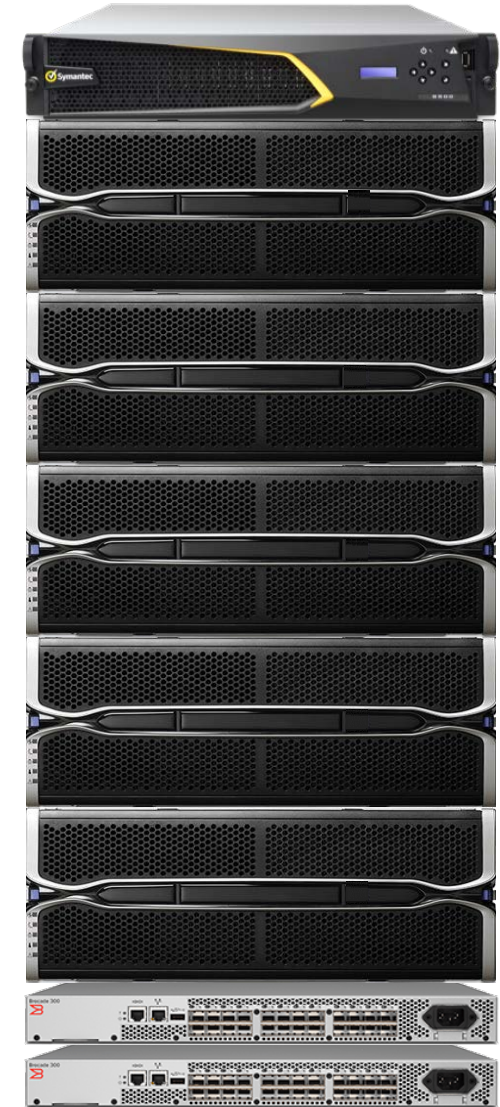
300TB



600TB



1.5PB 



Large Capacity Deployments



1.5 Petabytes of Storage

1.5PB

Security Analytics 10G-HD

5 – 300TB Storage Arrays

Brocade 6500 series
Fibre Channel Switches



Security Analytics

Key Features



Security Analytics Software Overview



- Web-based interface accessible from any browser
- Deep analysis of every network event
- Alerts for “up-to-the-minute” notification of suspicious, malicious, or prohibited behavior
- Investigator’s interface quickly narrows or expands scope, shifts timeline
- Event and file recreation through “Extractions”
- Interactive reports on essential Layer 2-7 metadata

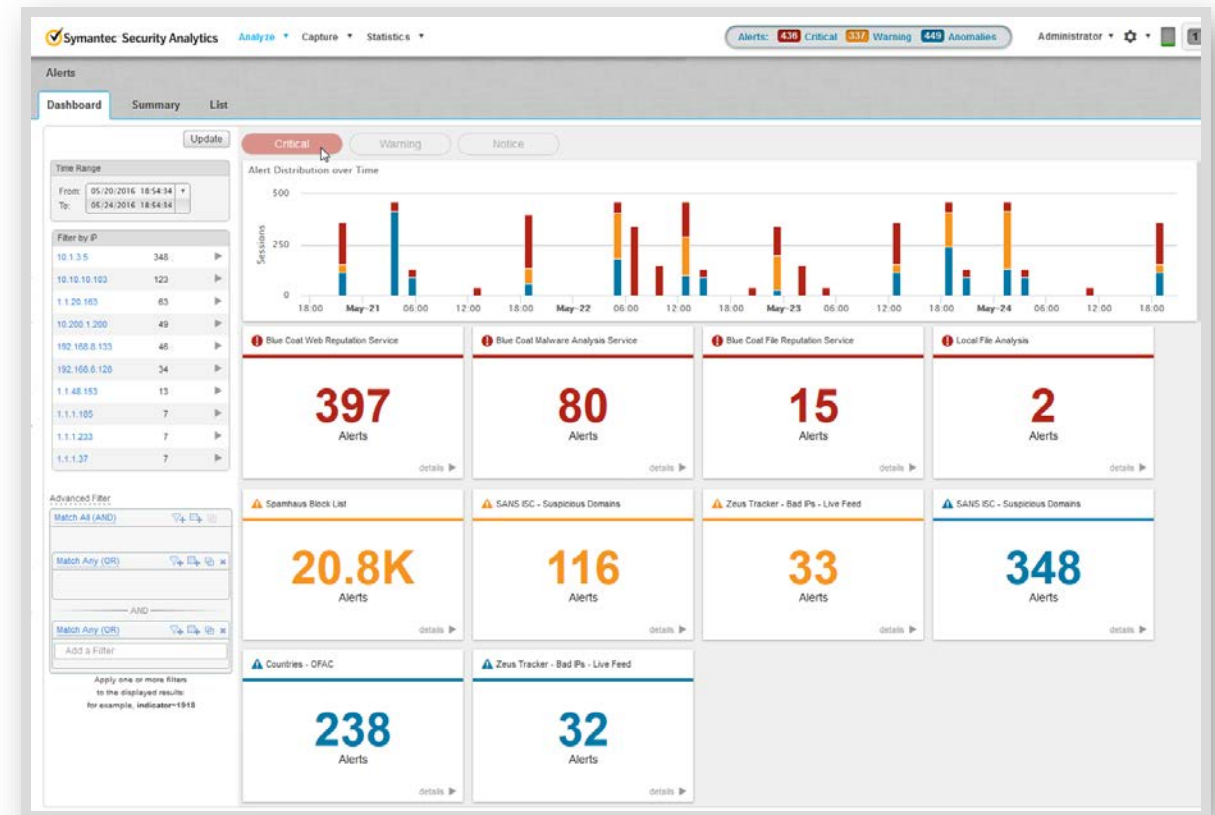


Alerts Management Dashboard



Incident Response Launchpad

- Key alerts at your fingertips
- “What is critical to my organization?”
- What should I focus on?
- Timeline of alerts
- Pivot directly to detailed reports
- Assign alert to analysts and manage status
- **New:** Assign alert to analysts and manage status
- **New:** Exposed via API

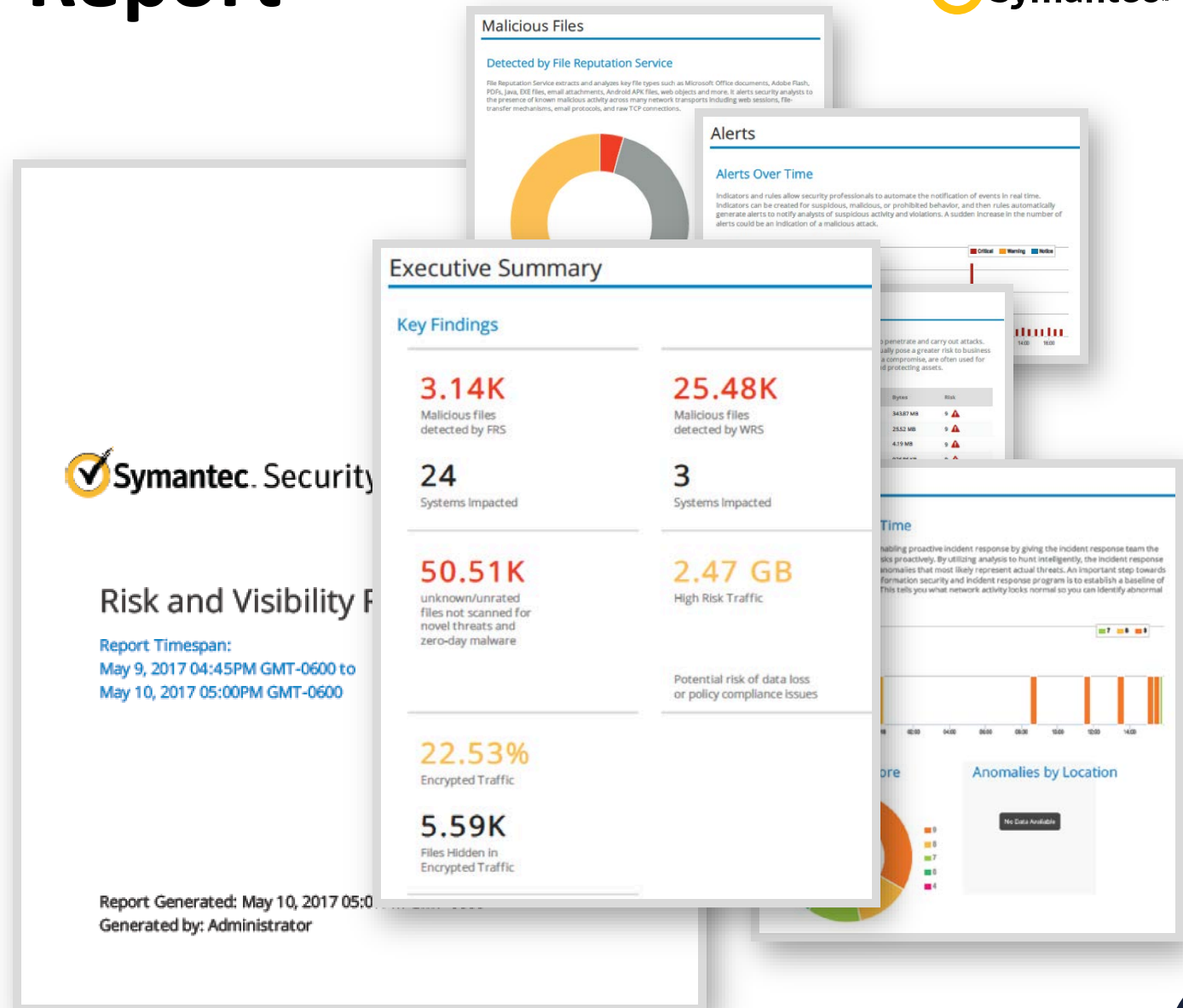


New – Threat Analysis Report



Push Button – See Results!

- Capture network traffic
- Push button
- Generate report with executive summary
- See exactly what's happening on your network
- Reports on alerts, malicious files, SSL traffic, risky applications, anomalies and more

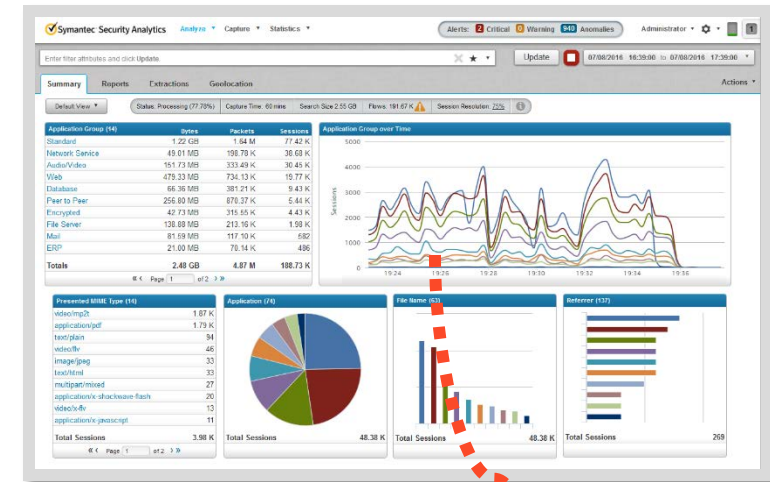


New – Symantec ATP Integration

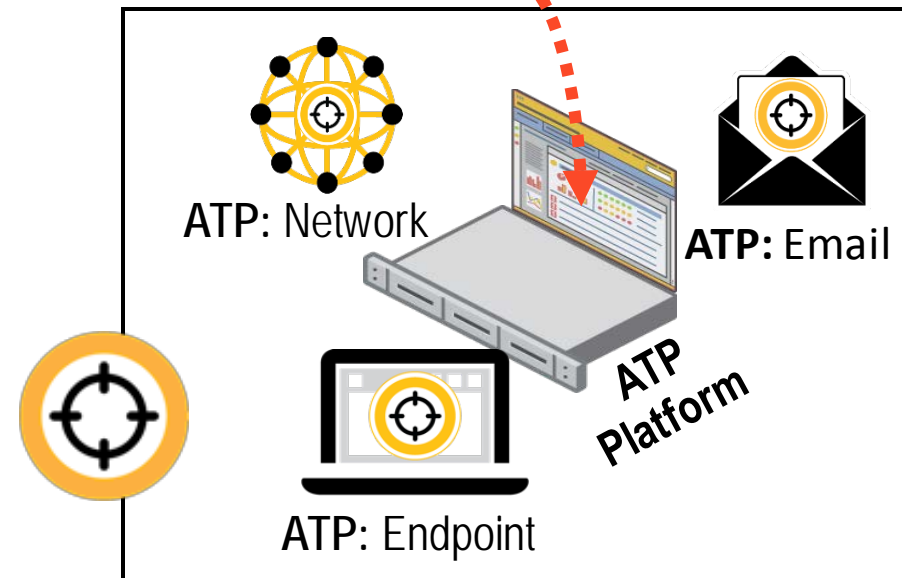


Network to Endpoint Visibility

- Expand investigations into the ATP console
- Pivot from correlated network findings within Security Analytics
- Endpoint, network, and email convictions
- ATP provides a layered approach at the email, cloud, network, and endpoint levels



Security
Analytics

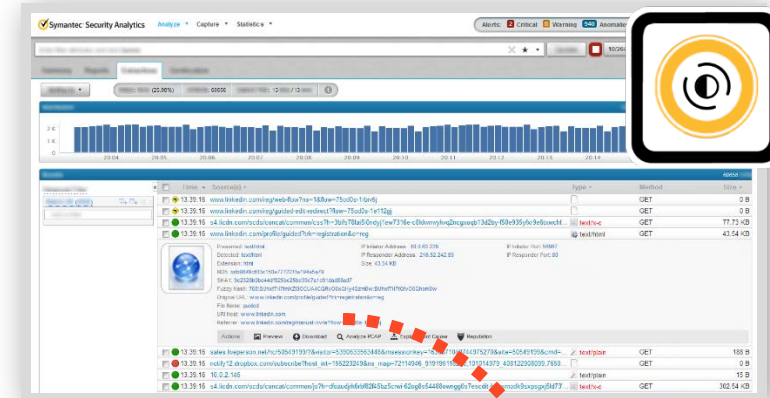


New – Symantec DeepSight™ Integration



Deep Adversary Intelligence

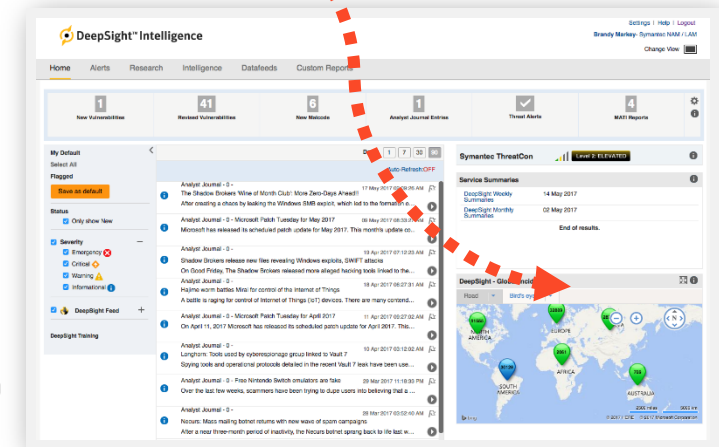
- Pivot from Security Analytics to DeepSight™
- Detailed adversary threat intelligence
 - vulnerabilities, malware, indicators of compromise, campaigns, tactics/techniques/procedures, and profiles
- Full view of relevant threats and exposures
- Managed Adversary and Threat Intelligence (MATI) research
- Directed Threat Research (DTR)
- Full range of technical intelligence



Security Analytics

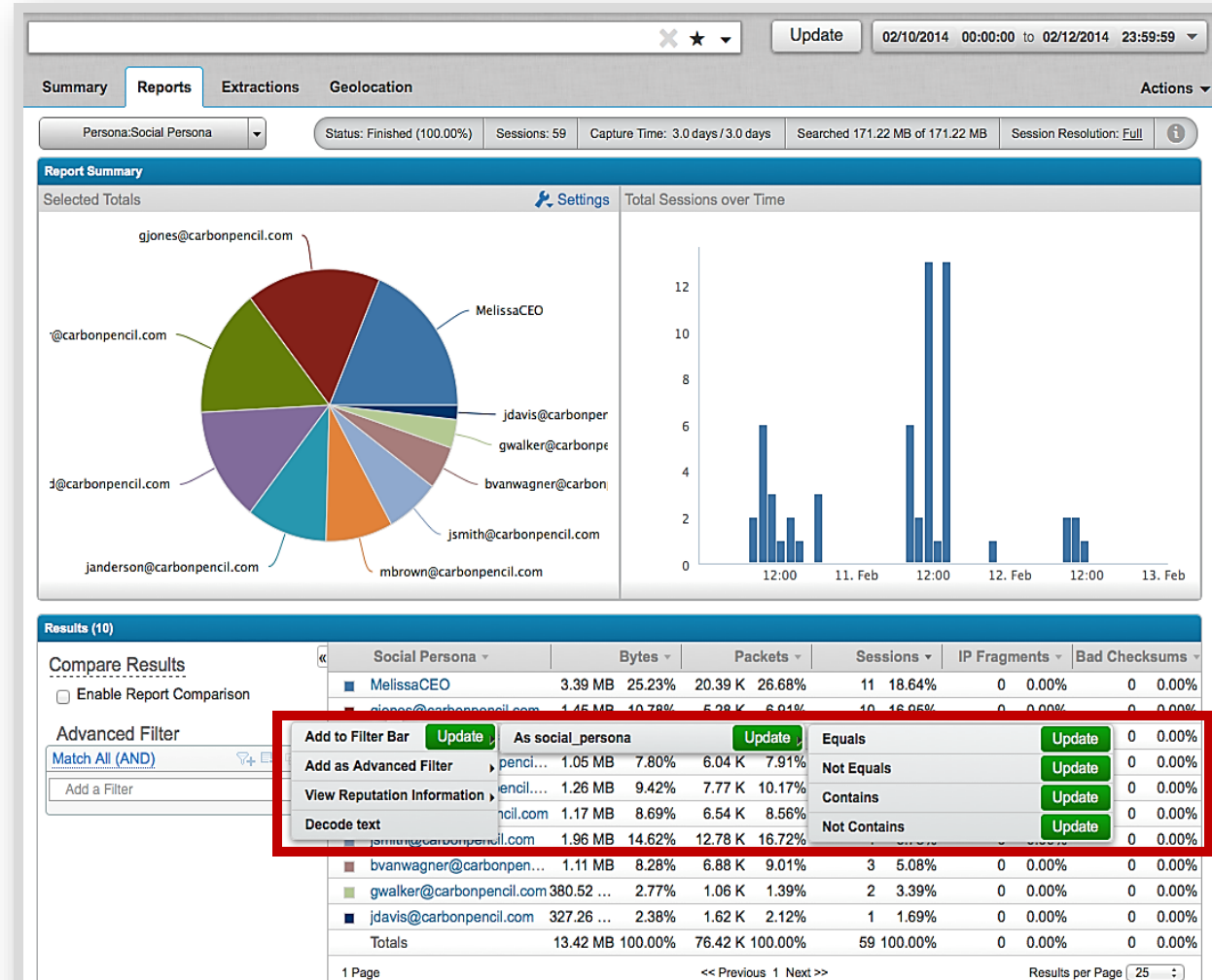
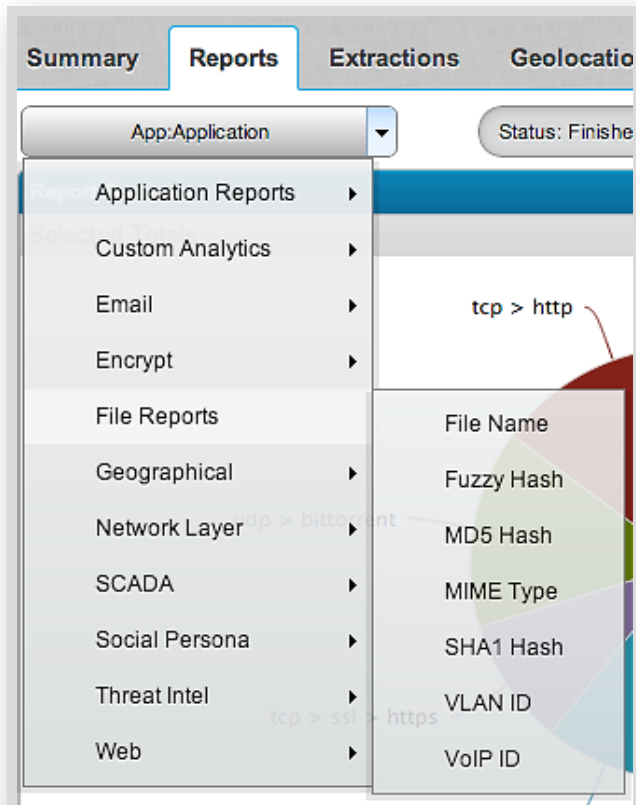


DeepSight™
Intelligence



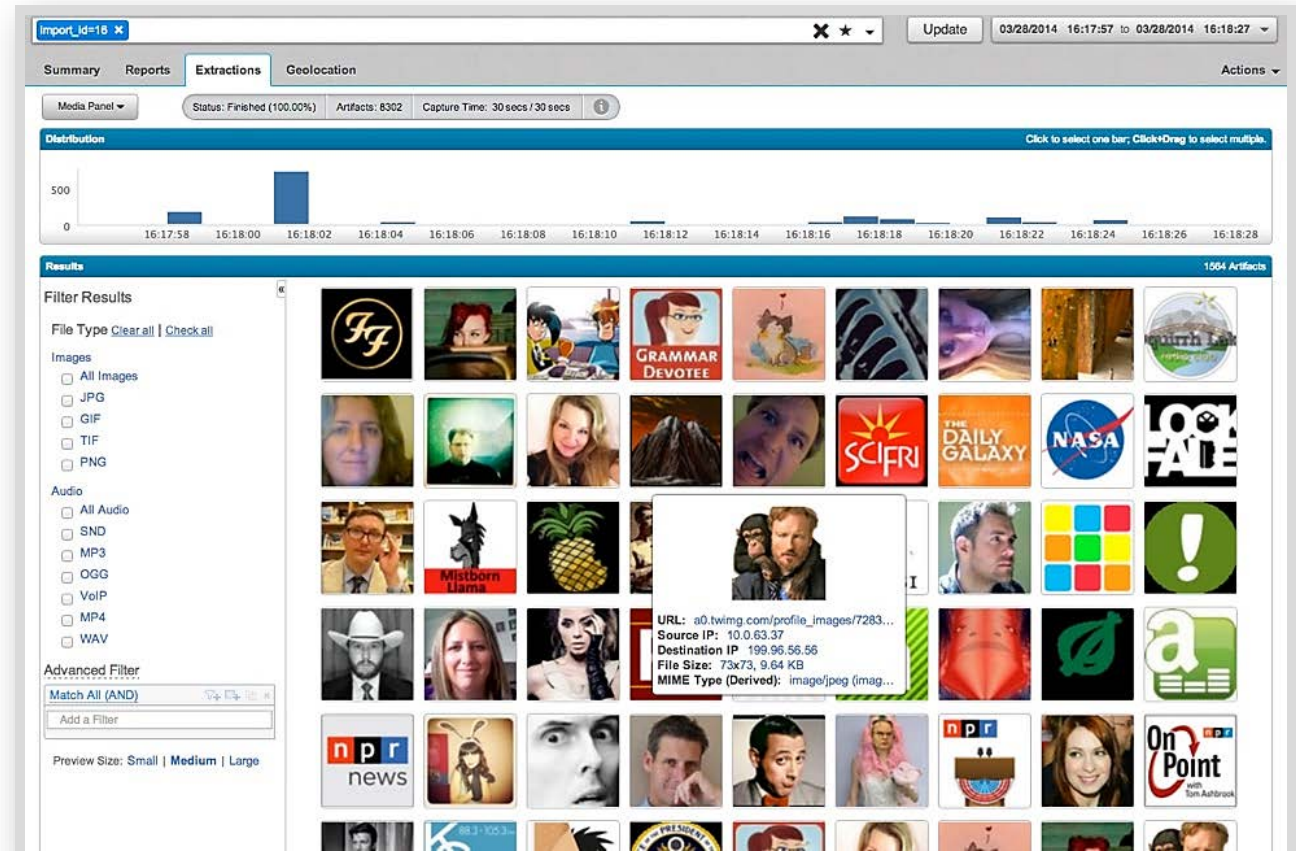
Reports

Numerous customizable reports to instantly view granular detail of all event activity



Media Panel

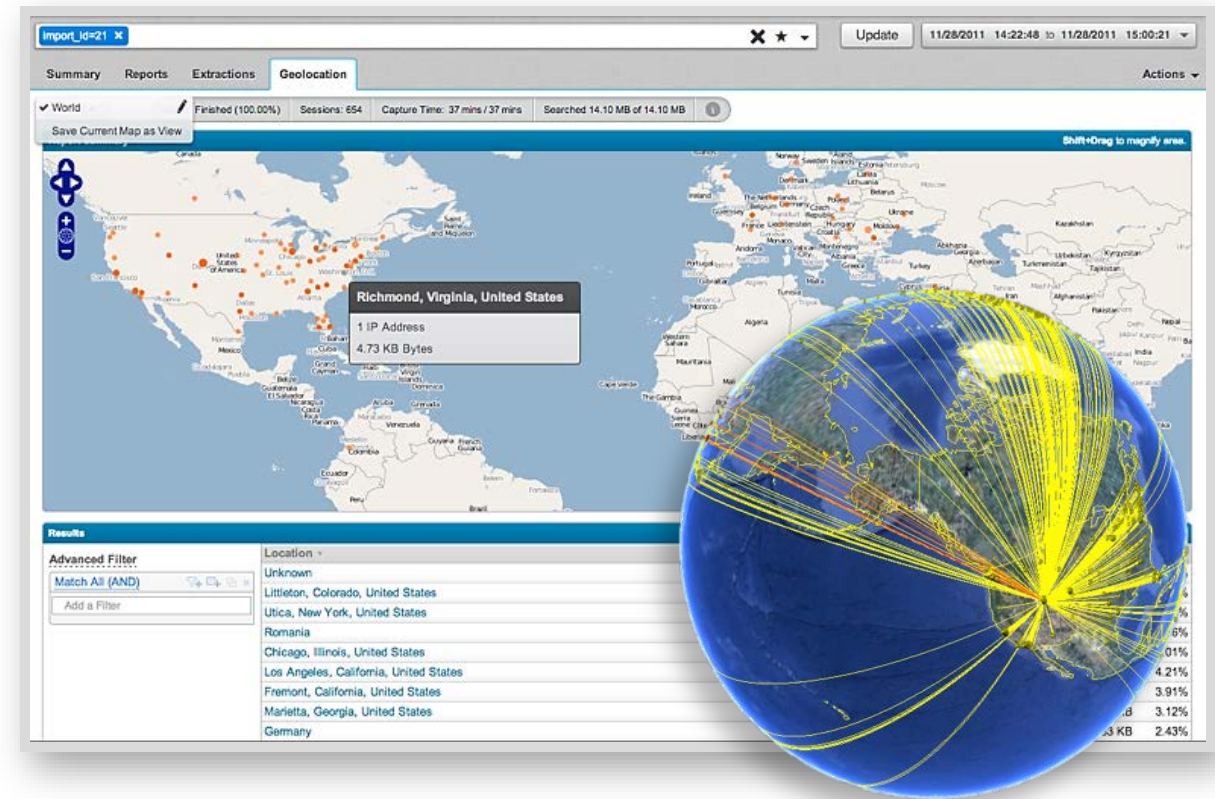
- Quickly analyze all images/audio files recreated from raw packets
- Filter by file type, extension, size
- See all associated metadata
 - URL
 - Source IP
 - Destination IP
 - Size
 - MIME Type



*A Picture is worth a thousand words.
“No denying what my user saw...good or bad”.*

Geolocation

- Visually identify traffic (and volume of traffic) to locations of interest
- Filter and alert on traffic to suspect countries
- Integrated map database requires no external connection
- Configurable location of private networks
- Export data and view time-based representation of connections in Google Earth™

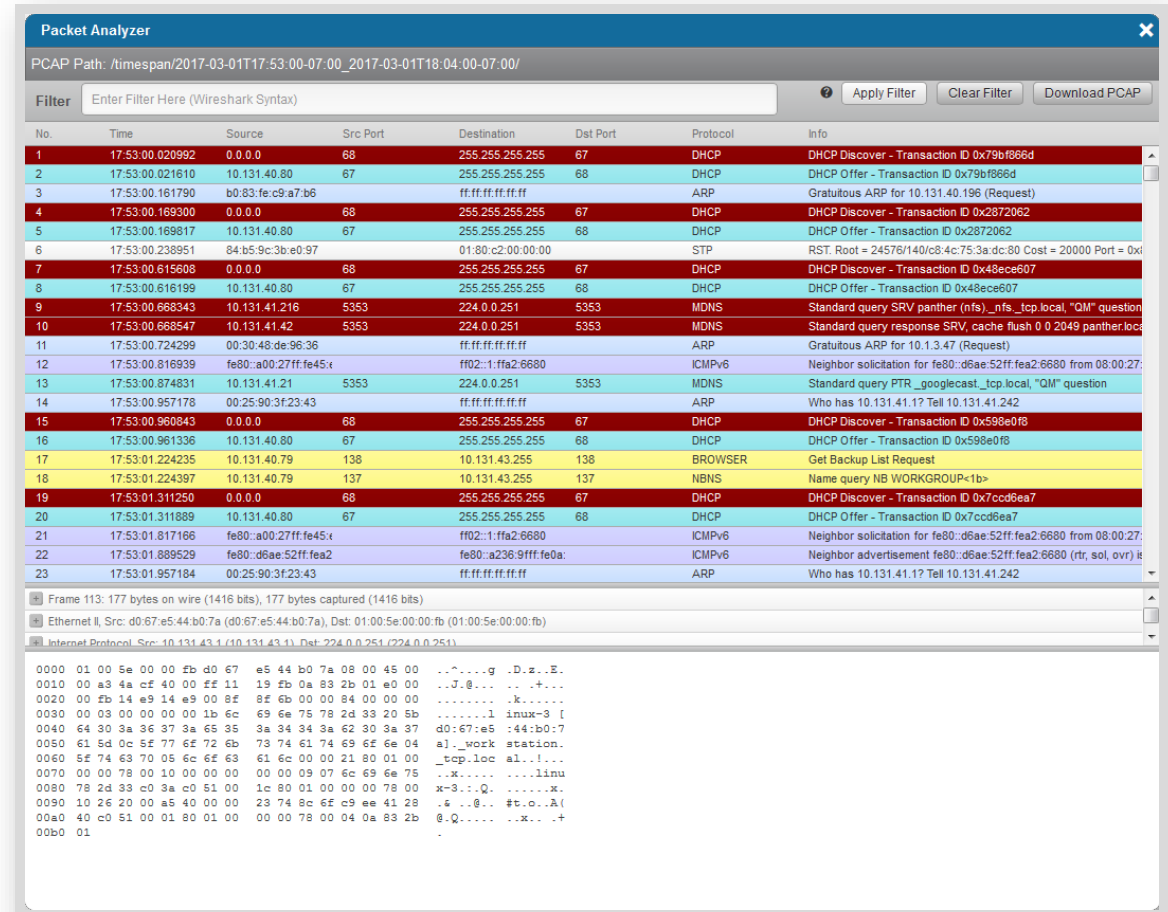


See hotspots of activity and where your traffic is coming from...and going to
“Traffic to North Korea – that’s not right!”

Packet Analyzer



- Enter Packet Analyzer through multiple starting points
- Save time: filter and view packets before transferring PCAPs over the wire
- No need to launch outside packet analysis applications



*No more waiting to download a huge file for Wireshark to analyze.
It's "Wireshark directly on the server – that's efficient!"*

Comparative Reporting

- Compare data to previous periods to identify abnormal patterns
- Establish a baseline and target deviations
- Understand trends over time

Results (124)

Compare Results

☒ Enable Report Comparison

Bytes Packets Sessions

Comparison Time Range

From: 03/28/2014 16:17:57 To: 03/28/2014 16:18:17 Update

Advanced Filter

Match All (AND)

Add a Filter

Application	Previous	Current	Change	Change %
tcp > ssl > https	1.38 GB	1.70 GB	322.29 MB	22.73%
tcp > http > youtube	21.39 MB	81.10 MB	59.71 MB	279.14%
tcp > http	13.46 MB	34.55 MB	21.09 MB	156.72%
tcp > http > redhat_update	0 B	7.58 MB	7.58 MB	-
tcp > unknown	9.28 MB	15.73 MB	6.45 MB	69.57%
tcp > http > pandora	0 B	4.16 MB	4.16 MB	-
tcp > ssl > https > salesforce	613.27 KB	2.33 MB	1.73 MB	289.54%
tcp > http > linkedin	550.41 KB	2.06 MB	1.52 MB	283.04%
tcp > http > google_gen > google	634.94 KB	2.10 MB	1.48 MB	238.63%
tcp > ssl > https > google	504.09 KB	1.83 MB	1.34 MB	272.02%
tcp > ssl > jabber	1.36 MB	2.58 MB	1.22 MB	89.38%
tcp > http > firefox_update > mozilla	0 B	1.05 MB	1.05 MB	-

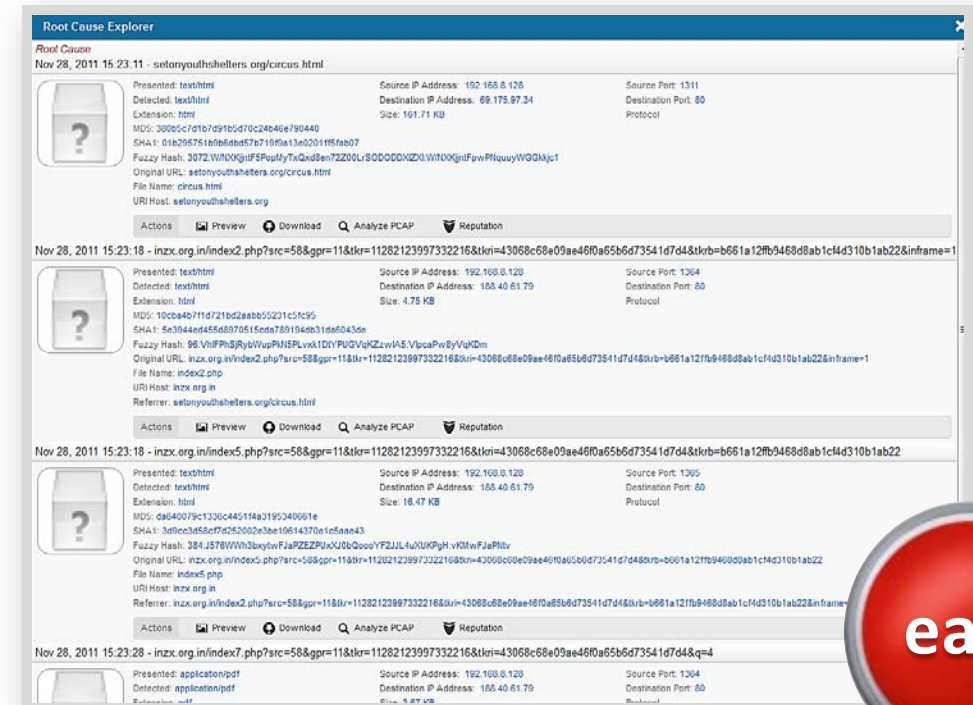
"I can compare traffic against a 'normal' window of traffic and identify anomalies or discover trends."

Root Cause Explorer



Context, multiple data sources to attribution

- Automates tracing of HTTP referrer chains
- Correlates relevant email, IM, and HTTP information for quick analysis



You've made one of the most time-consuming, rote functions of my job as simple as pushing a button ...That was easy!"

Reputation Services/Data Enrichment



On-demand Reputation Checks, including:

- ISC/SANS
- Google SafeBrowse
- VirusTotal
- CarbonBlack
- LastLine
- Domain Age
- RobTex
- SORBS
- WHOIS



Reputation Information

Local File Analysis
File: www.jailbreakme.com/saffron/_/iPad_4.3.3_8J2.pdf
Overall Verdict: 5/10
ClamAV: False

Blue Coat File Reputation Service
File: www.jailbreakme.com/saffron/_/iPad_4.3.3_8J2.pdf
Overall Verdict: 10/10
Anti Virus Last Seen Date: 2012-09-11 19:22:57
Anti Virus Engines Count: 21
Anti Virus Engines:
ESET-NOD32: PDF/Exploit.Pidief.PGP
Ikarus: Exploit.iPhoneOS
AntiVir: EXP/Pidief.aar
McAfee: Artemis!EB8A08346AED
PCTools: Trojan.Gen
Kaspersky: Exploit.IphoneOS.Pdfka.c
Antiy-AVL: Exploit/IphoneOS.Pdfka
DrWeb: iPhoneOS.Cydia
Emsisoft: Exploit.iPhoneOS!IK
VIPRE: Exploit.iPhoneOS.Pdfka.a (v)
BitDefender: Exploit.PDF.AM
GData: Exploit.PDF.AM
Fortinet: W32/IphoneOS_Pdfka.C!tr
TrendMicro-HouseCall: TROJ_PIDIEF.SMXZ
nProtect: Trojan-Exploit/W32.Pidief.17682.JTQ
TrendMicro: TROJ_PIDIEF.SMXZ
Avast: Other:Malware-gen Trj
F-Secure: Exploit:W32/Pidief.DFY
Comodo: UnclassifiedMalware
ViRobot: Trojan.IphoneOS.A.EX-Pdfka.17682
Sophos: Troj/PDFEx-ES

Blue Coat Web Reputation Service
Url: www.jailbreakme.com/saffron/_/iPad_4.3.3_8J2.pdf
Category: Hacking

"I can lookup IPs, URLs, files and hashes against multiple reputation services? Multiply 12 keystrokes and 2 browser tabs by 100x a day and you just gave me an extra day a month!"

Anomaly Detection

That looks odd! I better take a look!

Automated machine learning determines
“Normal” baseline

Sophisticated statistical modeling identifies
“Abnormal” activity

Reduce manual effort, human effort,
and false positives → resolve faster

Combine behaviors to show correlated anomaly

- One indicator = not so suspicious ... multiple indicators = I better look!

Why is Anomaly Detection unique?

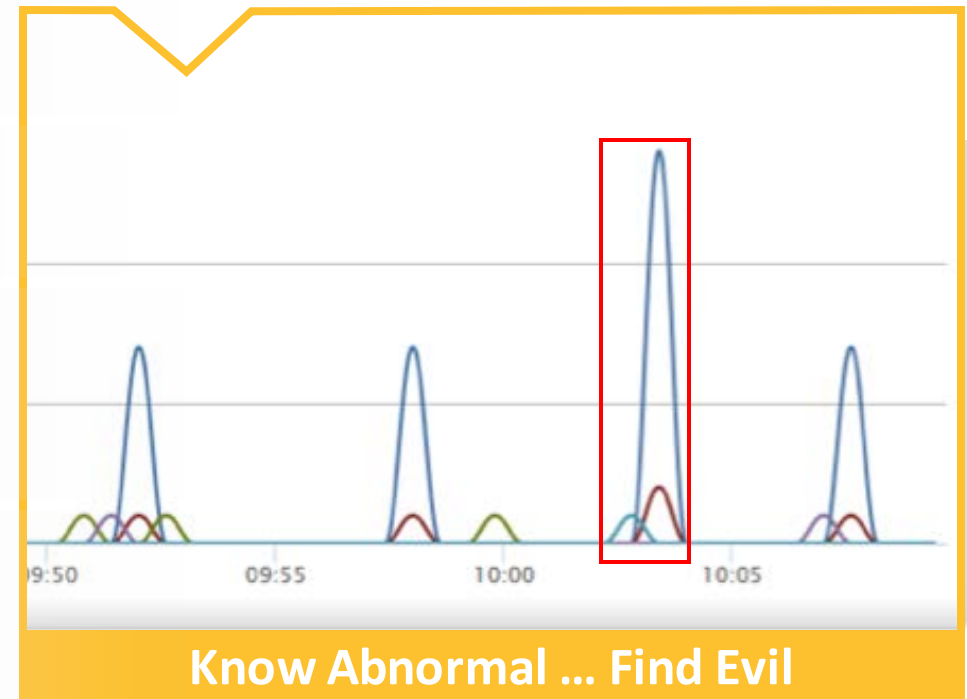
- It's your data, your activity, your patterns ... your threats
- Find problems that your Static signature tools miss
- Combined with full packet capture = complete evidence

“

Organizations need to understand their environment and what constitutes normal and abnormal behavior, train staff on how to use analytic tools and define the data they need to collect.

- SANS

”



Key Anomaly Detection Use Cases



Identify unusual counts, signatures, protocols, and destinations



Detect high traffic to and from a restricted country



Detect suspicious movement within the network



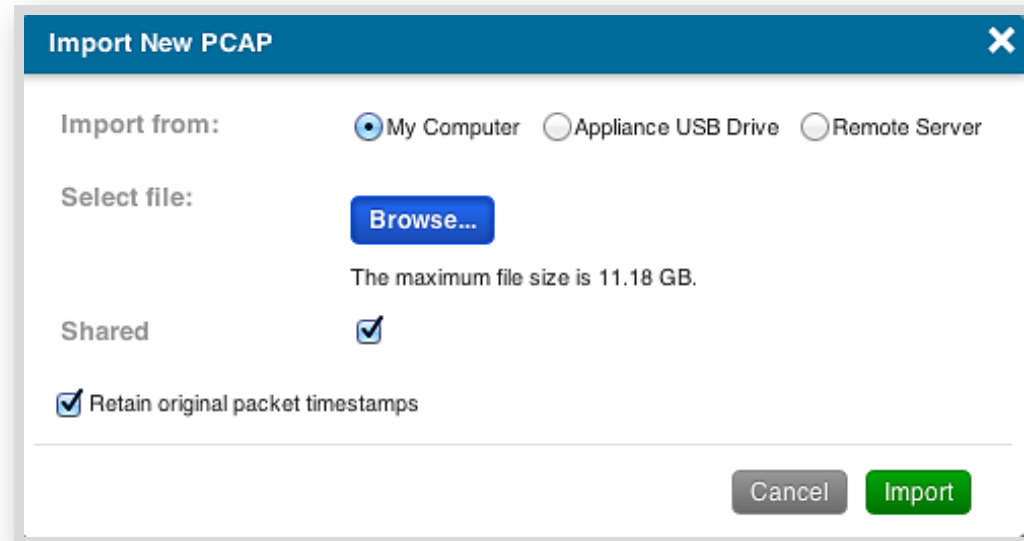
Detect data exfiltration via web, email or application



Detect a sudden spike in activity for a specific application type

PCAP Import

- Rich analysis now applied to PCAPs from other sources
- Optimize available appliance storage – save captured data to PCAP for later import as needed
- Allows analyst to obtain high-level information quickly to aid investigation targeting



*Packet Renaissance –
“It’s like I’ve traveled back in time and made my old data more valuable.”*

Extended Metadata Retention



- Independent allocation of storage for metadata and full packets
- Allows for retention and analysis of multiple generations of metadata (weeks/months/...)
- Enables long-term trend analysis window
- Optimize limited amount of storage



*"I can save full packet data for a comfortable window of a few weeks or a month, but can **save the metadata for many months or more to see trends.**"*

Capture-only Mode

- When Packet Capture is Primary Objective
- Switch off data enrichment
- Ensure 24/7 full packet capture
- Boost performance to 10Gbps sustained capture on a single appliance



“Performance is key. I just want the packets”

Dynamic Filtering

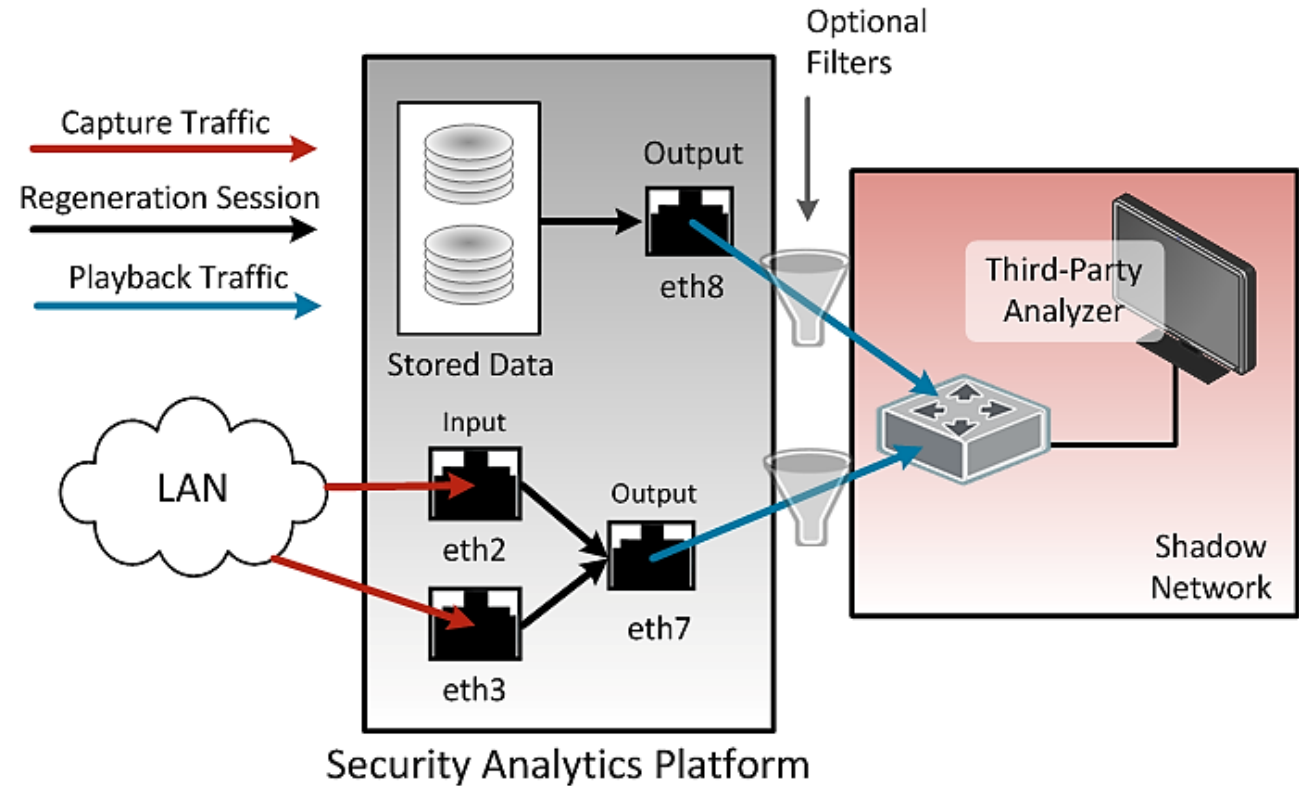
Selectively filter (not capture) packets based on indicators settings



Should it stay or should it go? – Prioritize available capture storage

Playback

- Transmit captured data flows to third party tools for further analysis
- Regenerate traffic with less than 1 ms of latency, even on 10GBps networks
- Throttle traffic playback so other tools don't bog down
- Replay traffic to other tools to validate effectiveness

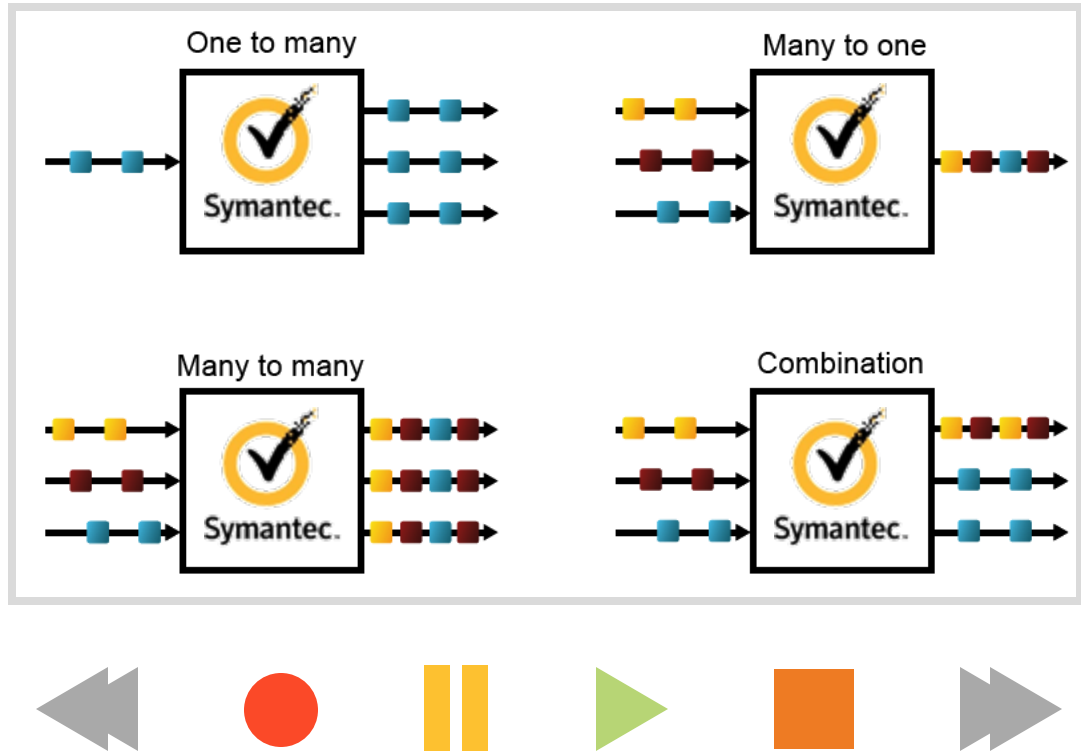


*"This is the DVR for my network.
I can confirm that my other security tools are effective after signature updates."*

Filter and Replay Network Traffic



- Replay any traffic
- Combine segments
- Throttle playback
- Filter Inbound/Outbound Traffic by protocol, IP, MAC address, payload type, or unique bit pattern
- Filter at the header or payload level
- Multiple filters – start and stop at any time, continue to capture
- Import filters using standard Berkley Packet Filter (BPF) format



"I can optimize the use of my available storage and capture and replay just what I need to"

Security Analytics

Partner Integrations
(Network Security)



ArcSight™ Integration



The screenshot displays the ArcSight Console 6.5.0.1459.0 interface. The main window shows a list of events under the 'Active Channel: 24hr Critical IDS' filter. The 'Inspector/Event' pane on the right shows details for an event titled 'EXPLOIT-KIT Blackholev2 exploit kit url structure detected'. A context menu is open over the event list, with the 'Blue Coat Security Analytics' option highlighted in red. The menu includes options like 'Integration Commands', 'Tools', 'Export', 'Add to Case', 'Print Selected Rows', 'Payload', 'Report', 'Close', 'Knowledge Base', 'Reference Pages...', and 'Help'. The 'Blue Coat Security Analytics' option is located at the bottom of the menu.

Manager Receipt Time	End Time	Name	Attacker Address	Target Address	Priority
2 Sep 2014 21:51:50 PDT	3 Sep 2014 00:46:38 PDT	EXPLOIT-KIT Phoenix exploit kit post-compromise behavior	192.168.100.130	203.114.112.156	7
2 Sep 2014 21:51:50 PDT	3 Sep 2014 00:46:38 PDT	MALWARE-CNC Win.Trojan.Zeus encrypted POST Data exfiltration	192.168.100.130	203.114.112.156	7
2 Sep 2014 21:51:50 PDT	3 Sep 2014 00:46:38 PDT	MALWARE-CNC Win.Trojan.Fareit variant outbound connection	192.168.100.130	203.114.112.156	7
2 Sep 2014 21:51:50 PDT	3 Sep 2014 00:46:38 PDT	EXPLOIT-KIT Blackholev2 exploit kit url structure detected	192.168.100.130	203.114.112.156	7
2 Sep 2014 21:51:45 PDT	3 Sep 2014 00:46:36 PDT	EXPLOIT-KIT Multiple exploit kit Payload detection - readme.exe	192.168.100.130	203.114.112.156	7
2 Sep 2014 21:51:25 PDT	3 Sep 2014 00:36:00 PDT	OS-WINDOWS DCERPC NCACN-IP-TCP srsvnc NetPathCanonicalize c	192.168.100.130	203.114.112.156	7
2 Sep 2014 21:51:25 PDT	3 Sep 2014 00:38:30 PDT	EXPLOIT-KIT Blackholev2 exploit kit url structure detected	192.168.100.130	203.114.112.156	7
2 Sep 2014 21:51:25 PDT	3 Sep 2014 00:38:31 PDT	EXPLOIT-KIT Multiple exploit kit Payload detection - readme.exe	192.168.100.130	203.114.112.156	7
2 Sep 2014 21:51:25 PDT	3 Sep 2014 00:38:40 PDT	EXPLOIT-KIT Phoenix exploit kit post-compromise behavior	192.168.100.130	203.114.112.156	7
2 Sep 2014 21:51:25 PDT	3 Sep 2014 00:38:40 PDT	MALWARE-CNC Win.Trojan.Zeus encrypted POST Data exfiltration	192.168.100.130	203.114.112.156	7
2 Sep 2014 21:51:18 PDT	2 Sep 2014 22:29:55 PDT	EXPLOIT-KIT Blackholev2 exploit kit url structure detected	192.168.100.130	203.114.112.156	7

Splunk™ Integration



splunk> App: Blue Coat Security Analytics App For Splunk

Blue Coat Security Analytics For Splunk Dashboard Views Threat Views Search

New Search

index=estreamer sourcetype=estreamer

71,951 of 71,951 events matched

Events (71,951) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect

Oct 22, 2014

List Format 50 Per Page

< Hide Fields All Fields

Selected Fields

- host 1
- source 1
- sourcetype 1

Interesting Fields

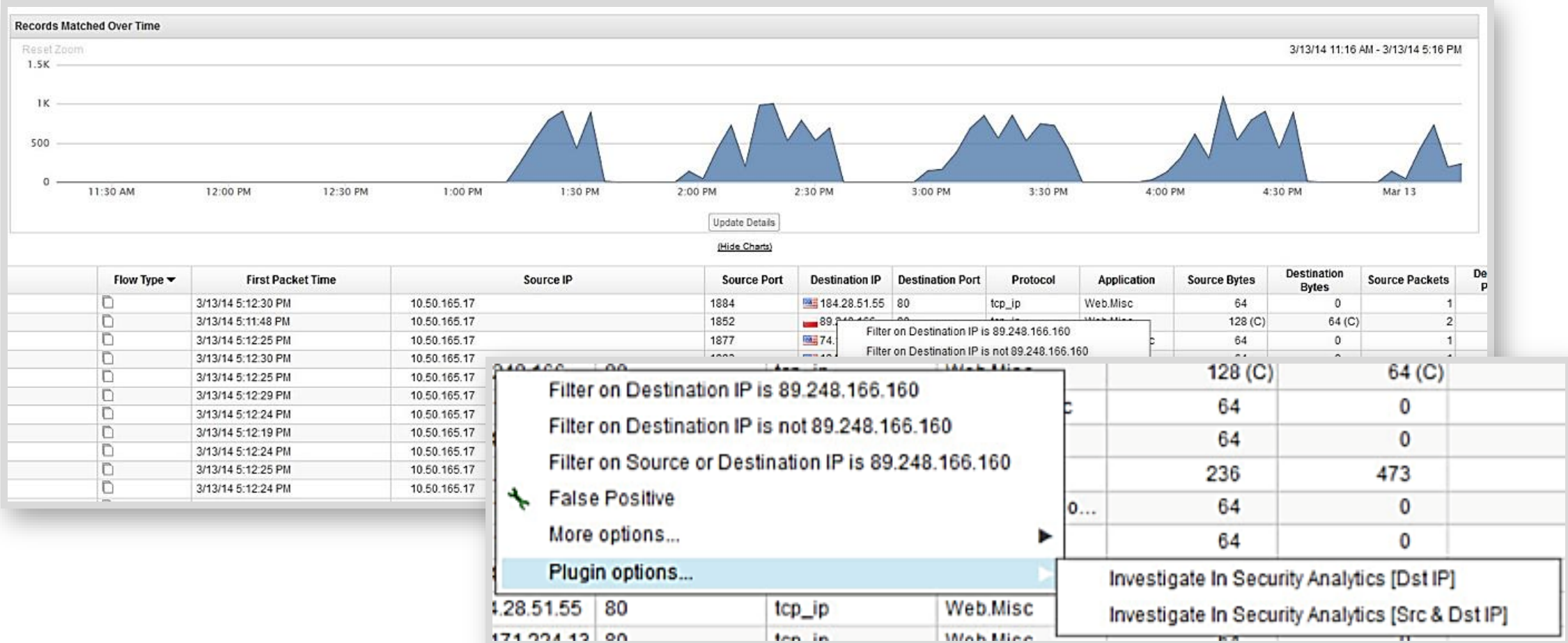
- app_proto 1
- blocked 2
- class 13
- class_desc 13
- client_app 1
- connection_id 1
- connection_sec 1
- date_hour 24
- date_mday 31
- date_minute 60
- date_month 7

i	Time	Event
>	4/7/15 11:35:33.000 AM	rec_type=9 rec_type_simple=IMPACT event_sec=1428431733 event_id=132455 sensor=172.21.0.1 host = blackhole source = eStreamer sourcetype = eStreamer
>	4/7/15 11:35:33.000 AM	rec_type=400 rec_type_simple="IPS EVENT" event_sec=1428431733 event_usec=917257 sensor=172.21.0.1 c="A Network Trojan was Detected" ids_policy="Initial Passive 0-0000-0000-000000000000 sec_0
>	4/7/15 11:35:33.000 AM	rec_type=9 rec_type_simple=IMPACT event_sec=1428431733 event_id=132455 sensor=172.21.0.1 host = blackhole source = eStreamer sourcetype = eStreamer
>	4/7/15 11:35:33.000 AM	rec_type=9 rec_type_simple=IMPACT event_sec=1428431733 event_id=132455 sensor=172.21.0.1 host = blackhole source = eStreamer sourcetype = eStreamer
>	4/7/15 11:35:33.000 AM	rec_type=400 rec_type_simple="IPS EVENT" event_sec=1428431733 event_usec=917257 sensor=172.21.0.1 c="A Network Trojan was Detected" ids_policy="Initial Passive 0-0000-0000-000000000000 sec_0

Event Actions

- Build Event Type
- Extract Fields
- Analyze IPs with Security Analytics
- Show Source

IBM QRadar™ Integration





Thank You

