



LookingGlass Solution Overview



LOOKINGGLASS



LookingGlass Product Portfolio



Threat Intelligence Services

Threat Analysis

- Watch Desk
- Brand Protection
- Dedicated Analysts

Response & Takedown Services

- Phishing Attacks
- Identity Theft
- Stolen Credentials
- Rogue Applications
- IP Theft
- Social Media Impersonation

Special Investigations Unit

- Executive Threat Assessments
- Sensitive Data Disclosure
- Physical Security

Machine Readable Threat Intelligence

CYVEILLANCE®

- Malicious C2
- Infection Records
- Malicious URL
- Phishing
- Newly Registered Domains
- PII (Personal Information Indicators)
- Malware Total Lifecycle Protection (TLP) Bundle

- Cyber Safety Awareness training

Threat Intelligence Management

SCOUTVISION®

Threat Intelligence Platform with 140+ data feeds

SCOUTINTERJECT™

Internal Network Telemetry Correlation

SCOUTPRIME™

Configurable Confidence Scoring

CTC PORTAL™

OSINT Customized Tasking & Collection

Threat Mitigation

NETSENTRY™

Hyper Accelerated Intrusion Detection

NETDEFENDER™

Security Orchestration & Threat Mitigation

DNSDEFENDER®

DNS Threat Aware Firewall & Caching

Network Appliances:

CS-4000, CS-4000E

“CTC” & “DNS” Legacy Naming

A Fragmented Threat Intelligence & Security Market



Threat Intelligence Services



Machine Readable Threat Intelligence



Threat Intelligence Management



Threat Mitigation



Format for Acquisition of LookingGlass Solutions



Threat Intelligence Services



- As an annual subscription per service
- Per takedown
- Amount of analyst hours
- Customized investigations

Machine Readable Threat Intelligence



- Per data feed as an annual subscription
- Included with ScoutVision and ScoutPrime – no additional fee

Threat Intelligence Management



- ScoutVision aaS - annual subscription
- ScoutVision or ScoutPrime - hosted
- ScoutVision - on prem with annual support
- Scout InterXect - on prem
- CTC Portal – mentions per month

Threat Mitigation



- DNS Defender - on prem with annual support
- Net Sentry – annual subscription
- Net Defender - annual subscription

Additional fees may apply as some solutions also incur per user, per takedown, etc. pricing.

Threat Intelligence Services/ MRTI

Brand Protection Services

Response Services

Global Security & Intelligence

Watch Desk Support

Special Intelligence Unit

Machine-Readable Data

Feed/API Details



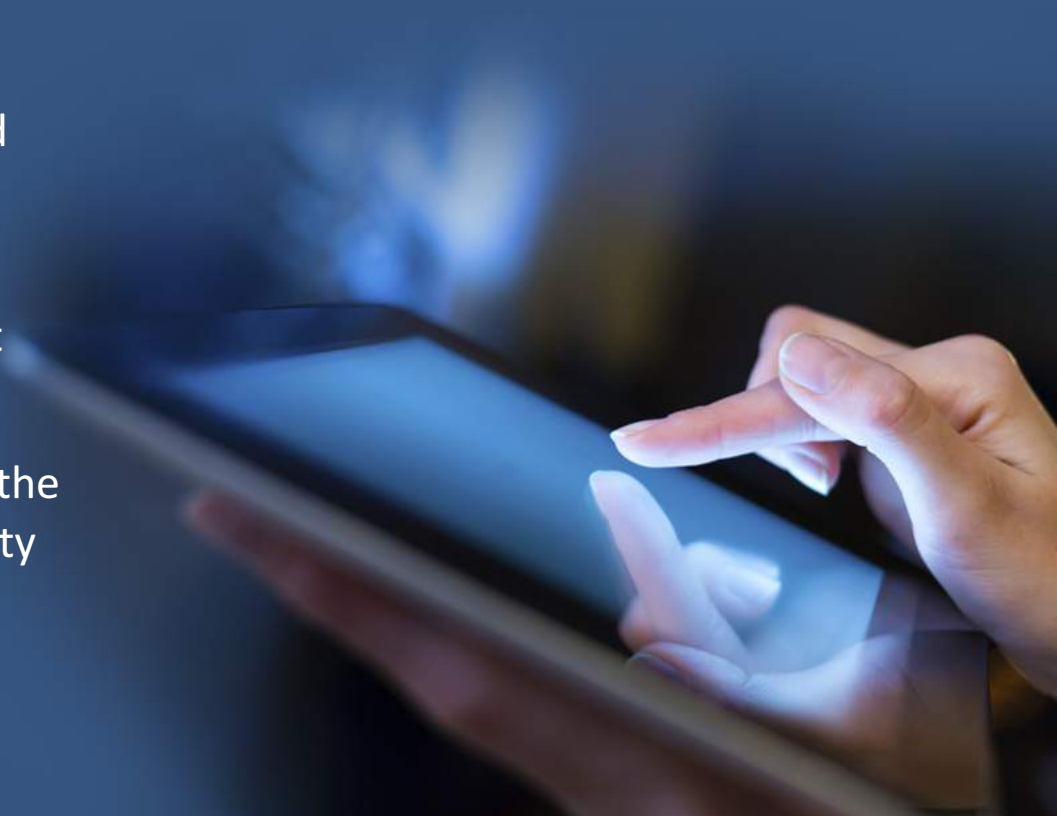
Threat Intelligence Services



Brand Protection Services

Challenge: Maintaining Brand Integrity

- The volume and variety of online brand abuse continues to expand
- From the web to social media to mobile apps, criminals are using brand names to steal data, divert customers, and reap illicit profits
- An active monitoring program is the best way to protect brand integrity and customer trust



Solution: Brand Protection



Brand Abuse Detection



- Brand Abuse Detection alerts you to uses of your brand and logos online
- Our systems and analysts isolate and identify infringements – freeing up your resources to review only relevant data
- Proactive monitoring is the best way to limit risk to customers and brand equity

5

rc

Exact-brand and variation matching including typos, look-alikes and bitsquatting

Go-Live warnings
when suspect domain
names become active

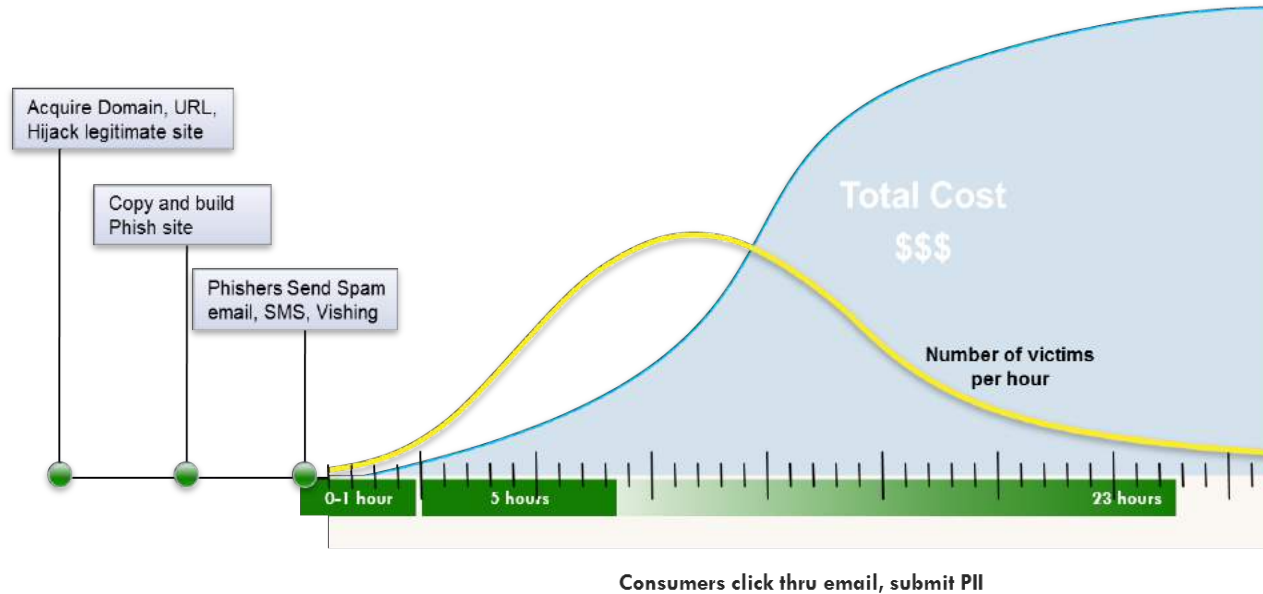
Immediate response/
recovery upon
registration if desired

Expired-domain name alerts to empower acquisition of desired domain names



Phishing Detection

Speed is critical to minimize impact: the longer a phishing site is up, the more consumers and your organization are at risk



Detection Diversity

Diverse sourcing is one key to rapid detection. Cyveillance monitors the broadest possible set of sources to maximize attack discovery. Inputs include:

- Millions of emails and email-based links per day
- Customer abuse-box feeds
- Client web logs
- Phone messages
- SMS messages
- Domain Registrations
- IRC/Chat Rooms in which “kits” are sold and traded



LookingGlass monitors the broadest possible set
of sources to maximize detection and speed



Honeypots,
spam email,
and links



Customer Abuse
Box
Feed/Monitoring



Client Web
Logs



Phone/SMS
messages



Domain Name
Registrations
and “Go Live”
Alerts



Patented Site-
Seal Early-
Detection
System



A blurred background image showing several people running on a track, overlaid with a dark blue gradient.

Response Services

Challenge: Prompt Global Content Removal



Malware



Imposters



Confidential
Files



Phishing



Phone

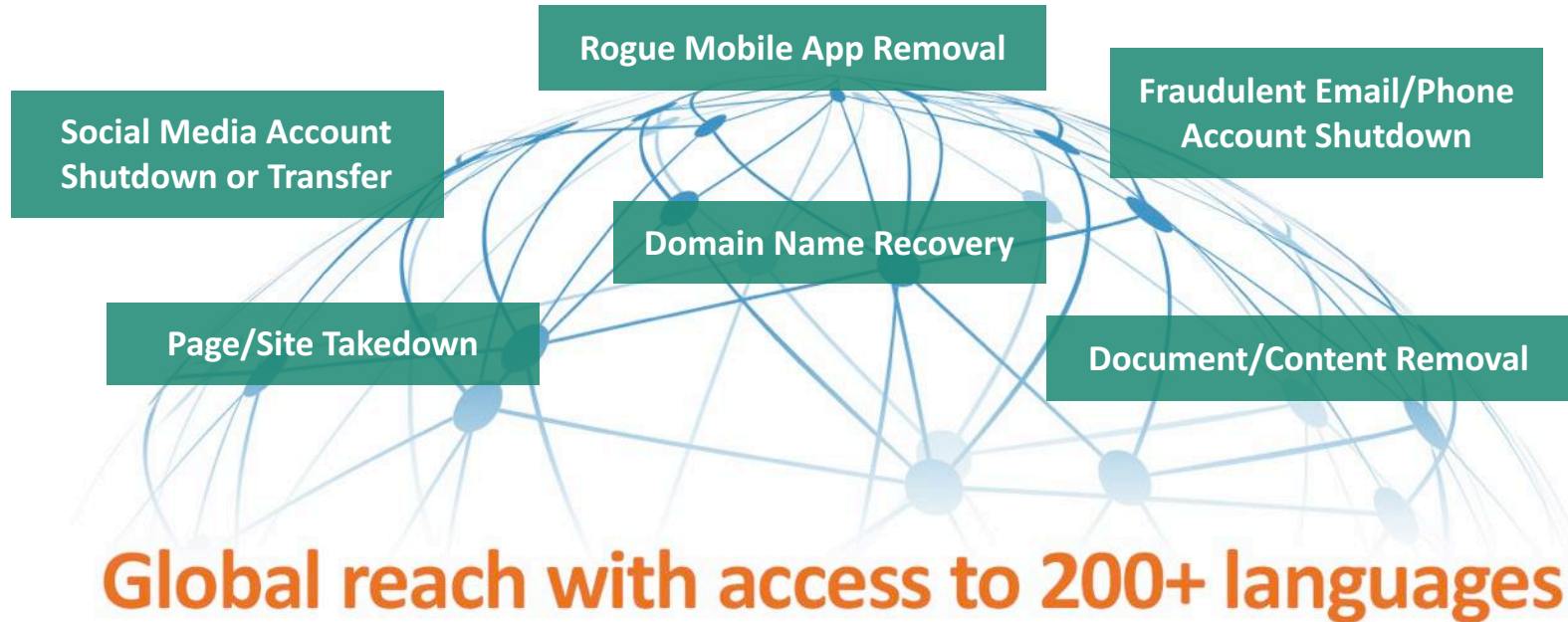


Email



Solution: Response Services

Fast, efficient, and affordable response services
to insure prompt removal



Phishing Response Services



- Anti-Phishing Detection Guarantee
- Anti-Phishing Accuracy Guarantee
- System Availability Guarantee
- Configuration Change Guarantee
- Response Service 100% Commitment Pledge
- Phishing Response Discount Commitment
- Takedown, Staydown™ Lifetime Guarantee



Global Security & Intelligence

Challenge: Shortage of In-House Expertise



- Cisco Annual Security Report estimates a million unfilled security jobs worldwide in 2014
- Data from Boston-based labor analytics firm Burning Glass says cyber security job postings grew 74% from 2007 to 2013, more than twice the growth rate of all IT jobs



Solution: Our Cyber Analysts

A diverse team of expert analysts with extensive experience and training to help with day-to-day threat intelligence needs

- Degrees in computer science, business, law and intelligence
- Average individual experience of 7+ years
- 30% of team hold Masters degrees or have advanced graduate work
- Fluency in 20+ languages



Cyber Analyst Capabilities

Physical Risks



- Protests, marches, and other disruptions
- Threats to employees or executives
- Risks to physical plant or infrastructure
- Weather and disaster events
- Civil/political unrest and conflict

Cyber Threat Activity



- Targeting by known hackers, threat actors, or other adversaries
- System or customer credentials
- Breaches of customer PII or company IP
- Leaks and disclosures of sensitive internal documents

Brand & Reputation Issues



- Online abuse of brands and trademarks
- Negative commentary and PR risks
- Commentary on executive behavior, performance, or ethics
- Internal or external accusations of wrongdoing

Legal and Compliance Concerns



- Class-action and divestiture campaigns
- Unauthorized statements by employees
- Exposure of statutorily- or export-controlled data
- Regulatory violations by agents, employees or contractors



Flexible Engagement Options

Multiple options to engage our 80+ intelligence analysts, either on-site or at our Washington, D.C. headquarters



Long-term Analyst

Typically as half- or full-time employees



Short-term & "Surge"

Typically around a specific event or in special need



Scheduled

For infrequent but regular (e.g. weekly or monthly) requirements



A person wearing glasses and a dark sweater is sitting at a desk, leaning forward and writing on a document. The background shows a modern office with large windows and other people working. The entire image has a blue tint.

Watch Desk Support

Challenge: Above & Beyond Support

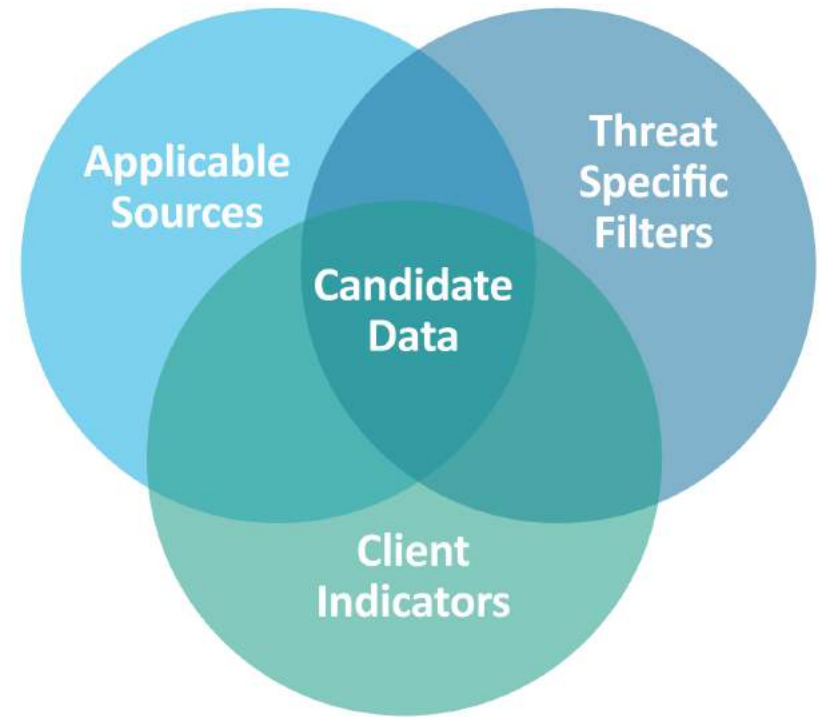


- Risks, threats, and bad actors don't follow a 9 to 5 schedule
- Staffing to review, vet, and alert on online risks 24x7 is complex and costly
- Some risks lead to a massive surge in detected incidents, requiring the ability to quickly scale up operations.
- Reporting and escalation can vary by risk and audience, requiring detailed SOPs to ensure proper notification

Solution: 24/7 Intelligence Monitoring

Around-the-clock vetted alerting on a variety of risks

- Relevant, human-vetted alerting to ensure timely, relevant delivery of critical items, including during sudden increases in volume
- Experienced Analysts can monitor for Physical, Cyber, and Executive threats
- Customized reporting and escalation processes with phone, SMS, and email delivery options
- Stand-alone alerting service or integrated with other LookingGlass solutions



A person wearing a dark cap and a dark shirt is shown from the back, holding a walkie-talkie to their mouth. The background is a bright, hazy outdoor scene. The entire image is overlaid with a dark blue semi-transparent filter.

Special Investigation Unit

Challenge: In-depth Investigations

- Special or ad-hoc reports and investigations for large or private events, executive hires, etc.
- Investigations for mergers and acquisitions, due diligence, vendor evaluations, etc., particularly in situations that require discretion



Investigations and Custom Projects

The Special Investigation Unit (SIU) comprises our senior-most analysts, who handle a wide array of security issues, including physical and digital threats

- Decades of experience conducting web-based investigations for the Intelligence Community and the Fortune 500
- Expertise in cyber intelligence, intelligence studies, security, terrorism, law, and behavioral sciences
- SIU analysts become an extension of your team that you can call on as needed



Organization for Security and
Co-operation in Europe

Online Risk Assessments

In addition to ad-hoc projects and custom investigations, the SIU also offers online risk assessments for enterprises, executives, and key suppliers

- Executive Threat Assessments examine the online environment for potential physical and information security risks to executives and their family members
- Vendor and Company Assessments offer snapshot assessment of online exposure in key areas, including:
 - Cyber and hacker activities
 - Sensitive data disclosures
 - Physical security issues
 - Regulatory compliance
 - Brand abuse and infringements
 - Reputation risks



Machine-Readable Threat Intel: Feeds & APIs

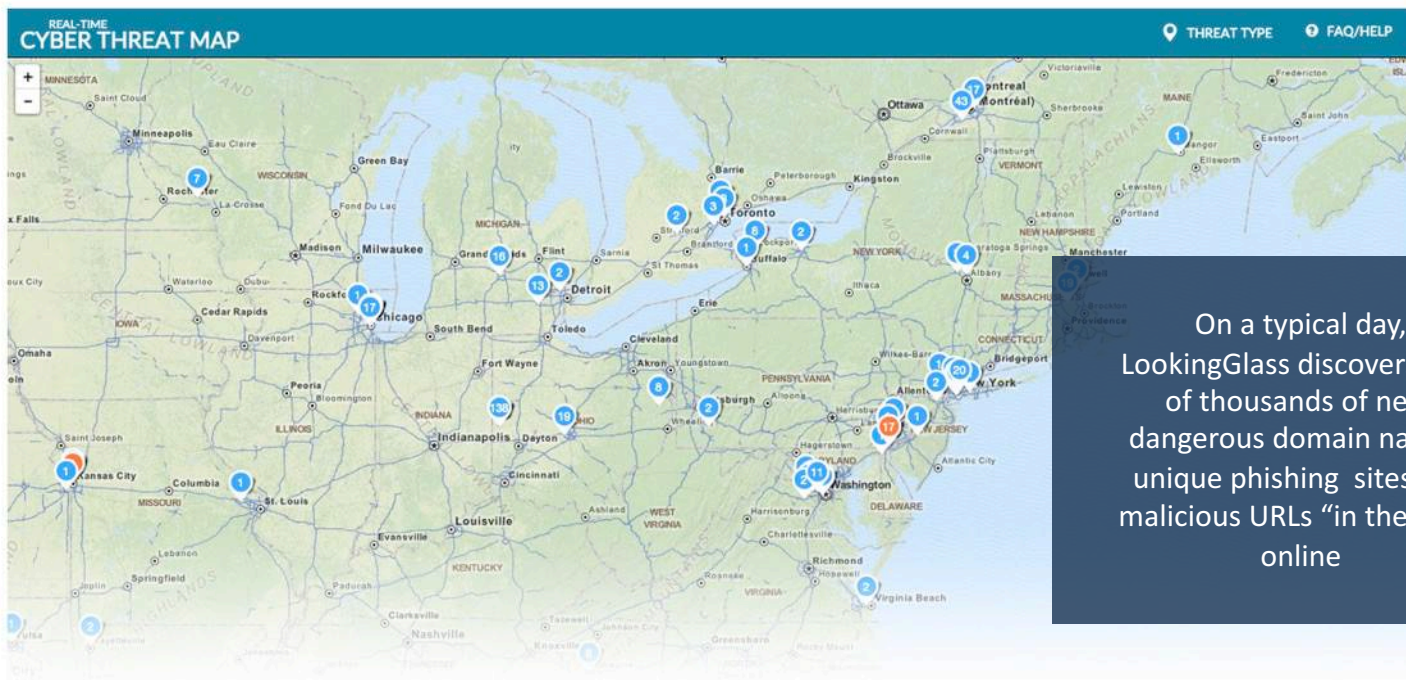
Challenge: Real-time Protection for the Network



All “intelligence” is not created equal. Many data feeds include outdated or generic information that is not useful and can actually be harmful to your security processes. LookingGlass provides valuable, timely, and actionable intelligence.

Solution: Real-time Data on What's Happening *Now*

LookingGlass currently has five machine-readable data services related to malicious online activity available in General Release



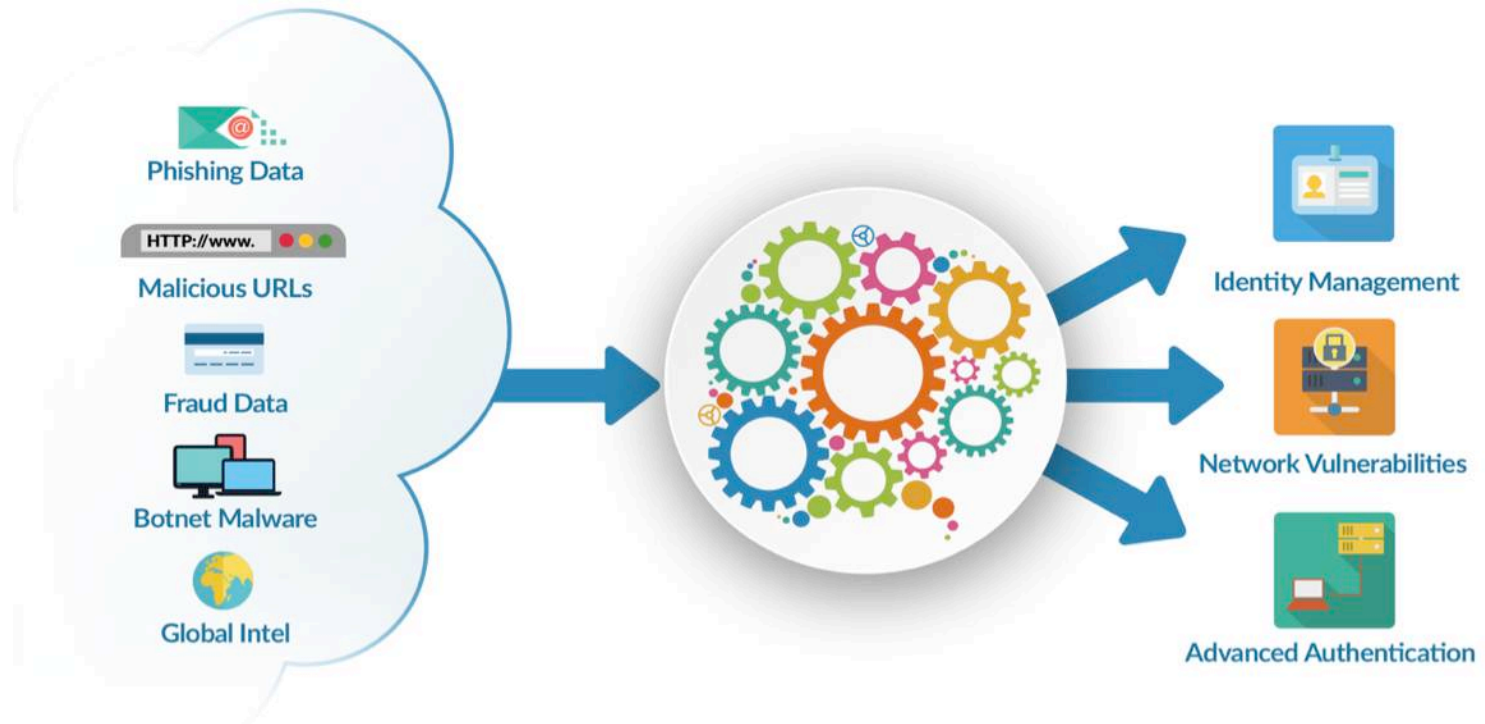
Data Services – In Production



- Real-Time Phishing Attack Data: Thousands of phishing attacks per day across industries and geographies
- Malicious URLs: In-the-wild malware discovered as, and where, it is being hosted and distributed
- New Domain Names: EVERY new domain name registered the preceding day in .COM, .NET, .ORG, and 200+ other gTLDs
- High-Risk Domain Names: A subset of the new gTLD feed, this isolates new domain names exhibiting highly suspect characteristics
- PII Lookup Service: Thousands of SSNs and CCNs found each day in underground channels, checked via secure, encrypted lookup

Data Services – In Production

Our machine-readable data are easily integrated into SIEMs, firewalls, and other security devices and analytical tools



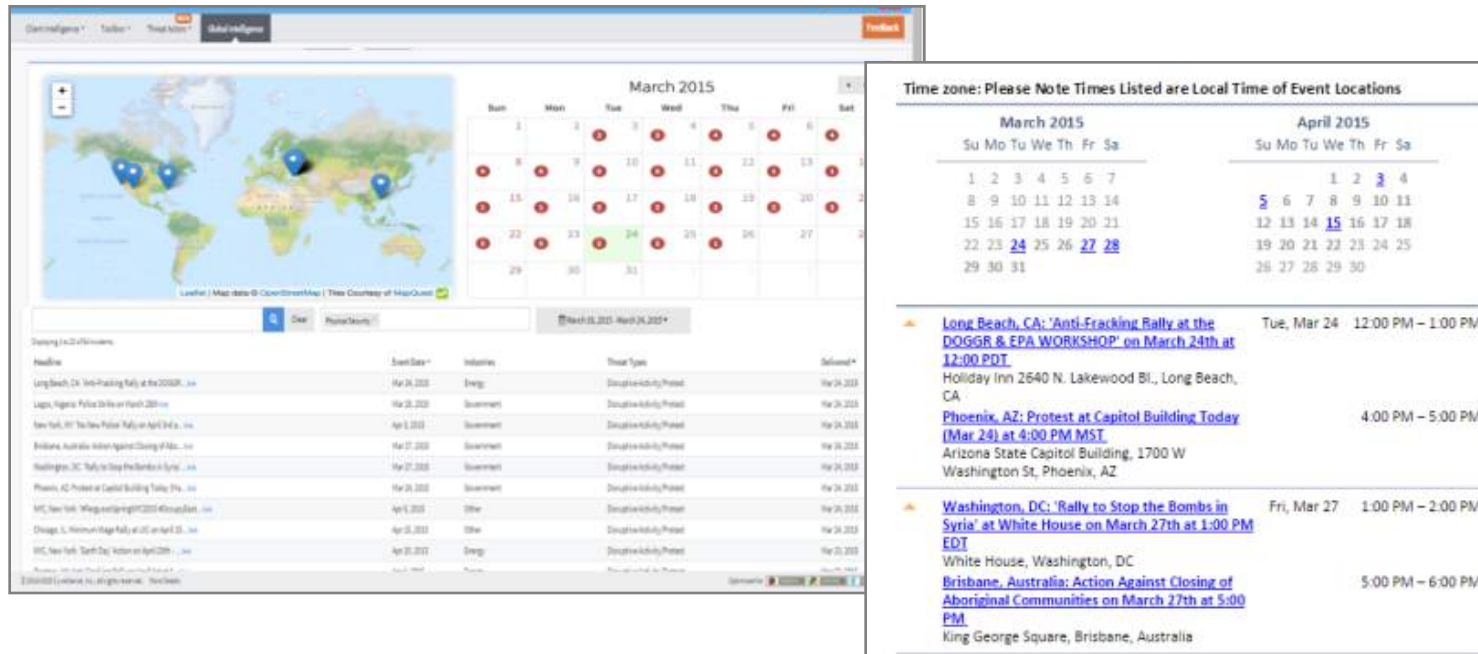
Data Services – In Beta

The Cyber Threat Center collection platform is now in beta for streaming open-source data directly into a client application or big-data index



Data Services – In Beta

Global Intelligence reports, including all text, map and calendar data, are also available via API



The screenshot displays the LookingGlass Global Intelligence interface. On the left, a world map shows event locations with blue pins. In the center, a calendar for March 2015 highlights specific dates. On the right, a detailed view of events is shown, including dates, times, and locations.

Time zone: Please Note Times Listed are Local Time of Event Locations

March 2015							April 2015						
Su	Mo	Tu	We	Th	Fr	Sa	Su	Mo	Tu	We	Th	Fr	Sa
1	2	3	4	5	6	7				1	2	3	4
8	9	10	11	12	13	14	5	6	7	8	9	10	11
15	16	17	18	19	20	21	12	13	14	15	16	17	18
22	23	24	25	26	27	28	19	20	21	22	23	24	25
29	30	31					26	27	28	29	30		

Long Beach, CA: 'Anti-Fracking Rally at the DOGGR & EPA WORKSHOP' on March 24th at 12:00 PDT
Tue, Mar 24 12:00 PM – 1:00 PM
Holiday Inn 2640 N. Lakewood Bl., Long Beach, CA

Phoenix, AZ: Protest at Capitol Building Today (Mar 24) at 4:00 PM MST
4:00 PM – 5:00 PM
Arizona State Capitol Building, 1700 W Washington St, Phoenix, AZ

Washington, DC: 'Rally to Stop the Bombs in Syria' at White House on March 27th at 1:00 PM EDT
Fri, Mar 27 1:00 PM – 2:00 PM
White House, Washington, DC

Brisbane, Australia: Action Against Closing of Aboriginal Communities on March 27th at 5:00 PM
5:00 PM – 6:00 PM
King George Square, Brisbane, Australia



A hand is pointing at a laptop screen, which is partially visible in the background. The entire image is covered with a semi-transparent blue overlay. The text 'Feed/API Technical Details' is centered in white, with a thin blue horizontal line underneath the word 'API'.

Feed/API Technical Details

Feed Details – Malicious URL Data

Format: XML

Delivery: HTTPS Web Service or API

Typical Volume: 500-3000 unique URLs/day

Update Frequency: ~ Every 10 minutes

Documentation: Schema, samples, implementation instructions etc. available with password at Feeds.LookingGlass.com

Live Trial: Available on request for 14 days

What it looks like:

```
<inspected_url>
- <URL reference_url="http://www.famujacksonville.com/forum/viewtopic.php?
t=108552&postdays=0&postorder=asc&start=0&sid=cd6cc33b4a0dcbbf1045c52a07163d0f">
  <IP>67.212.80.125</IP>
  <Domain_Name>famujacksonville.com</Domain_Name>
  <Host_Name>www.famujacksonville.com</Host_Name>
  <Exploit_Type />
  <Exploit_Description />
- <Binary>
  <Binary_Path Link="http://www.worldweb.com/load.php?id=225" />
  <Pest_Name>New threat delivered by exploit</Pest_Name>
  <File_Size>12098</File_Size>
  <File_Name>load.exe</File_Name>
- <Hash>
  <MD5>13d48523b832c7e2a947fa7361072a63</MD5>
  <MD5_8k>68857345db04283fca48cf4b9f6bba52</MD5_8k>
  <SHA1_160>7578ed4c0d23e32fe37493d13c2c7ddb4e7b91d6</SHA1_160>
  <SHA1_160_8k>a101ebbef003678b3f6e15087ba8f8d2e2dc155b</SHA1_160_8k>
  <CRC>8f344d3d</CRC>
</Hash>
```



Feed Details – Phishing URL Data

Format: XML or CSV

Delivery: HTTPS Web Service (API coming soon)

Typical Volume: 2K-5K Unique Phish URLs/day

Update Frequency: ~ Every 10 minutes

Documentation: Schema, samples, implementation instructions etc. available with password at Feeds.LookingGlass.com

Live Trial: Available on request for 14 days

What it looks like:

```
<feed>
  <delivery_ts>2009-04-20T00:00:01-04:00</delivery_ts>
  <version>1.386802</version>
  <description>Cyveillance Phishing Feed</description>
  <total_entries>972</total_entries>
- <entries>
- <entry>
  <url>http://www.smi1523.hosting4you.net/www.paypal.com/paypal.com/online-secure/us/cgi-bin/webcmd=login-run/webcmd=login-run&dispatch=ad7a161bac07c418b197e8c07b8cd648ad7a161bac07c418b197e8c07b8cd648</url>
  <indicator>+</indicator>
  <discovery_ts>2009-04-19T00:10:54-04:00</discovery_ts>
  <domain>hosting4you.net</domain>
  <host>www.smi1523.hosting4you.net</host>
  <title>Login - PayPal</title>
  <ip>208.89.214.205</ip>
- <feed_specific_properties>
  <target>PayPal</target>
</feed_specific_properties>
</entry>
- <entry>
```



Feed Details – New Domain Names

Format: TXT

Delivery: sFTP

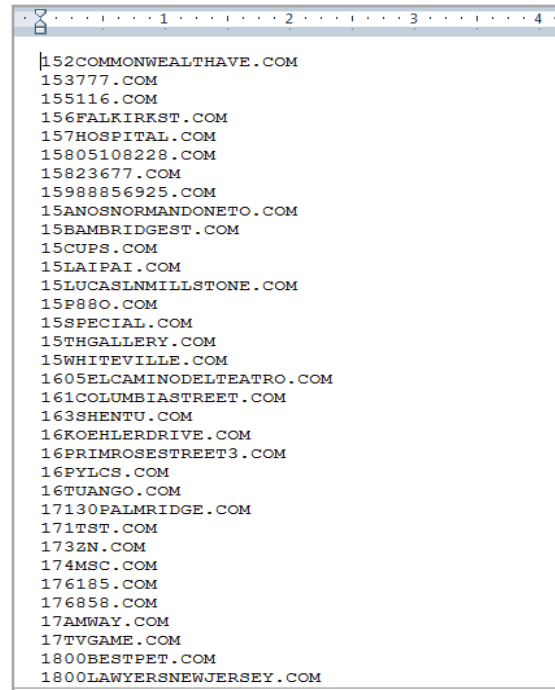
Typical Volume: 50-200K+ domains/day

Update Frequency: 1x daily

Documentation: Samples, implementation instructions etc. available with password at Feeds.LookingGlass.com

Live Trial: Available on request for 14 days

What it looks like:

A screenshot of a text editor window showing a list of domain names. The window has a title bar with a close button and a tab labeled '1'. The text inside the window is a list of domain names, each on a new line, starting with '152COMMONWEALTHAVE.COM' and ending with '1800LAWYERSNEWJERSEY.COM'.

```
152COMMONWEALTHAVE.COM
153777.COM
155116.COM
156FALKIRKST.COM
157HOSPITAL.COM
15805108228.COM
15823677.COM
15988856925.COM
15ANOSNORMANDONETO.COM
15BAMBRIDGEST.COM
15CUPS.COM
15LAIPAI.COM
15LUCASLNMILLSTONE.COM
15P880.COM
15SPECIAL.COM
15THGALLERY.COM
15WHITEVILLE.COM
1605ELCAMINODELTEATRO.COM
161COLUMBIASTREET.COM
163SHENTU.COM
16KOEHLERDRIVE.COM
16PRIMROSESTREET3.COM
16PYLCS.COM
16TUANGO.COM
17130PALMBRIDGE.COM
171TST.COM
173ZN.COM
174MSC.COM
176185.COM
176858.COM
17AMWAY.COM
17TVGAME.COM
1800BESTPET.COM
1800LAWYERSNEWJERSEY.COM
```

Feed Details – New High Risk Domain Names

Format: TXT

Delivery: sFTP


Typical Volume: 1-3K domains/day

Update Frequency: 1x daily

Documentation: Samples, implementation instructions etc. available with password at Feeds.LookingGlass.com

Live Trial: Available on request for 14 days

What it looks like:



```
007HJDCXZ.COM
008530000.COM
008530001.COM
008530002.COM
008530003.COM
008530004.COM
008530005.COM
008530006.COM
008530007.COM
008530008.COM
008530009.COM
008530010.COM
008530011.COM
008530012.COM
008530013.COM
008530014.COM
008530015.COM
008530016.COM
008530017.COM
008530018.COM
008530019.COM
008530020.COM
008530021.COM
008530022.COM
008530023.COM
008530024.COM
008530025.COM
008530026.COM
008530027.COM
008530028.COM
008530029.COM
008530030.COM
008530031.COM
008530032.COM
```



A person wearing a dark cap and a dark shirt is shown from the back, holding a walkie-talkie to their mouth. The background is a bright, hazy outdoor scene. The entire image is overlaid with a dark blue semi-transparent filter.

Threat Intelligence Platforms

A person wearing a white lab coat is holding a tablet. The tablet screen shows a dashboard with various charts, including a pie chart and a bar chart, and some text. The background is a dark blue gradient.

Cyber Threat Center

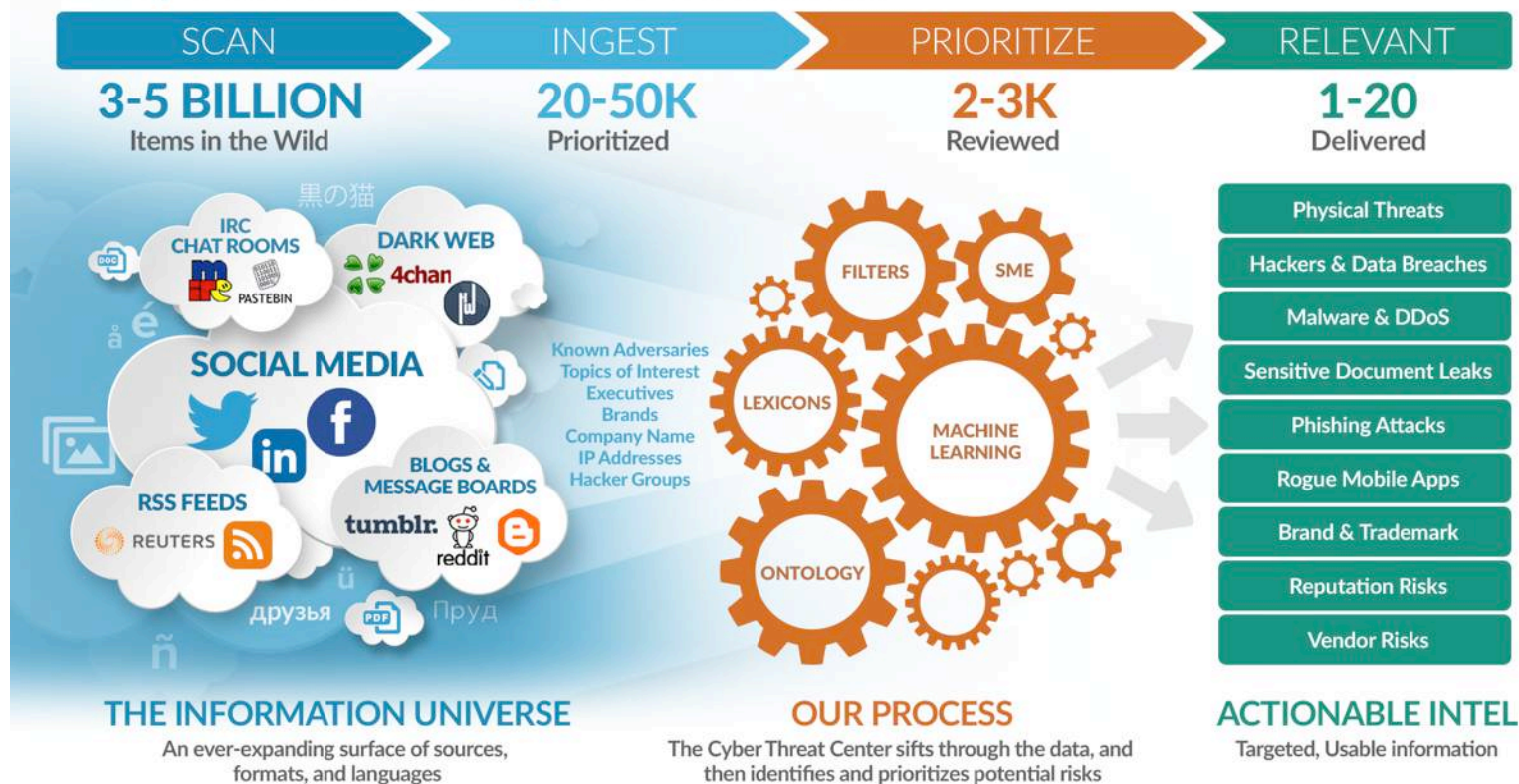
Challenge: Too Much Data, Too Little Time



- Security and threat analysts spend far too much time sifting through data, and too little time analyzing it
- Analysts need ability to quickly isolate online risks and threats from a vast array of online sources and in any language
- Real-time threat intelligence enables faster detection and mitigation of potential issues

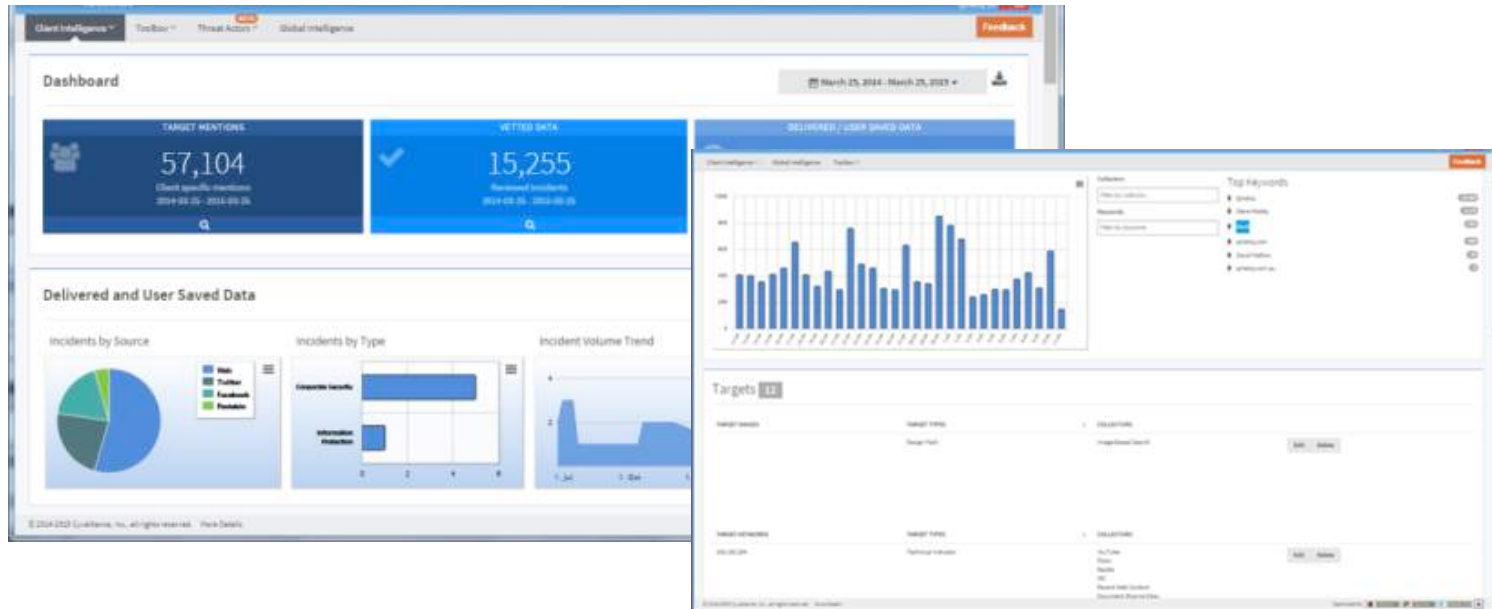
Solution: Efficient Collection and Prioritization

Daily Process for a Typical Customer



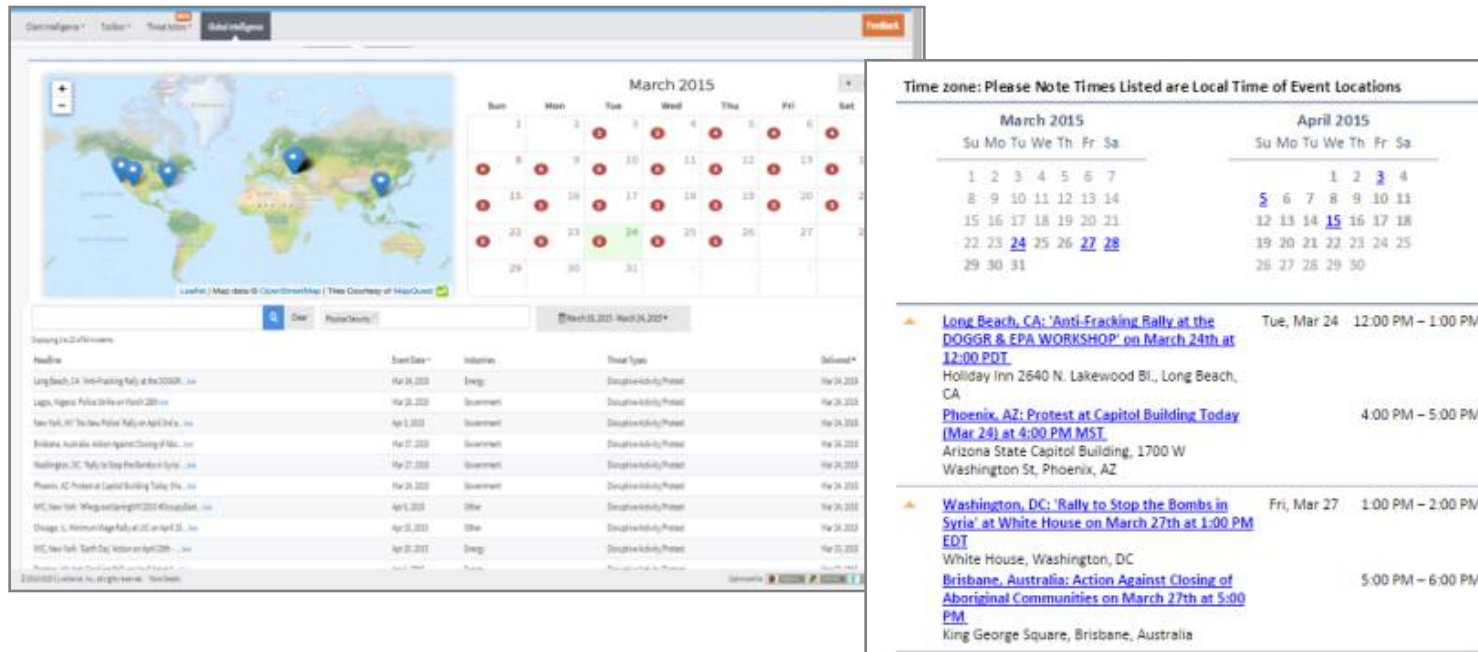
Flexible Configuration, Search, Alerts

Online monitoring allows custom collection on terms, indicators, and even images from a wide range of sources



Global Intelligence on Upcoming Threats

Every day, 80+ LookingGlass analysts post updates about global cyber risks, breaches, and physical disruptions



The screenshot displays the LookingGlass Global Intelligence dashboard. It features a world map on the left with blue location pins. In the center is a calendar for March 2015, with dates 24, 25, 26, 27, and 28 highlighted in green. On the right, a detailed event list is shown, including:

- Long Beach, CA: 'Anti-Fracking Rally at the DOGGR & EPA WORKSHOP' on March 24th at 12:00 PDT.** (Tue, Mar 24 - 12:00 PM - 1:00 PM)
- Phoenix, AZ: Protest at Capitol Building Today (Mar 24) at 4:00 PM MST.** (4:00 PM - 5:00 PM)
- Washington, DC: 'Rally to Stop the Bombs in Syria' at White House on March 27th at 1:00 PM EDT.** (Fri, Mar 27 - 1:00 PM - 2:00 PM)
- Brisbane, Australia: Action Against Closing of Aboriginal Communities on March 27th at 5:00 PM.** (5:00 PM - 6:00 PM)

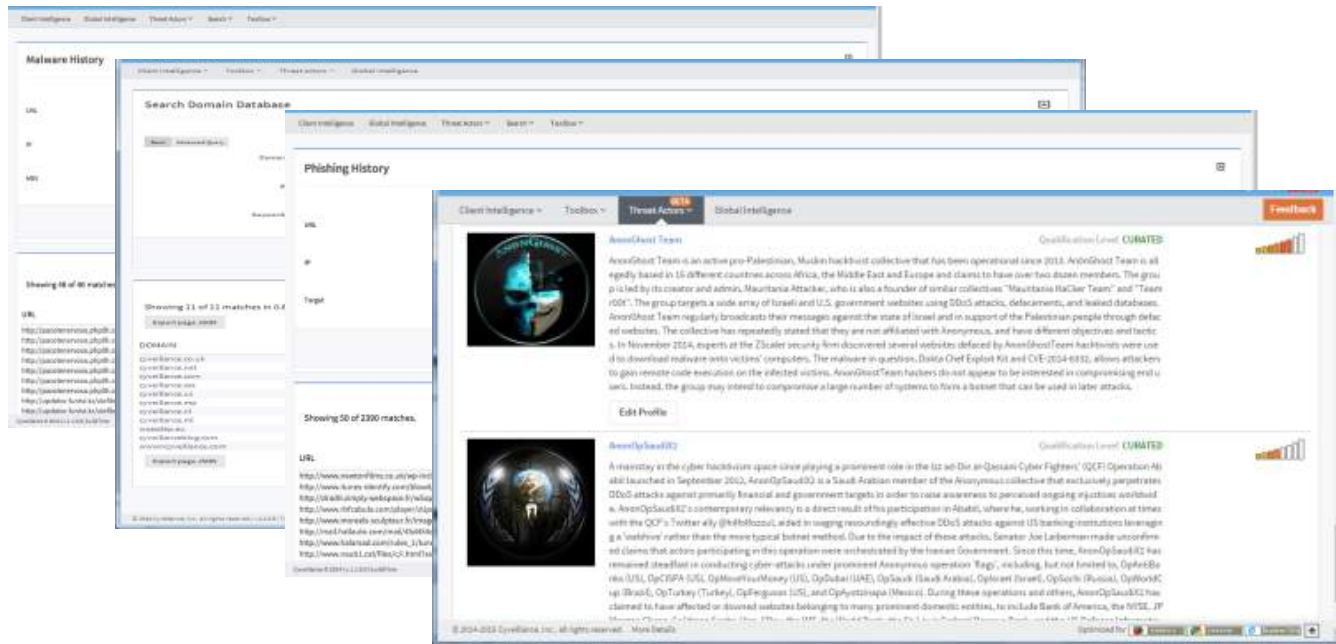
Below the map, a table lists various events with columns for Event Date, Location, Industry, Threat Type, and Severity.

Event Date	Location	Industry	Threat Type	Severity
Mar 24, 2015	Long Beach, CA	Energy	Disruptive Activity/Protest	High
Mar 24, 2015	Lagos, Nigeria	Police	Disruptive Activity/Protest	High
Mar 24, 2015	New York, NY	The New Police	Disruptive Activity/Protest	High
Mar 27, 2015	Brisbane, Australia	Aboriginal	Disruptive Activity/Protest	High
Mar 27, 2015	Washington, DC	Rally to Stop the Bombs in Syria	Disruptive Activity/Protest	High
Mar 24, 2015	Phoenix, AZ	Protest at Capitol Building Today	Disruptive Activity/Protest	High
Apr 5, 2015	NYC, New York	Wingman	Disruptive Activity/Protest	High
Apr 5, 2015	Chicago, IL	Wingman	Disruptive Activity/Protest	High
Apr 22, 2015	NYC, New York	Earth Day	Disruptive Activity/Protest	High



Investigative Tools

Analyst Toolbox provides access to years' worth of unique data about IPs, domain names, malicious URLs, phishing attacks, and threat actors



Flexible Delivery



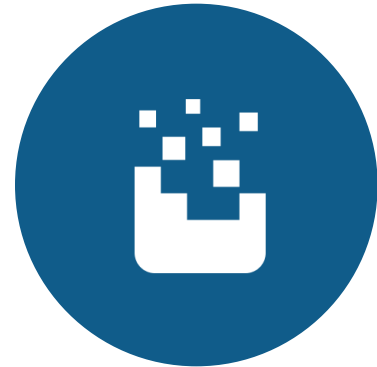
Portal



API




Alerts



Data Feeds

Platform Summary

	Typical Social Media Monitoring Tools	 LOOKINGGLASS	Typical Brand Monitoring Services
Social Media			
Facebook	✓	✓	—
Twitter	✓	✓	—
GooglePlus	✓	✓	✗
Youtube	✓	✓	✗
Instagram	✓	✓	✗
Flickr	✓	✓	✗
Reddit	✓	✓	✗
Web Sources			
In-House Crawlers	✗	✓	✓
Search Engine Results	✗	✓	✓
Message Boards	—	✓	✗
Paste Sites (e.g. Pastebin etc.)	✗	✓	✗
Document Sharing Sites (Docstoc & 30 others)	✗	✓	✗
Code sharing sites (e.g. Github)	✗	✓	✗
Forums	—	✓	✗
Blogs	—	✓	✗
Wikipedia	✗	✓	✗
Non-Web Sources			
Domain Name Registrations	✗	✓	✓
Image-Based Search	✗	✓	—
Hacker IRC Channels	✗	✓	✗
RSS Feeds	✗	✓	✗
Additional Features			
Global WHOIS Information	✗	✓	✓
IP/ISP/Geolocation Lookup	✗	✓	—
Global Threat Map and Event Calendar	✗	✓	✗
Global Phishing Data	✗	✓	✗
Malicious URL, signature and payload data	✗	✓	✗
Domain/IP database for 180 MM+ domains	✗	✓	✗
Threat Actor Profiles	✗	✓	✗
Web portal PLUS feed, alert and API options	—	✓	—

A person wearing a dark cap and a dark jacket is shown from the back, holding a walkie-talkie to their mouth. The background is a bright, hazy outdoor scene. The entire image is overlaid with a dark blue semi-transparent filter.

ScoutVision

Enterprise Cyber Risk Management

Addressing the Spectrum



THREAT
RESEARCH

SCOUTVISION™

SCOUTVISION™
HOSTED

VIRUSTRACKER™
 **LOOKINGGLASS**



3rd PARTY RISK
MONITORING

SCOUTVISION™

SCOUTVISION™
HOSTED



NETWORK
SECURITY

DNS DEFENDER®

**CYBER SECURITY
ORCHESTRATOR**

**CONTENT
INSPECTION
GATEWAY**



INCIDENT
RESPONSE

SCOUTINTERXECT™

SCOUTVISION™
SCOUTVISION™
HOSTED



SECURITY
OPERATIONS

SCOUTINTERXECT™

SCOUTVISION™
SCOUTVISION™
HOSTED

VIRUSTRACKER™
 **LOOKINGGLASS**

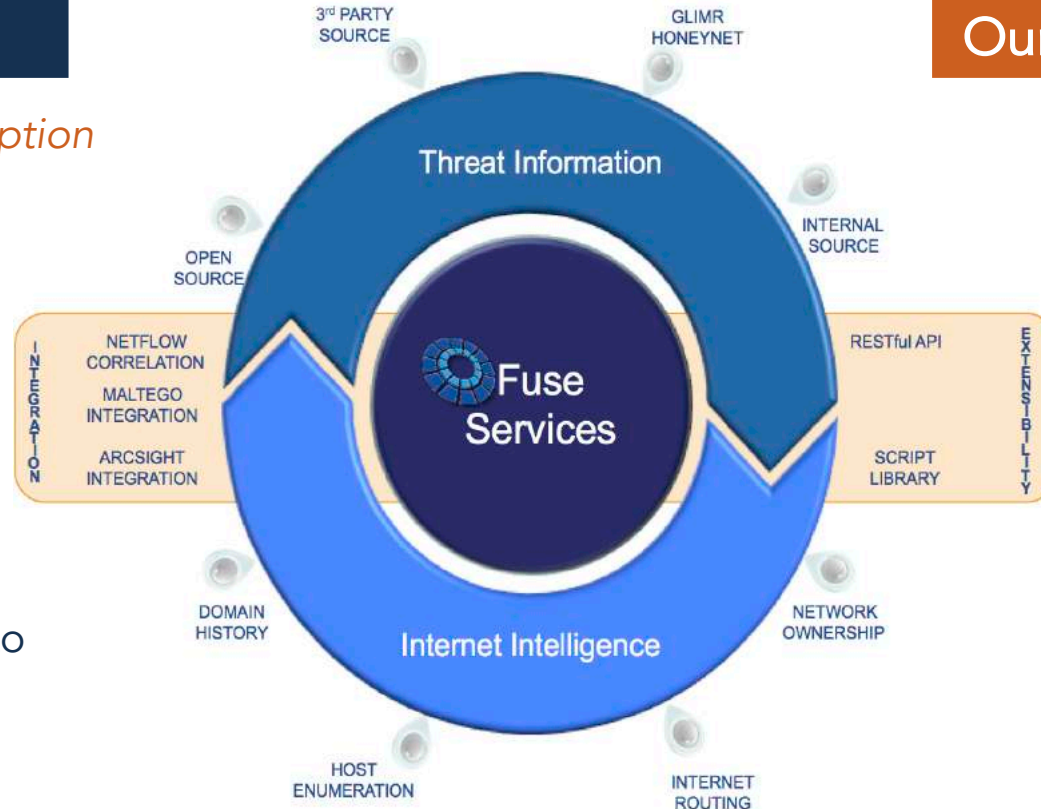
SCOUTVISION

Introducing ScoutVision – A Threat Intelligence Platform

What We Do

Simplify the consumption of global threat and internet intelligence

Deliver efficiencies and effectiveness into threat, security, and risk operations



Our Advantage

Flexibility

Scalability

Global Visibility

Internal Integration

Ecosystem Integration

Our machine-readable TI is easily integrated into SIEMs, other security devices and analytical tools – one example Splunk

The image displays three screenshots illustrating the integration of LookingGlass with Splunk.

Top Left: LookingGlass Setup for Splunk

This screenshot shows the 'LookingGlass Setup for Splunk' interface. It includes fields for 'Lookingglass Username' (entered as 'admin'), 'Lookingglass Password', and 'Confirm password'. Below these is a field for 'LookingGlass Domain' with the value '10.16.16.55'. A 'Cancel' button is at the bottom.

Top Right: LookingGlass System_Tag Lookup

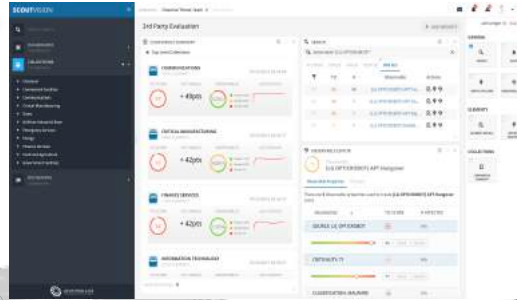
This screenshot shows the 'LookingGlass System_Tag Lookup' interface. It displays a table of results for the IP address '2.2.2.2,3.3.3.3,4.4.4.4,5.5.5.5,6.6.6.6,8.8.8.8,20.20.20'. The table includes columns for 'ipaddress', 'City', 'Country', 'Region', 'lat', 'lon', and 'system_tags'. The results show data for France, United States, Germany, and United States.

Bottom: LookingGlass Threat Report

This screenshot shows the 'LookingGlass Threat Report' interface. It features two pie charts: 'LookingGlass Threat Report' and 'LookingGlass Threat Report - Detailed'. Below the charts is a 'Threats by Geolocation' map showing a world map with colored dots representing threats. A table of threat data is also displayed, including columns for 'Latitude', 'Longitude', 'Country', 'City', 'Region', 'lat', 'lon', and 'system_tags'.

Global Threat Intelligence Correlation

SCOUTVISION



 ScoutVision™

- Global Internet Topology
- Malware & Threat Analysis
- Configurable Threat Indicator Confidence*
- “Web Scale” Scale Out Architecture*
- Streaming Threat Analysis*



Ecosystem Integration

Our machine-readable TI is easily integrated into SIEMs, other security devices and analytical tools – one example Splunk

The image displays three screenshots illustrating the integration of LookingGlass with Splunk.

Top Left: LookingGlass Setup for Splunk

This screenshot shows the 'LookingGlass Setup for Splunk' interface. It includes fields for 'Lookingglass Username' (set to 'admin'), 'Lookingglass Password', and 'Confirm password'. There is also a field for 'LookingGlass Domain' with the value '10.16.16.55' and a 'Cancel' button.

Top Right: LookingGlass System_Tag Lookup

This screenshot shows the 'LookingGlass System_Tag Lookup' interface. It displays a table of results for the IP address '2.2.2.3.3.3.4.4.4.5.5.5.6.6.6.8.8.8.20.20.20'. The table includes columns for 'ipaddress', 'City', 'Country', 'Region', 'lat', 'lon', and 'system_tags'.

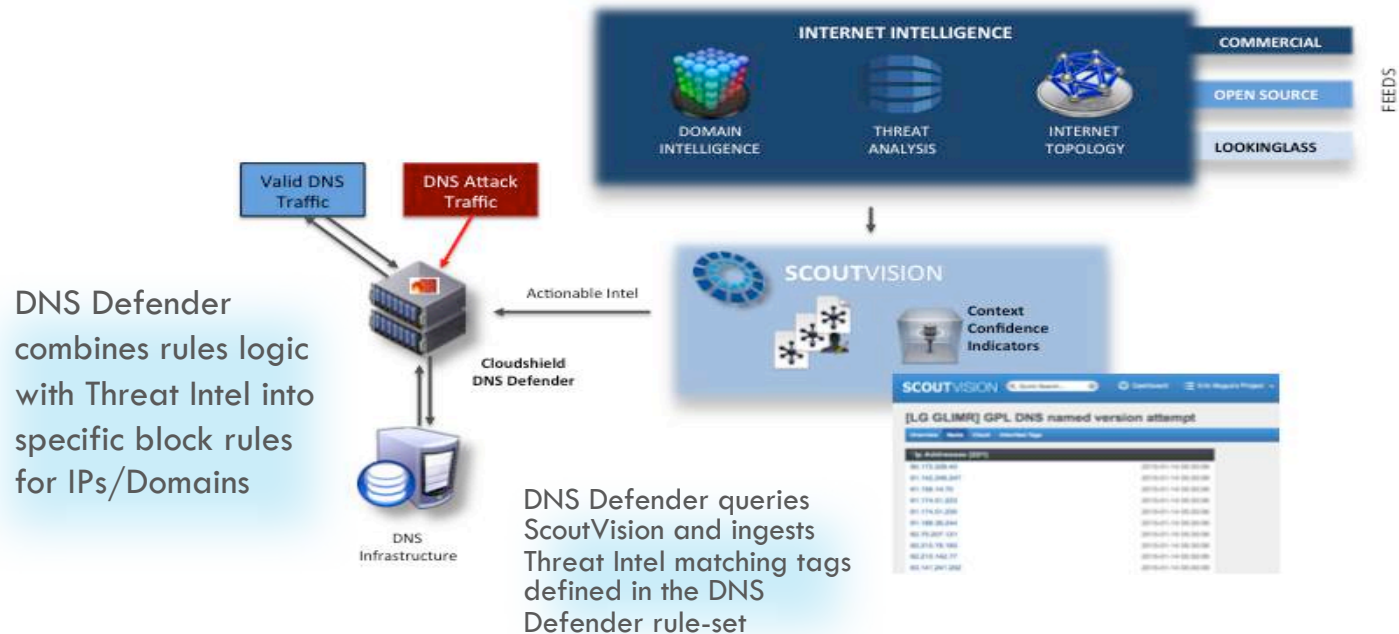
Bottom: LookingGlass Threat Report

This screenshot shows the 'LookingGlass Threat Report' interface. It displays two pie charts representing threat data. The left chart is titled 'Threats by Geolocation' and shows a distribution of threats by country. The right chart is titled 'Threats by System Tag' and shows a distribution of threats by system tag. Below the charts is a map of the world with markers indicating threat locations.

Dynamic Threat Defense - DTD

Customer requires DNS infrastructure protection from cyber attacks

- Deploys DNS Defender in front of their DNS servers and ScoutVision
- Creates Threat Intelligence-based rules in DNS Defender to strengthen protection



- Lookingglass continuously monitors global internet
- Automatically adding context and Threat Intel
- Hosted in Core Intelligence Processor (CIP)
- Distributed to customer's SV instance

A person wearing a dark cap and a dark jacket is shown from the back, holding a walkie-talkie to their mouth. The background is a bright, hazy outdoor scene. The entire image is overlaid with a dark blue semi-transparent filter.

ScoutPrime

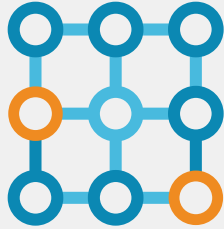
What We Deliver: Unified Threat Protection



LookingGlass provides a suite of products and services that deliver **UNIFIED THREAT PROTECTION** designed for your defense

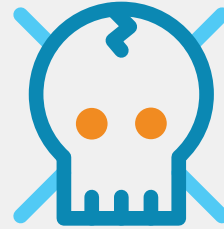


LookingGlass – Unified Threat Protection



UNIFIED

- All Source Intelligence
- Structured IoC's
- OSINT / Social Media
- LG Proprietary MRTI
- 3rd Party Threat Data
- Deep & Dark Web
- Shared Data



THREAT

- Threat Actors
- Malware & Vulnerabilities
- Compromised Credentials
- Phishing Sites / Malicious URLs
- DDoS Attacks
- Brand & Reputation
- Physical



PROTECTION

- Response & Takedown Services
- Network Detection
- Mitigation Appliances
- Email & Syslog Alerts
- Protocol Specific Protection
- Executive & Enterprise Assessments

LookingGlass Product Portfolio



Threat Intelligence Services

Threat Analysis

- Watch Desk
- Brand Protection
- Dedicated Analysts

Response & Takedown Services

- Phishing Attacks
- Identity Theft
- Stolen Credentials
- Rogue Applications
- IP Theft
- Social Media Impersonation

Special Investigations Unit

- Executive Threat Assessments
- Sensitive Data Disclosure
- Physical Security

Machine Readable Threat Intelligence

CYVEILLANCE®

- Malicious C2
- Infection Records
- Malicious URL
- Phishing
- Newly Registered Domains
- PII (Personal Information Indicators)
- Malware Total Lifecycle Protection (TLP) Bundle

- Cyber Safety Awareness training

Threat Intelligence Management

SCOUTVISION®

Threat Intelligence Platform with 140+ data feeds

SCOUTINTERJECT™

Internal Network Telemetry Correlation

SCOUTPRIME™

Configurable Confidence Scoring

CTC PORTAL™

OSINT Customized Tasking & Collection

Threat Mitigation

NETSENTRY™

Hyper Accelerated Intrusion Detection

NETDEFENDER™

Security Orchestration & Threat Mitigation

DNSDEFENDER®

DNS Threat Aware Firewall & Caching

Network Appliances:

CS-4000, CS-4000E

“CTC” & “DNS” Legacy Naming



“.....if threat intelligence indicators were really able to help an enterprise defense strategy, one would need to have access to *all of the feeds* from *all of the providers* to be able to get the “best” possible coverage.” – Verizon DBIR 2015

Threat Intel Sources: 24-Hour Data Context



350,000
FQDN

345,000,000
Flows

61,000,000 IP

1.035B
Websites

2.1 B
Social Media
Users

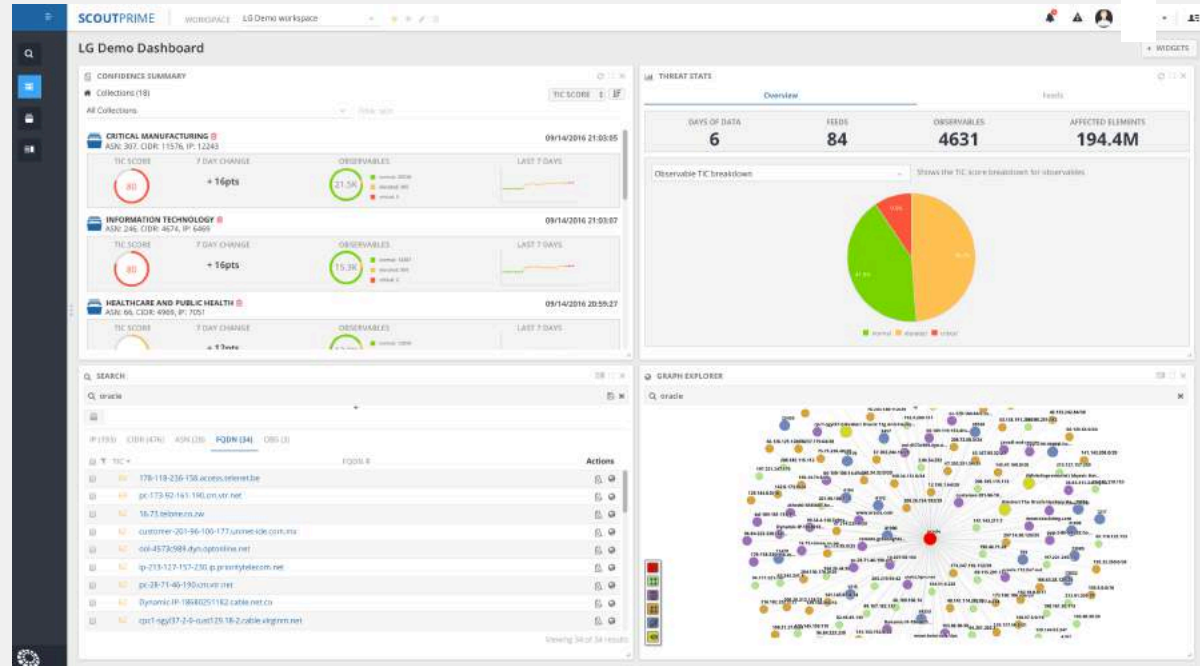
240
Countries

14,000,000
CIDR

131,000 ASN

ScoutPrime – Next Generation Threat Intelligence Platform

- **100+ Unique Threat Data Feeds**
- **Secure, Cloud Based, Single Tenant Deployment**
- **API access, ArcSight (CEF) integration**
- **Flexible per user pricing that scales as your organization grows**



User Configurable Scoring (Threat Indicator Confidence)



- Default & user configurable scoring of all threats currently being tracked.
- Value Add: Provides customers the ability to match threat scores to their organization security posture creating relevant threat intelligence.

OBSERVABLE EDITOR

Observable
APT Black Vine

Observable Properties TIC Score

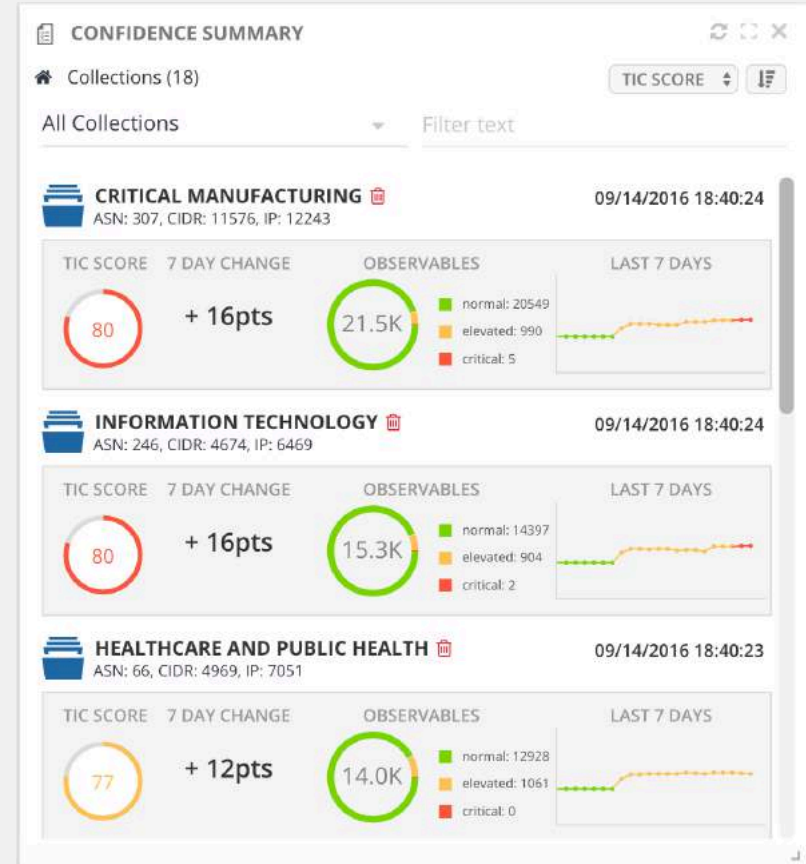
There are **4** Observable properties used to create **APT Black Vine** score.

PROPERTIES	TIC SCORE	AFFECTED OBSERVAB...
- SOURCE: CYVEILLANCE INFECT...	90	37845
- CRITICALITY: 80	80	1
- CLASSIFICATION: APT	90	8623

Customizable Organization and Sector Risk Scores



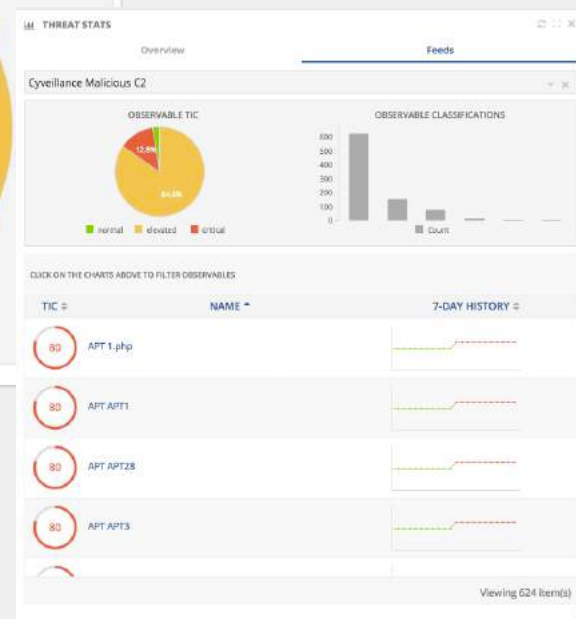
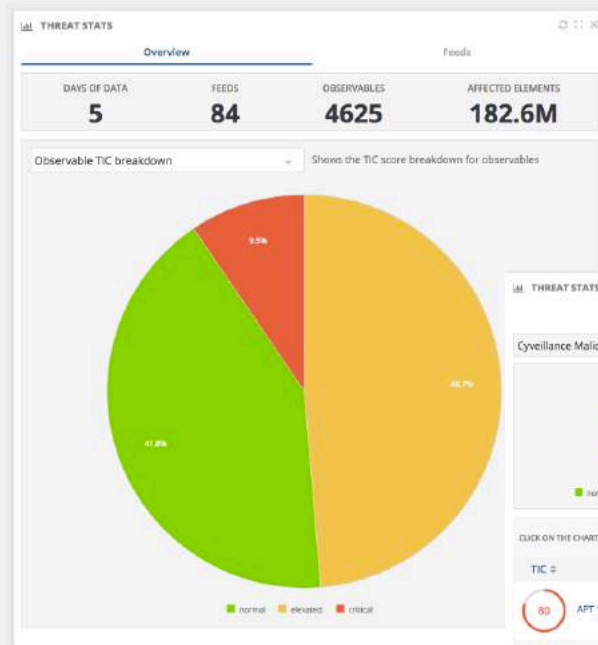
- Create & visualize current threat data metrics for your organization, your supply chain, or your industry.
- Value Add: Eliminates noise and provides customers immediate actionable intelligence relevant to only the things they deem critical.



Threat Stats Widget



- Visualize current threat data metrics for ALL data in the platform. Provides overview and individual data feed statistics.
- Value Add: Provides customers an insight into the quantity and sources of threat data in the system and what networks they are targeting.



Malware Hash Support



- Search for a hash with IPs and FQDNs returned with meta data
- Value Add: Search for and identify the hashes associated with an IP address or FQDN in the element details widget.

ELEMENT DETAILS ID: -TJ9[HSM=OF>FP/AC@<IWN, ~V

52.206.247.168 - 1 pts since yesterday

Active (2) Ownership Historical (9) DNS History (58) Location (0)

Observed Malware Distribution

Timestamp	Source
09/07/2016 17:50:24	VirusTotal

TIC	Classifications
67	Malware Artifacts, IP Watchlist, Domain Watchlist, Malware, Watchlist

e_sha256_H	e_hash_H
8086c9012d43a20793af09cb1b5980f21ea7b2d68184c868fcd151640c491131	ab3d69cd0317d6f02991be50d92258e2, 8086c9012d43a20793af09cb1b5980f21ea7b2d68184c868fcd151640c491131, a433b67f5a97af095eb2650271d68907dc372142

File
20160908040311_VirusTotalCollector.json

Malicious URL Detected

Timestamp	Source
09/08/2016 04:03:12	VirusTotal

- [illegible]

Our Clients



Get Started on Your Defense



- 1 | Schedule a Demo
<https://lgscout.com/request-a-demo>
- 2 | Meet with a LookingGlass Rep
- 3 | Craft a Customized Threat Defense Solution



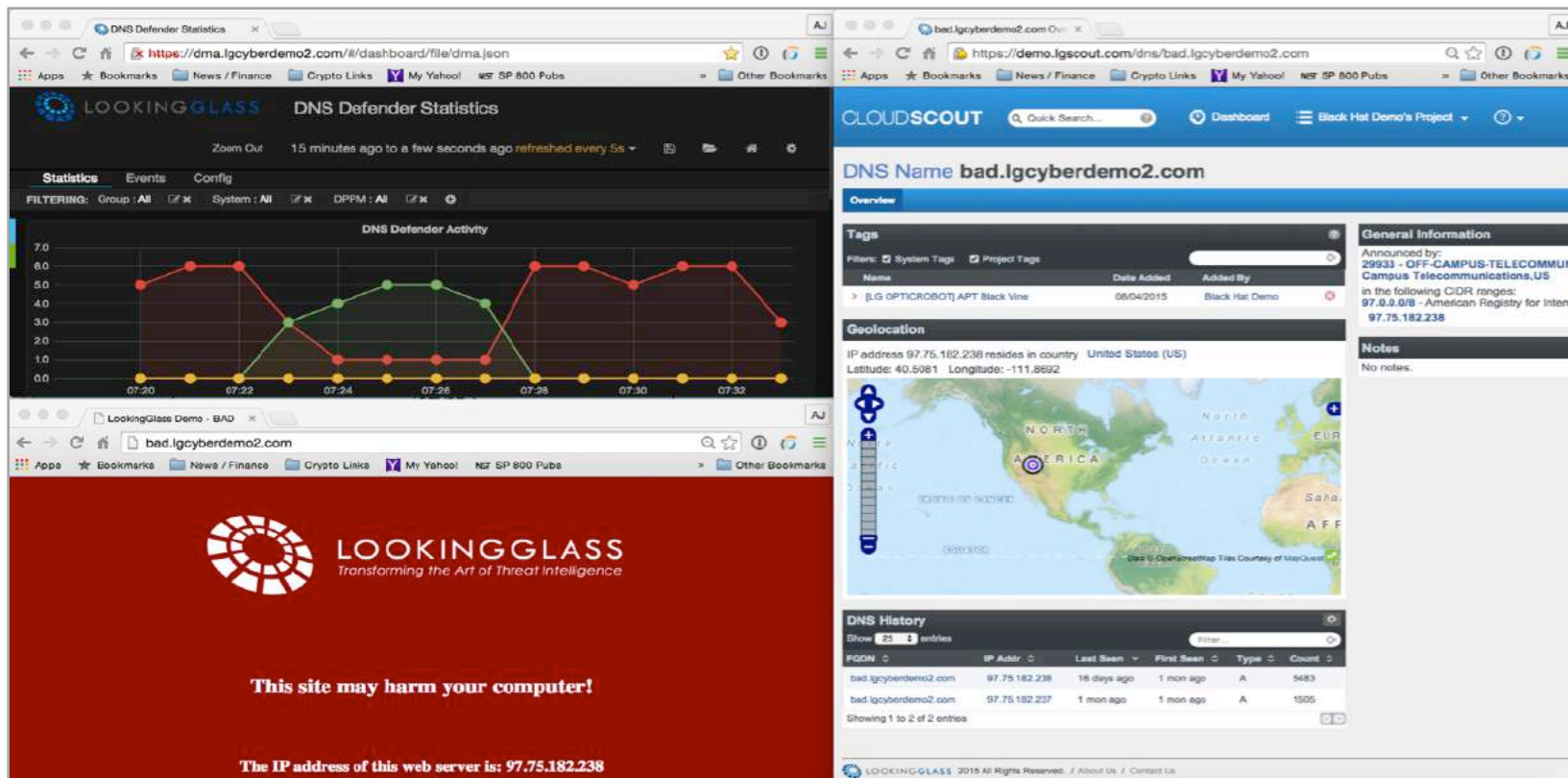
Threat Mitigation



Dynamic Threat Defense

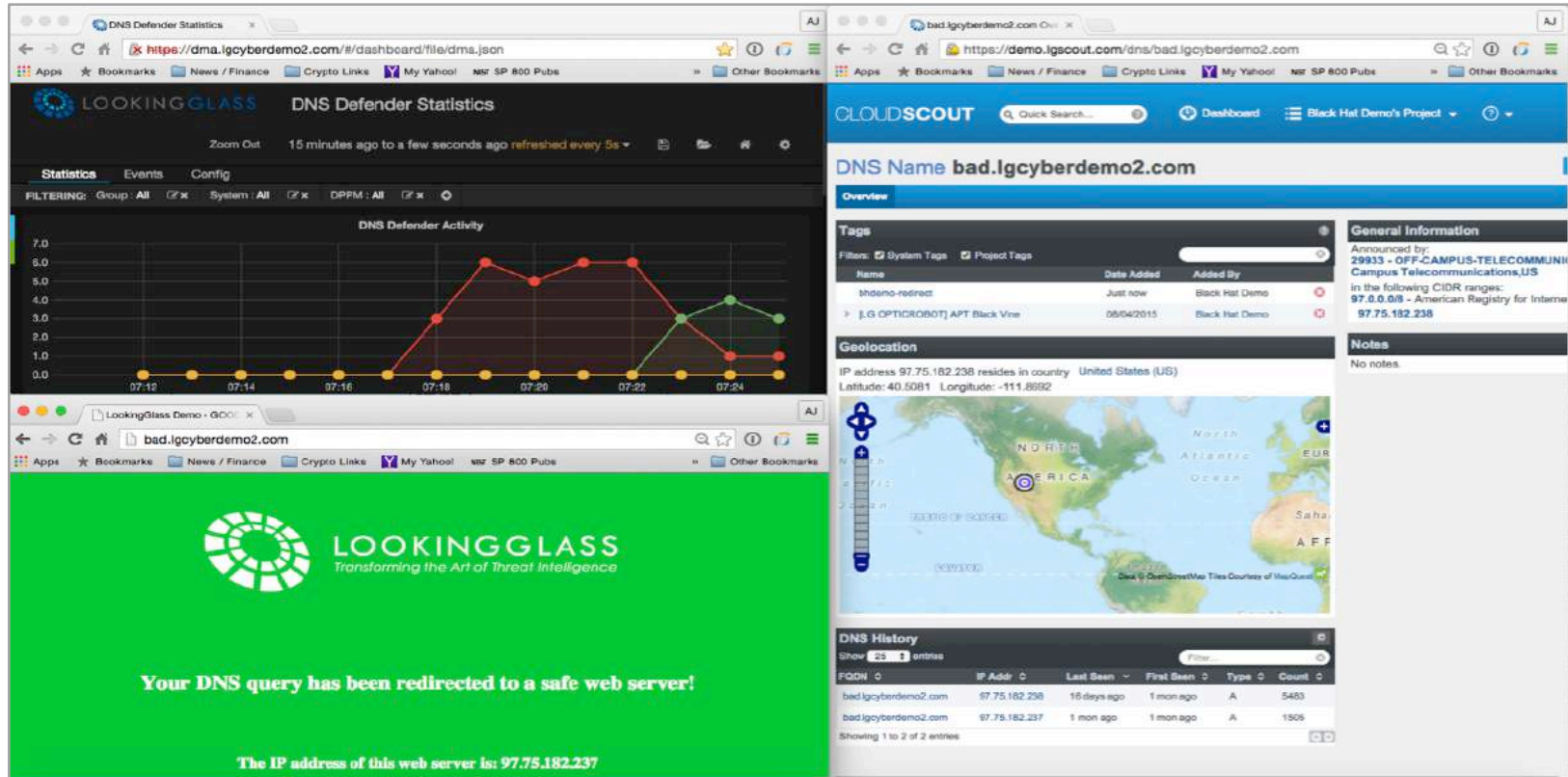
Dynamic Threat Defense Actionable

Mitigation automation w/ DNSD + ScoutVision Threat Intelligence



Dynamic Threat Defense Redirect Mitigation

Mitigation DNSD plus ScoutVision Threat Intelligence Domain Redirect

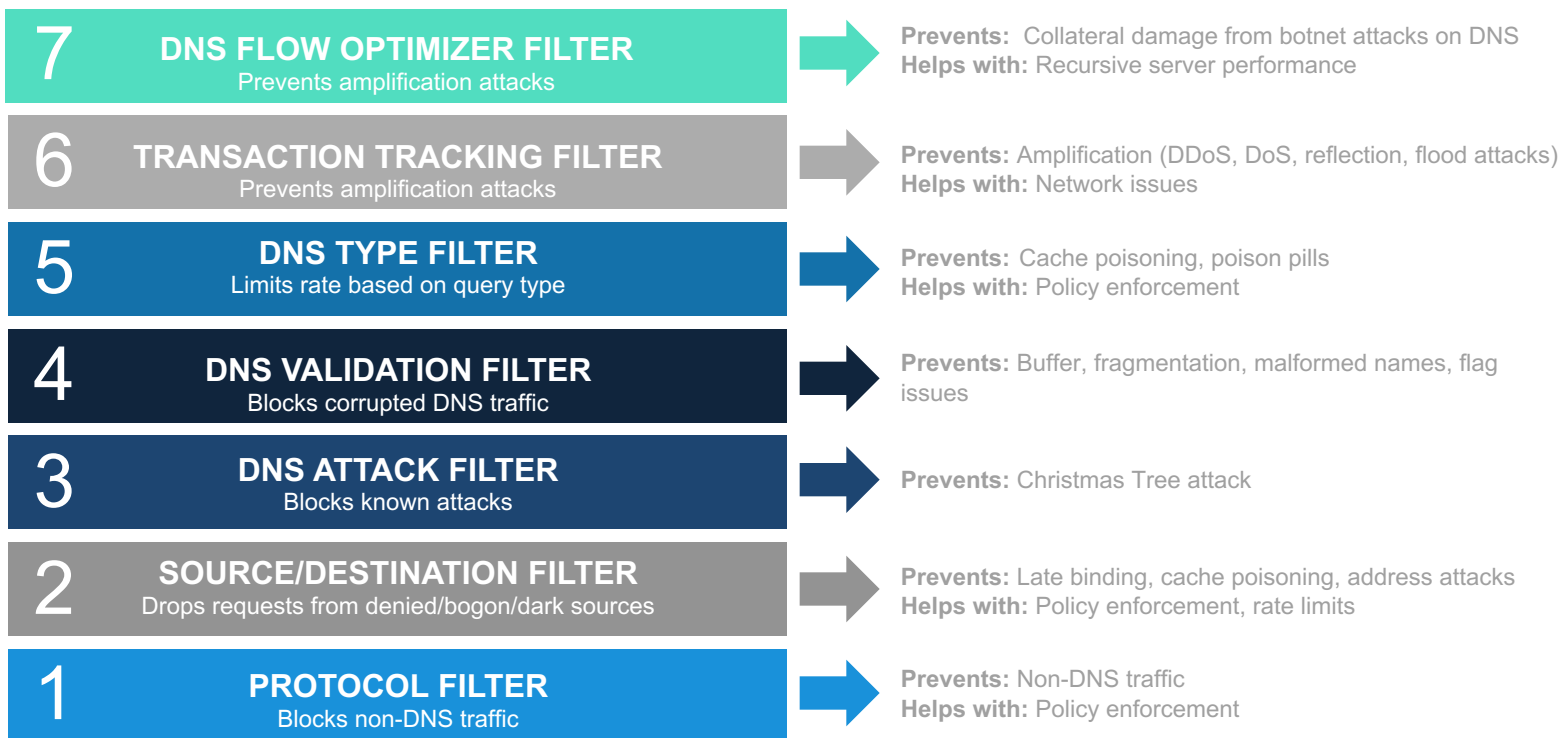




DNS Defender

DNS Defender is 7 Layer Security

Each layer is uniquely specialized in to protect against all kinds of DNS attacks



Deep Packet Processing

Going beyond Deep Packet Inspection

Deep Packet Inspection

- Can prioritize traffic/flows
- Provide traffic information

Use information to manually

- Adjust router configuration
- Adjust firewall rules
- Tune IPS

VS

Deep Packet Processing

- Can prioritize traffic/flows
- Provide traffic information

Information + intelligence

- Fully programmable
- Rapid traffic management solutions
- Open to partners and customers
- Extensible for any solution

Information > action > resolution:
HOURS TO DAYS

Information > action > resolution:
MILLISECONDS



DNS Defender Platforms

DNS Defender is the **original** application firewall designed to protect against DNS-specific attacks. It is the **only** solution with DPP technology and an open architecture, and is perhaps your only security solution that actually enhances performance.

CS-2000

Content Processing Platform



CS-4000

The Trusted Network Security Platform



A dark blue, semi-transparent overlay covers the entire image. In the background, a person's hand is visible, pointing their index finger towards the screen of a laptop. The laptop screen and keyboard are partially visible but blurred. The text 'Example Solutions' is centered in a white, sans-serif font. A thin, light blue horizontal line is positioned directly beneath the text.

Example Solutions

Example Solution: Healthcare InfoSec Group

Challenges

- Management is awakened to risks after the Anthem breach, but team/budget are small
- Want alerts about risks to company data and networks, as well as industry monitoring
- Need proactive way to look for potential leaks or theft of sensitive data
- Concerned about look-alike domain names like the one used in the Anthem spear-phish
- Need cost-effective means to monitor online for both company and industry issues

Solutions

- Cyber Threat Center subscription
- Global Intel via Cyber Threat Center and/or API (Included in subscription) to track health industry cyber activity
- Watch Desk to “pre-digest” volume and alert on genuine issues within modest budget
- Domain Name Alerts and Response Services to watch for and shut down “look alike” domain names
- Machine-readable feeds for perimeter defense

Example Solution: Large Energy Firm CSO

Challenges

- Far-flung staff in remote, often hostile locations all over the world
- Operations affected by a wide range of potential risks from terrorism to weather
- Adversarial groups range from Boko Haram to Greenpeace
- The Corporate Security Staff is primarily US based and English-speaking

Solutions

- Cyber Threat Center subscription
- Global Intel via Cyber Threat Center and/or API (Included in subscription)
- 40 hours of SIU time to investigate known threat groups and support ad hoc projects
- Two half-FTE analysts on long-term support contracts to provide daily support and reporting in English, Russian and Arabic

Example Solution: Large Global Commercial Bank

Challenges

- Divided operations run out of London and Hong Kong, thousands of branches worldwide
- A controversial CEO who is often targeted by activist groups
- Recent acquisitions add to an already-wide brand portfolio
- Constantly subjected to all manner of physical, cyber, and reputational threats
- Numerous divisions, each with differing concerns and priorities

Solutions

- Cyber Threat Center subscription
- Global Intel via Cyber Threat Center and/or API (Included in subscription)
- 200 hours of SIU time to investigate known threat groups and support ad hoc projects
- Watch Desk support for 24x7 alerting
- Brand, Phishing, and Mobile App detection
- Two dedicated analysts for English and Mandarin coverage
- Annual Open-Source Threat Assessments of all C-Suite executives to understand risk exposure

Example Solution: Small Regional Bank

Challenges

- Primary method of phishing discovery is customer reporting, but staff work only 9-5
- In-house IT team is averaging 2-3 day response times for phishing takedowns
- An employee recently discovered a rogue mobile app, even though the bank doesn't have an "official" app at all

Solutions

- Phishing Detection service including customer abuse mailbox and web log monitoring
- Rogue Mobile App Discovery
- Response services for 200 items
- Completely offloads phishing and mobile app monitoring duties to LookingGlass, freeing up small in house team



Cyber Safety Awareness Training

Cyber Safety Awareness Training

Our award winning computer-based training program for Cyber Safety Awareness has saved our clients millions of dollars in IT, data loss and legal costs.

- Winner of the Marcomm Industry Platinum Award for “Best Computer Based Training Program”
- Available in three ~15 minute courses, or mini-modules for “just in time” education
- Available in both cloud-hosted and LMS (SCORM-compliant) delivery models



Cyber Safety Awareness Training

Help reduce risks that technology and the firewall don't stop: spear phishing and advanced cyber attacks that lead to network breaches and theft of data.

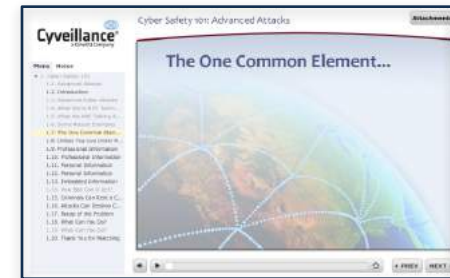
Module 1 – Data loss through People: Phishing, Leaks and Outright Theft



Module 2 – Data Loss through Machines: Viruses, Malware and Rogue Apps



Module 3 – Advanced Attacks: The Olympics of Hacking and Cyber Crime





Q&A



LOOKINGGLASS

www.LookingGlass.com



twitter.com/LGScout



linkedin.com/company/LookingGlass