DATA SHEET

SITUATIONAL THREAT INTELLIGENCE DETECTION

Managed Security Services

Si CYBER

AT A GLANCE

Harvesting the dark web for targeted attacks and breaches related to your organisation, in real time.

We harvest the public and dark web to extract situational intelligence relating specifically to our customers' assets & users, industry verticals and geographical regions. The objectives are to identify targeted threats, breached material and potentially avoid attacks altogether. Our threat advisors look for signs that sensitive client data, credentials or intellectual property have been exposed on the Internet.

The customer specific threat intelligence is gathered by examining over 720,000 sources including TOR Sites, Forums, social sites, paste sites and IRC traffic, cloud-based file sharing sites and other points of compromise across a multi-lingual, global environment spanning the visible, dark and deep web.

HOW IT WORKS

We utilise a range of commercial (Recorded Future) and open source tools to provide the widest possible harvesting of intelligence from over 720,000 sources including dark web activity. We monitor these sources against our customers' assets, users, email domains, URL's and intellectual property to detect breaches, organised attack campaigns and Indicators of Compromise (IOC's) against our customers.

1. HARVEST THE WEB

- 720,000+ sources
- 6 years of history
- Every language
- 11 billion data points
- 400+ Tor site
- 200+ IRC channels
- 645+ forums
- 25+ paste sites
- 20+ theat feeds

2. EXTRACT AND ORGANISE

Patented algorithms help you timeline and connect:

- IOCs
- Actors
- Events
- Malware
- Products
- Companies
- Technologies
- + 140 more

3. MAKE IT RELEVANT

- Global / Industry / Company trends
- Investigate emerging attackers, methodologies, tools and tactics
- Corroborate other sources
- Monitoring and alerting tailored to yout threat surface

FEATURES SUMMARY

Customer IP monitoring
- Alert references to IPs when they appear on relevant channels

Customer domain & website monitoring
- Mentions of domains & websites on Pastebin, forums, IRC, etc..

Monitoring for direct threats to customer
- Awareness of malware, campaigns & attacks targeting customer

Events impacting customer locations
- Monitoring for cyber threats at a geographical level specific to customer sites

Monitoring threats to customer products & technologies
- Identify threats to products and technologies produced by customer

Monitoring threats to customer IT
- Identify threats to products & technologies used by customer
- Identify threats against social media
- Protect company reputation, social media, identify any directly stated risks or spoofs

Identifying threats to company executives
- Identify direct threats & personal data leaked online

Monitoring for direct attacks on an Industry
- Advisories of campaigns & attacks targeting [industry]

Monitoring for malware linked to customer's industry
- Advisories of methods or malware targeting [industry]

Track campaigns against an industry
- Advisories of public reporting on campaigns affecting industry.

Dashboards
- We tailor threat intelligence, specifically for all customers based on their geographical location, industry, technologies and risk profile

DATA SHEET

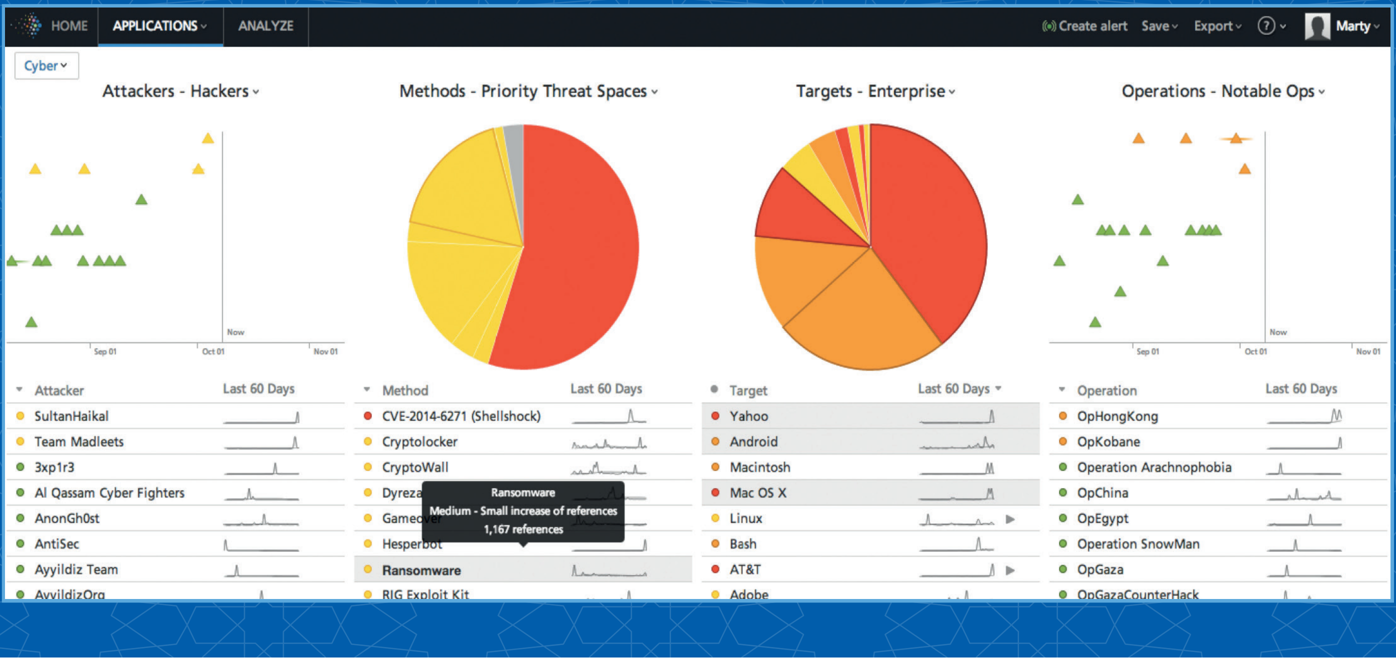
SITUATIONAL THREAT INTELLIGENCE DETECTION

Managed Security Services

Si CYBER

REPORTS AND DASHBOARDS

We provide visually rich reports with annotated details to keep customer security teams and leadership informed about the threat environment. Our SOC analysts can also detect events faster and better by ingesting these technical indicators into our SIEM.



Attacker	Last 60 Days
SultanHaikal	
Team Madleets	
3xp1r3	
Al Qassam Cyber Fighters	
AnonGh0st	
AntiSec	
Ayyildiz Team	
AyyildizOrg	

Method	Last 60 Days
CVE-2014-6271 (Shellshock)	
Cryptolocker	
CryptoWall	
Dyreza	
Gameover	
Hesperbot	
Ransomware	
RIG Exploit Kit	

Ransomware
Medium - Small increase of references
1,167 references

Target	Last 60 Days
Yahoo	
Android	
Macintosh	
Mac OS X	
Linux	
Bash	
AT&T	
Adobe	

Operation	Last 60 Days
OpHongKong	
OpKobane	
Operation Arachnophobia	
OpChina	
OpEgypt	
Operation SnowMan	
OpGaza	
OpGazaCounterHack	

REAL TIME ALERTING

We provide real time alerting to notify customers about breached content and credentials or planned attacks based on indexing customer URL's, domains, VIP's, IP and assets against specific mentions on the dark web.

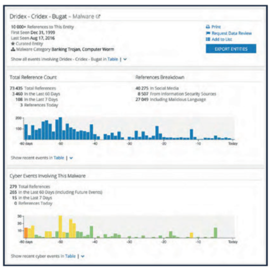
INTELLIGENCE BRIEFS

We provide customers with specific Intel Briefs relating to specific threat actors targeting their organisations or industry verticals. Our intel briefs provide technical indicators which our customers may ingest into their own tools to build defensive tactics to block or monitor these attackers, including IP addresses, hashes, vulnerabilities, domains, threat actor groups and malware, to provide threat analysts instant context into threats relevant to their organisations.

All intelligence is provided with a risk scoring based on evidence to enable prioritisation. Risk rating it based on the evidence collected and curated by our Web Intelligence Engine to help customers make fast and evidence-based information security decisions.

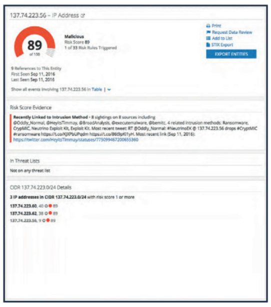
Threat Actor Groups

Malware

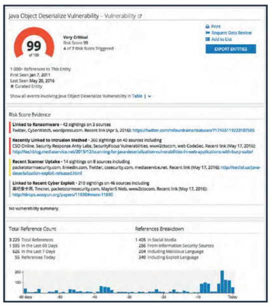


Domains

IP Addresses



Vulnerabilities



Hashes