Introduction to AutoFocus

Threat Product Management

paloalto NETWORKS

the network security company™

Increasingly complex security solutions

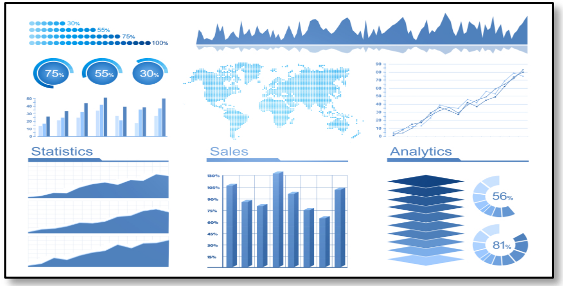
Threat intelligence feeds

Intrusion detection systems

Open source data

Data sharing organizations

Home-grown tools

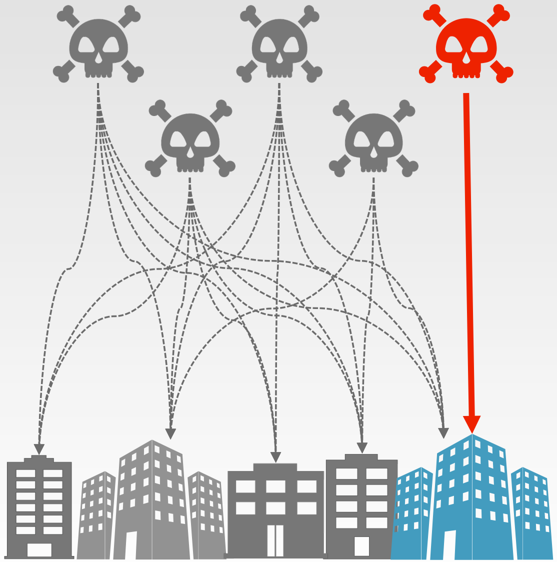


Attempts to bring it all together

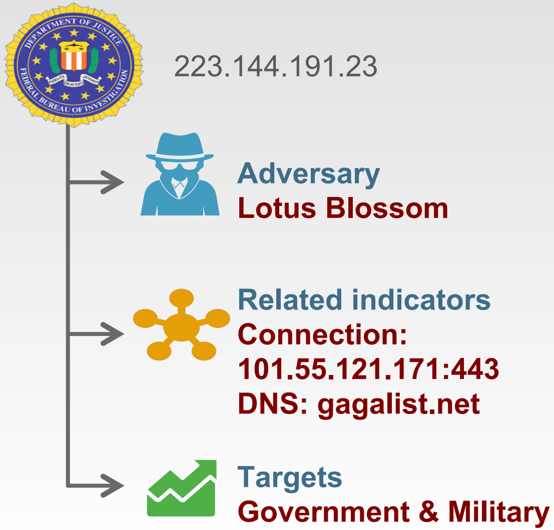
Longer response times and less effective protection

What we need …

Prioritize important events



Context around indicators and incidents



223.144.191.23

Adversary
Lotus Blossom

Related indicators
Connection: 101.55.121.171:443
DNS: gagalist.net

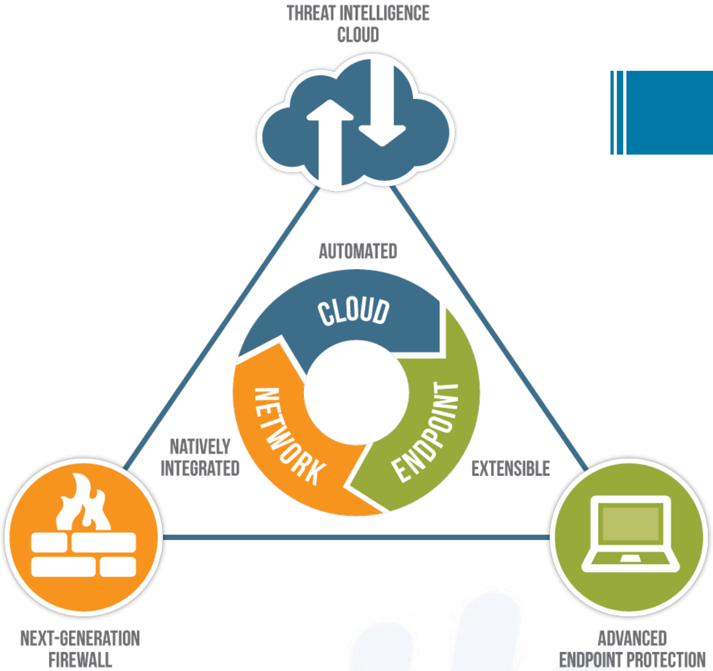
Targets
Government & Military

Quick and proactive response

Automatically export high-value indicator sets to security controls

Prevent future attacks

AutoFocus: Actionable intelligence



THREAT INTELLIGENCE CLOUD

AUTOMATED

CLOUD

NETWORK

ENDPOINT

NATIVELY INTEGRATED

EXTENSIBLE

NEXT-GENERATION FIREWALL

ADVANCED ENDPOINT PROTECTION

Analyst

Sec-Ops

AutoFocus is …	AutoFocus is not …
a Threat Intelligence & analysis Service	a Threat Intelligence Feed
A hosted service with web portal and APIs	required to be activated on firewalls or Traps
an off-line malware analysis tool	an in-line unknown malware detection tool
is priced based upon number of users	priced based upon number of devices
integrated with WildFire Cloud	integrated with WF-500
based on WildFire analysis reports	based on firewall traffic logs data or a SIEM

Prioritize events

Highlight unique, targeted attacks and take action

Find the important events

Tags alert on important events

Highlight important indicators

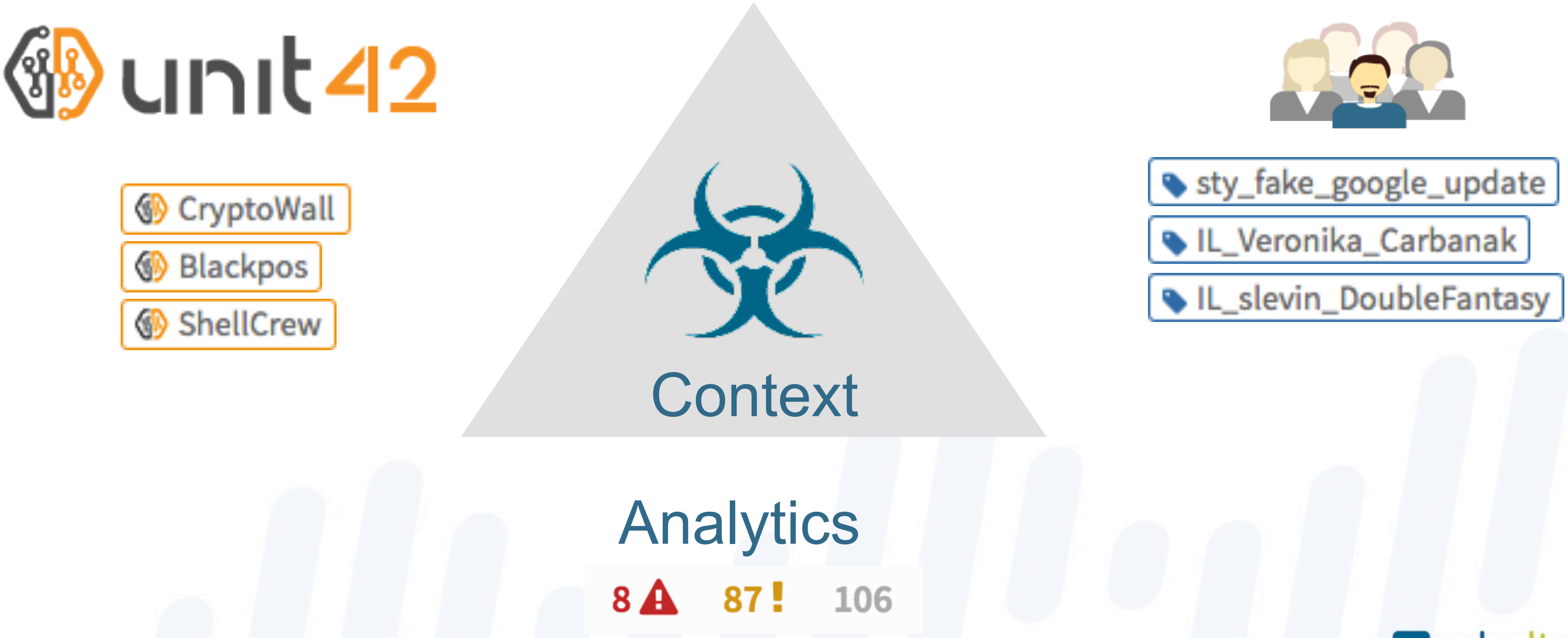
Statistical analysis surfaces unique indicators

Who is behind the attack

Tag identifies the actor and attack techniques

Adding Context

Intelligence on actors, campaigns and attack methods



unit42

- CryptoWall
- Blackpos
- ShellCrew

Context

- sty_fake_google_update
- IL_Veronika_Carbanak
- IL_slevin_DoubleFantasy

Analytics

8 ⚠ 87 ! 106

Proactive response

Quickly respond to events with actionable intelligence

1 Context around the adversary, attacks, and campaigns

2 Highlights associated attack techniques and indicators

3 Pivot to related high-value indicators

Export indicator sets to prevent future attacks

paloalto
NETWORKS

the network security company™

AutoFocus is ideal for …

- Majority of existing customers that have moderate to advanced in-house SOC/IR capability
- Customers who use WildFire public cloud
- SOC operators, who will use AutoFocus' Alerting based upon Unit42 tags and using export to file features to feed Dynamic Block lists on their firewalls
- Malware Analysts who will use AutoFocus searching, Tagging, Pivoting capabilities to
- Customers who have in house integrated dashboards will find AutoFocus API feature most appealing