Zero Trust

An Alternative Network Security Model
Palo Alto Networks Approach

Mark Harman
Federal Cyber Architect

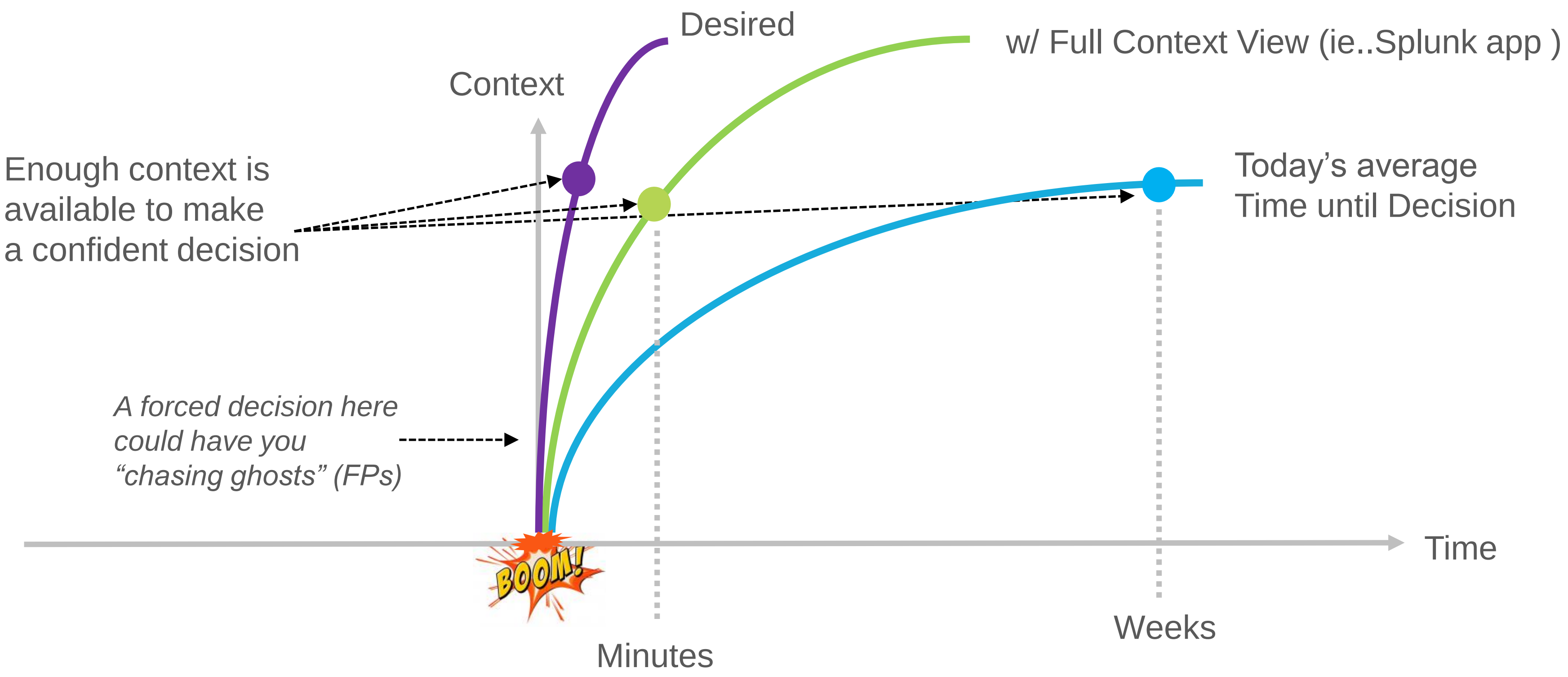
Agenda

- What is Zero Trust
- Why Palo Alto Networks/ Deep Rich Context
- Examples
- Steps to Zero Trust
- We all need friends

What is Zero Trust…

- **Zero trust** is a security model based on the principle of maintaining strict access controls down to the application and not trusting anyone or any port by default, even those already inside the network perimeter.
- Zero Trust, rooted in the principle of "**never trust, always verify**,"
- Leveraging **micro-segmentation** and **granular perimeters enforcement**, based on user, data and location
- Adopt a **least-privileged access strategy** and strictly enforce access control
- **"Always verify,"** meaning inspect and log all traffic with **deep rich context**.

Why do we need deep rich context….



Enough context is available to make a confident decision

A forced decision here could have you "chasing ghosts" (FPs)

What is Deep Rich Context, Palo Alto Networks style;

From TR

Traps

- **Exploit, Ransomware and malware** prevention
- **ML** and **AI** to detect and respond to sophisticated attacks
- **Zero Day** (Malware, Begin or Greyware)
- **Prevention** offline and online

From MG

Magnifier

XDR

Analysis

AF

- **1000+ behaviors**
- **ML** semi-supervise
- **Full chain of events** (including network)
- **Tags** (Actors, Campaigns, Exploits, Tools, IOCs**)**

From

Next-Generation Firewall

VM Series

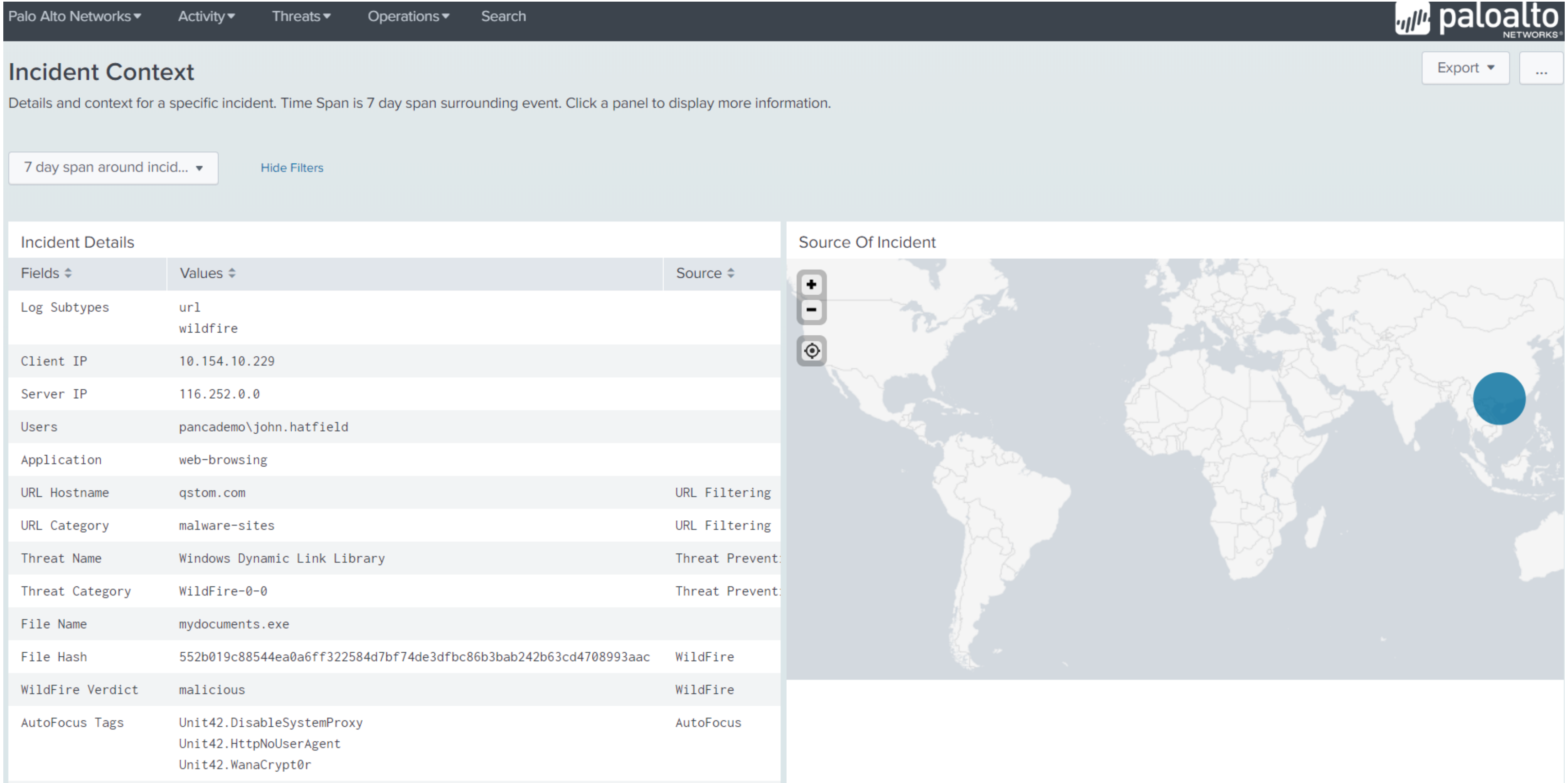
GP

GlobalProtect

- **AppID**
- **UserID** and **Group**
- **ThreatID** (IPS/IDS)
- **URL** and **URL Category**
- **Zero Day** (Malware, Begin or Greyware)
- **DLP** (contains CC, SSN, etc.)
- **File Info** (sha256, type, etc.)
- **Endpoint OS** (patched, drive encrypted, AV)

paloalto NETWORKS

Example 1 of deep context



Incident Context

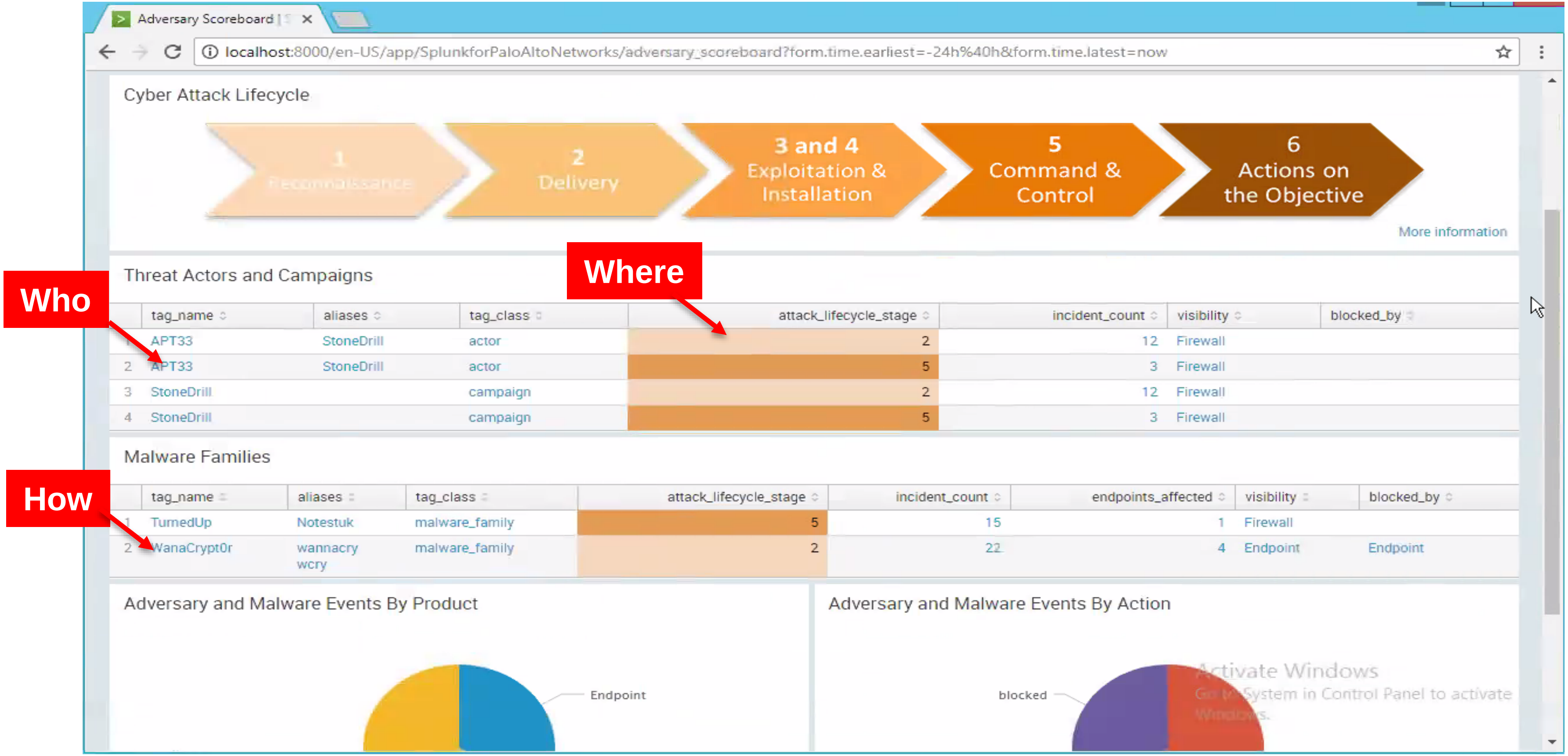
Details and context for a specific incident. Time Span is 7 day span surrounding event. Click a panel to display more information.

Incident Details

Fields	Values	Source
Log Subtypes	url wildfire	
Client IP	10.154.10.229	
Server IP	116.252.0.0	
Users	pancademo\john.hatfield	
Application	web-browsing	
URL Hostname	qstom.com	URL Filtering
URL Category	malware-sites	URL Filtering
Threat Name	Windows Dynamic Link Library	Threat Prevent:
Threat Category	WildFire-0-0	Threat Prevent:
File Name	mydocuments.exe	
File Hash	552b019c88544ea0a6ff322584d7bf74de3dfbc86b3bab242b63cd4708993aac	WildFire
WildFire Verdict	malicious	WildFire
AutoFocus Tags	Unit42.DisableSystemProxy Unit42.HttpNoUserAgent Unit42.WanaCrypt0r	AutoFocus

Source Of Incident

Leadership now knows Ops Risk—and can Build and Spend Accordingly



Adversary Scoreboard |

localhost:8000/en-US/app/SplunkforPaloAltoNetworks/adversary_scoreboard?form.time.earliest=-24h%40h&form.time.latest=now

Cyber Attack Lifecycle

1 Reconnaissance

2 Delivery

3 and 4 Exploitation & Installation

5 Command & Control

6 Actions on the Objective

More information

Threat Actors and Campaigns

Who

Where

	tag_name	aliases	tag_class	attack_lifecycle_stage	incident_count	visibility	blocked_by
1	APT33	StoneDrill	actor	2	12	Firewall	
2	APT33	StoneDrill	actor	5	3	Firewall	
3	StoneDrill		campaign	2	12	Firewall	
4	StoneDrill		campaign	5	3	Firewall	

Malware Families

How

	tag_name	aliases	tag_class	attack_lifecycle_stage	incident_count	endpoints_affected	visibility	blocked_by
1	TumedUp	Notestuk	malware_family	5	15	1	Firewall	
2	WanaCrypt0r	wannacry wcry	malware_family	2	22	4	Endpoint	Endpoint

Adversary and Malware Events By Product

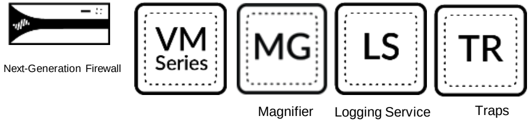
Adversary and Malware Events By Action

The 5 steps to a Zero Trust network

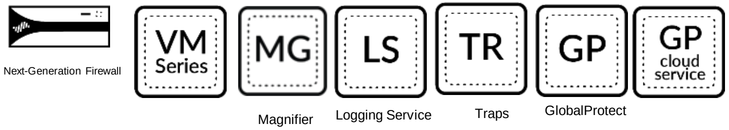
- Define your Protect Surface

Next-Generation Firewall
VM Series
MG
LS
Magnifier
Logging Service

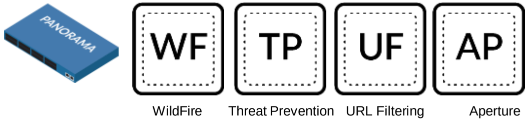
- Map the transaction flows



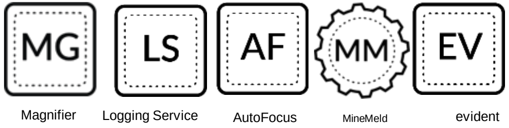
- Architect a Zero Trust network



- Create Zero Trust Policy



- Monitor and maintain the network



PARTNER ECOSYSTEM

CLOUD

amazon web services
Microsoft
Google Cloud Platform

THREAT INTELLIGENCE

THE MEDIA TRUST
PHISHME
WEBROOT
THREAT CONNECT
mnemonic
THREATQUOTIENT
ANOMALI
Threat STOP
Recorded Future

VIRTUALIZATION

openstack CLOUD SOFTWARE
vmware
hp
NUTANIX The Enterprise Cloud Company
nuagenetworks From Nokia
CITRIX
Juniper CONTRAIL
NEC
MIRANTIS
big switch networks
FUJITSU
cisco
ARISTA
intel

ENTERPRISE SECURITY

THALES
gemalto security to be free
savvius
TITUS
IONIC
AREA 1
DIGITALGUARDIAN
FOURV SYSTEMS
proofpoint
PHISHME
Attivo NETWORKS
PROTECTWISE™
TRAPX SECURITY
VENAFI
TANIUM™
tenable network security
SKYSEA Client View
NUBEVA
E8 SECURITY
GURUCUL PREDICTIVE SECURITY ANALYTICS
BeyondTrust
GUIDANCE SOFTWARE
Symantec.
VECTRA
esentire
Corvil
BACKBOX
tripwire
PICUS SECURITY
RAPID7
ziften
exabeam
HOB Cyber Security
IntelliGO
Canon

SD-WAN

riverbed
TALARI Network
nuagenetworks From Nokia
ECESSA™
CLOUDGENIX
silver peak
vmware
viptela Software Defined WAN
CITRIX
velocloud™

IDENTITY& ACCESS MANAGEMENT

Centrify
CYBERARK
DUO
SECUREAUTH
RSA
gemalto security to be free
Microsoft
okta
Ping Identity
altipeak security
SyferLock
AUTHOMATE SET YOURSELF FREE
Entrust Datacard
SWIVEL Adaptable. Active. Authentication

NETWORKING

AVAYA
Sonus
vmware NSX
ForeScout
Extreme Connect Beyond the Network
ARISTA
BRADFORD NETWORKS
GARLAND TECHNOLOGY See every bit, byte, and packet
Gigamon
plenarylogic™
Pulse Secure
Interface Masters TECHNOLOGIES Innovative Network Solutions
NIAGARA NETWORKS
cisco
AlaxalA
IXIA
Allied Telesis
RAD
Network Critical
portnox™
saasyan

SECURITY ANALYTICS

splunk>
LogRhythm
BlackStratus
SIFT SECURITY
plixer
EIQ ntinuous Security Intelligence
RSA
ArcSight ESM
Logsign
IBM Security QRadar
ALIEN VAULT
Infoscience
LogicMonitor

IOT

BAYSHORE
aruba a Hewlett Packard Enterprise company
armis
DRAGOS
NOZOMI NETWORKS
ForeScout
SECURITY MATTERS
Thomason TECHNOLOGIES, LLC
Honeywell

MOBILITY

airwatch by vmware
Extreme Connect Beyond the Network
Microsoft
aruba a Hewlett Packard Enterprise company
CITRIX
MobileIron
Ruckus WIRELESS

ORCHESTRATION & SECURITY AUTOMATION

tail-f
HEXADITE Automated Cyber Incident Response
ANSIBLE
Alcatel-Lucent
Phantom
intellment security
AppViewX
HashiCorp Terraform
NetCracker
servicenow
tufin
DFLABS
ManageEngine
swimlane
DEMISTO
indeni powering smart networks
REDSEAL
SIEMPLIFY
UBIqube
SKYBOX SECURITY
FIREMON
algosec

paloalto NETWORKS

THANK YOU

Twitter: @PaloAltoNtwks