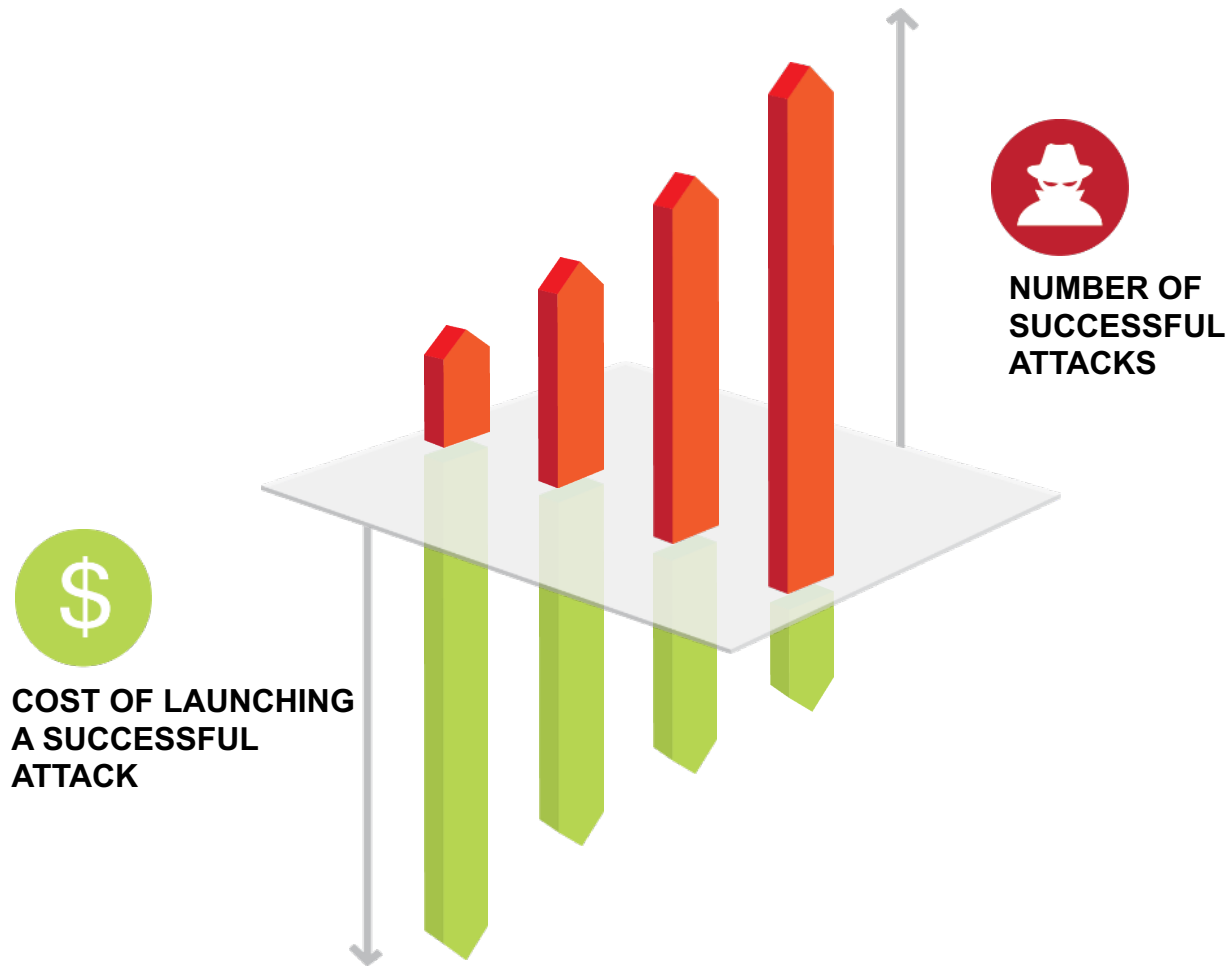


The Economics of Cyber Security

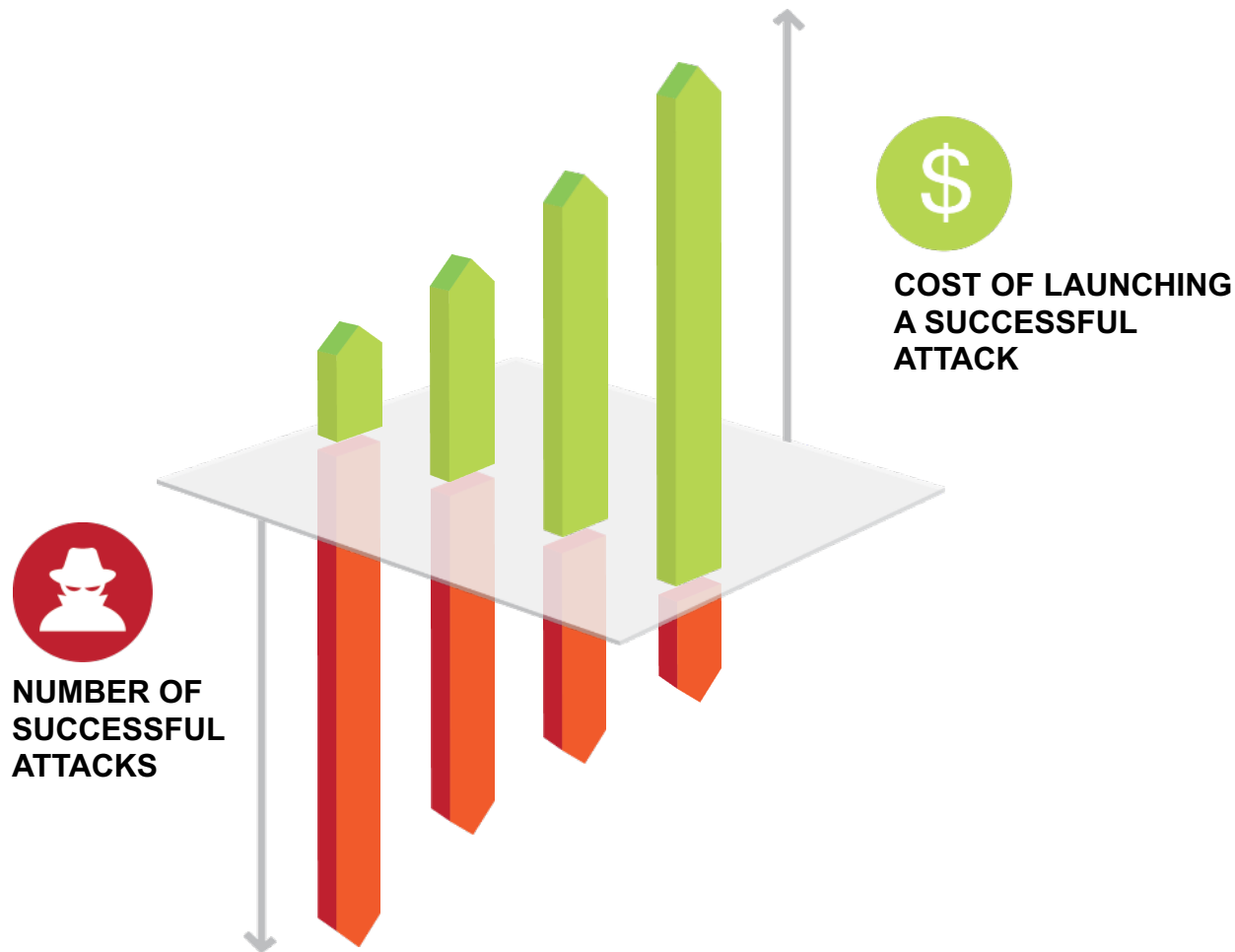
Mr Arnaud KOPP, Chief Security Officer, Southern Europe



Today



WE MUST CHANGE THE *COST* OF ATTACKS



THE ECONOMICS HAVE CHANGED



Available
malware &
exploits

+



Effective
automated
toolkits

+



Cheaper
computing
power

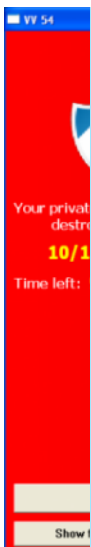
=



Successful
data
breaches

Adversary arithmetic

ATTACKERS ARE LAZY: TESLACRYPT



Take

```
.text:0041 1 PCHAR .text:00412A0D
.text:0041 2 { .text:00412A0E
.text:0041 3 .text:00412A11
.text:0041 4 PCHAR .text:00412A16
.text:0041 5 if .text:00412A18
.text:0041 6 .text:00412A1A
.text:0041 7 .text:00412A1F
.text:0041 8 .text:00412A22
.text:0041 9 .text:00412A23
.text:0041 10 PCHAR .text:00412A24
.text:0041 11 .text:00412A26
.text:0041 12 STR .text:00412A28
.text:0041 13 PCHAR .text:00412A2A
.text:0041 14 .text:00412A2B
.text:0041 15 .text:00412A2D
.text:0041 16 PCHAR .text:00412A2F
.text:0041 17 .text:00412A31
.text:0041 18 .text:00412A33
.text:0041 19 .text:00412A37
.text:0041 20 .text:00412A37 loc_412A37:
.text:0041 21 STR .text:00412A37
.text:0041 22 PCHAR .text:00412A3A
.text:0041 23 .text:00412A3F
.text:0041 24 .text:00412A41
.text:0041 25 STR .text:00412A43
.text:0041 26 PCHAR .text:00412A48
.text:0041 27 .text:00412A4B
.text:0041 28 .text:00412A4C
.text:0041 29 STR .text:00412A4E
.text:0041 30 .text:00412A51
.text:0041 31 .text:00412A56
.text:0041 32 .text:00412A58
.text:0041 33 .text:00412A5A
.text:0041 34 .text:00412A5F
.text:0041 35 .text:00412A62
.text:0041 36 .text:00412A64
.text:0041 37 .text:00412A65
.text:0041 38 }
.text:0041 39 ret
```

```
push edi
mov edi, [ebp+var_4]
push 0CEBF17E6h ; dwProcNameHash
push 2 ; dwModule
push 0 ; Dll
call GetProcAddressEx
add esp, 0Ch
push ebx
push esi
push 0
push 1
push 0
push edi
call eax
test eax, eax
jz short loc_412A37
mov ecx, [ebx]
mov byte ptr [esi+ecx], 0

; CODE XREF: sub_4129F0+3F'j
mov edi, [ebp+var_4]
push 0D4B3D42h ; dwProcNameHash
push 2 ; dwModule
push 0 ; Dll
call GetProcAddressEx
add esp, 0Ch
push edi
call eax
mov edi, [ebp+iv]
push 72760BB8h ; dwProcNameHash
push 2 ; dwModule
push 0 ; Dll
call GetProcAddressEx
add esp, 0Ch
push 0
push edi
call eax
```

2013 And mimics Cryptowall And uses dynamic library & function loading...



IMPACT OF AUTOMATION

68 percent

Automated tools make it easier to execute attacks

64 percent

Tools are highly effective

63 percent

Increased usage of toolkits

\$1,387

Spent on toolkits per attack

MASSIVE OVERLOAD



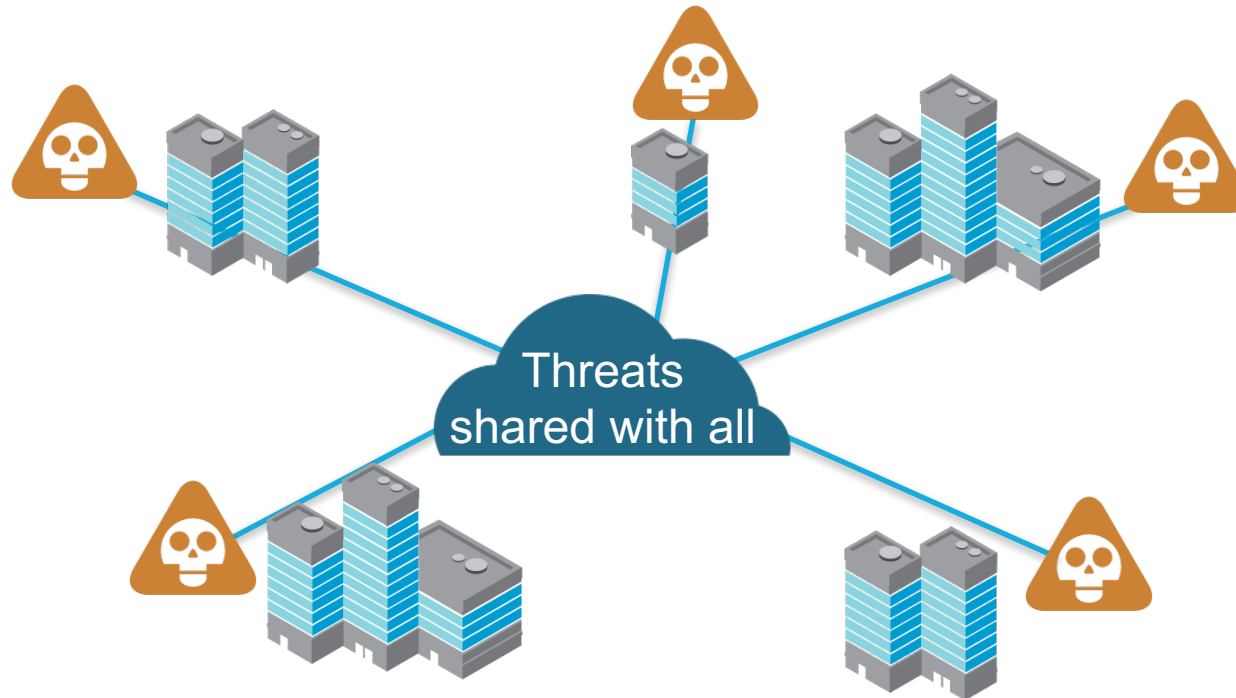
10,000+
events per month

64%
duplicates

52%
false positives

40%
human inspection

SHARING INCREASES RESILIENCE



Respondents believe that **39 percent** of attacks can be prevented by shared intelligence.

AUTOMATED: YOUR VIEW

AUTOFOCUS

Welcome, Greg Day Palo Alto Networks Researcher

Dashboard

Search

Alerts

Tags

Export List

Settings

Search

Match All of the following conditions:

WildFire Verdict is Malware
Destination Country is Netherlands
Time is in the range Aug 1, 2015 12:00:00am Nov 9, 2015 11:59:59pm

Search [Icons] debug

Samples Sessions Statistics Domain, URL & IP Address Information

My Samples Public Samples All Samples

Samples: 138 # Sessions: 842 First Seen: 08/30/2011 5:00:06am Last Seen: 11/08/2015 11:19:05am

Malware Download Sessions



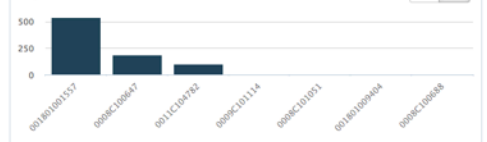
Top Applications



Top Malware



Top Firewalls



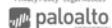
Source Countries



Top Tags

| Tag | Matching # Samples | Total # Samples | Last Hit |
|--|--------------------|-----------------|-----------------------|
| Bartalex | 53 | 31,529 | 11/07/2015 3:18:03pm |
| il_tm_word_download_exe | 53 | 777 | 11/08/2015 4:33:21pm |
| il_tm_winword_spawn_appdata | 49 | 6,701 | 11/08/2015 5:55:22pm |
| il_tm_winword_spawn_temp | 49 | 1,223 | 11/08/2015 10:37:23am |
| gsrt_ak_ModifyNetworkOrBrowserSettings | 42 | 12,498,668 | 11/08/2015 6:00:29pm |
| gsrt_blevene_UnusualNetworkBehaviors | 40 | 3,267,113 | 11/08/2015 6:00:22pm |
| Dridex | 38 | 15,372 | 11/08/2015 5:04:28pm |
| gsrt_ak_SuspectHTTP | 19 | 3,283,981 | 11/04/2015 10:45:20pm |

Component Versions
Server Time: 5:21AM PST
Privacy Policy Legal Notices



AUTOMATED: FOR ALL

AUTOFOCUS

Welcome, Greg Day Palo Alto Networks Researcher

Dashboard

Search

Alerts

Tags

Export List

Settings

Search

Match **All** of the following conditions:

WildFire Verdict is Malware
Destination Country is Netherlands
Time is in the range Aug 1, 2015 12:00:00am Nov 9, 2015 11:59:59pm

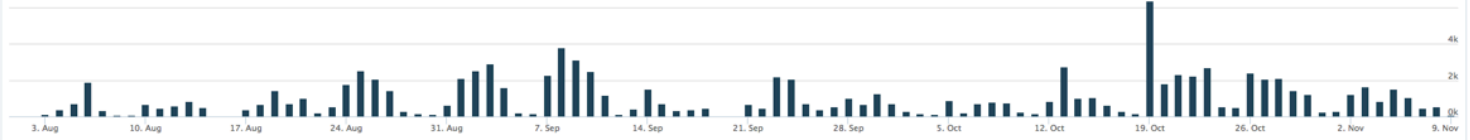
Q Search [Icons] # debug

Samples Sessions Statistics Domain, URL & IP Address Information

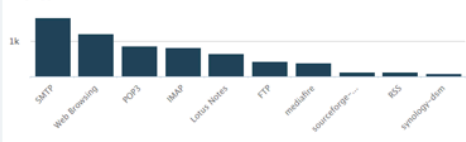
My Samples Public Samples All Samples

Samples: 9,752 # Sessions: 102,819 First Seen: 07/14/2011 10:15:04pm Last Seen: 11/09/2015 2:05:11am

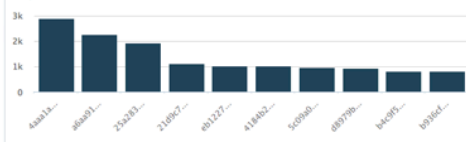
Malware Download Sessions



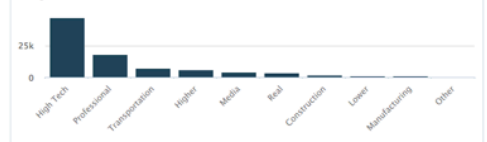
Top Applications



Top Malware



Target Industries



Source Countries




Top Tags

| Tag | Matching # Samples | Total # Samples | Last Hit |
|---|--------------------|-----------------|-----------------------|
| ggrt_blevene_UnusualNetworkBehaviors | 6,411 | 3,267,113 | 11/08/2015 6:00:22pm |
| ggrt_ak_SuspectHTTP | 4,144 | 3,283,981 | 11/04/2015 10:45:20pm |
| ggrt_ak_ModifyNetworkOrBrowserSettings | 2,750 | 12,498,636 | 11/08/2015 6:00:29pm |
| ggrt_blevene_upatre_UPDATE | 2,166 | 52,432 | 11/08/2015 5:59:11pm |
| ggrt_ak_SuspectUriDomainIp | 1,584 | 3,326,195 | 11/08/2015 6:01:17pm |
| tmalivanch_CreateSuspended_vbc_exe | 379 | 47,226 | 11/08/2015 5:41:37pm |
| il_tbar_commodity_download_ip_details_from_external_site | 290 | 58,828 | 11/08/2015 5:55:47pm |
| il_tbar_commodity_http_download_ip_details_from_external_site | 284 | 58,387 | 11/08/2015 5:55:47pm |



IDENTIFYING 1 IN 7.4 BILLION



GLEN STEWART GODWIN


Unlawful Flight to Avoid Confinement - Murder, Escape

REWARD: The FBI is offering a reward of up to \$100,000 for information leading directly to the arrest of Glen Stewart Godwin.

Glen Stewart Godwin is being sought for his 1987 escape from Folsom State Prison in California, where he was serving a lengthy sentence for murder. Later in 1987, Godwin was arrested for drug trafficking in Puerto Vallarta, Mexico. After being convicted, he was sent to a prison in Guadalajara. In April of 1991, Godwin allegedly murdered a fellow inmate and then escaped five months later.

Godwin is fluent in Spanish and may be traveling throughout Central and South America, and Mexico. He is thought to be involved in narcotics distribution.

| |
|----------------|
| SUMMARY |
| SCARS & MARKS |
| ALIASES |
| DESCRIPTION |
| MORE PHOTOS |
| GET POSTER |
| EN ESPAÑOL |
| SUBMIT A TIP |



Hair: Black/Salt and Pepper

Eyes: Green

Complexion: Medium to Dark

Sex: Male

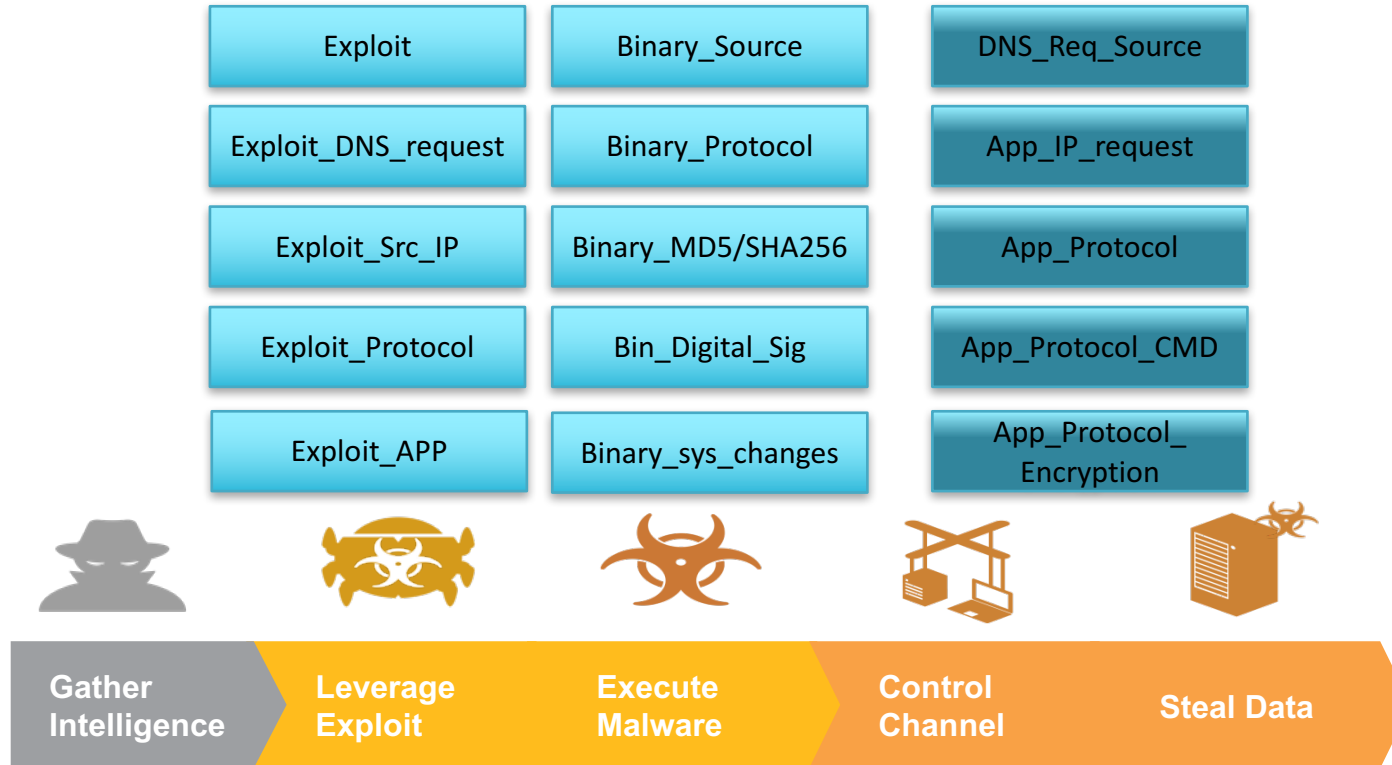
Race: White

Nationality: American



<https://www.fbi.gov/wanted/topten>

THE "MAGIC" : CORRELATION



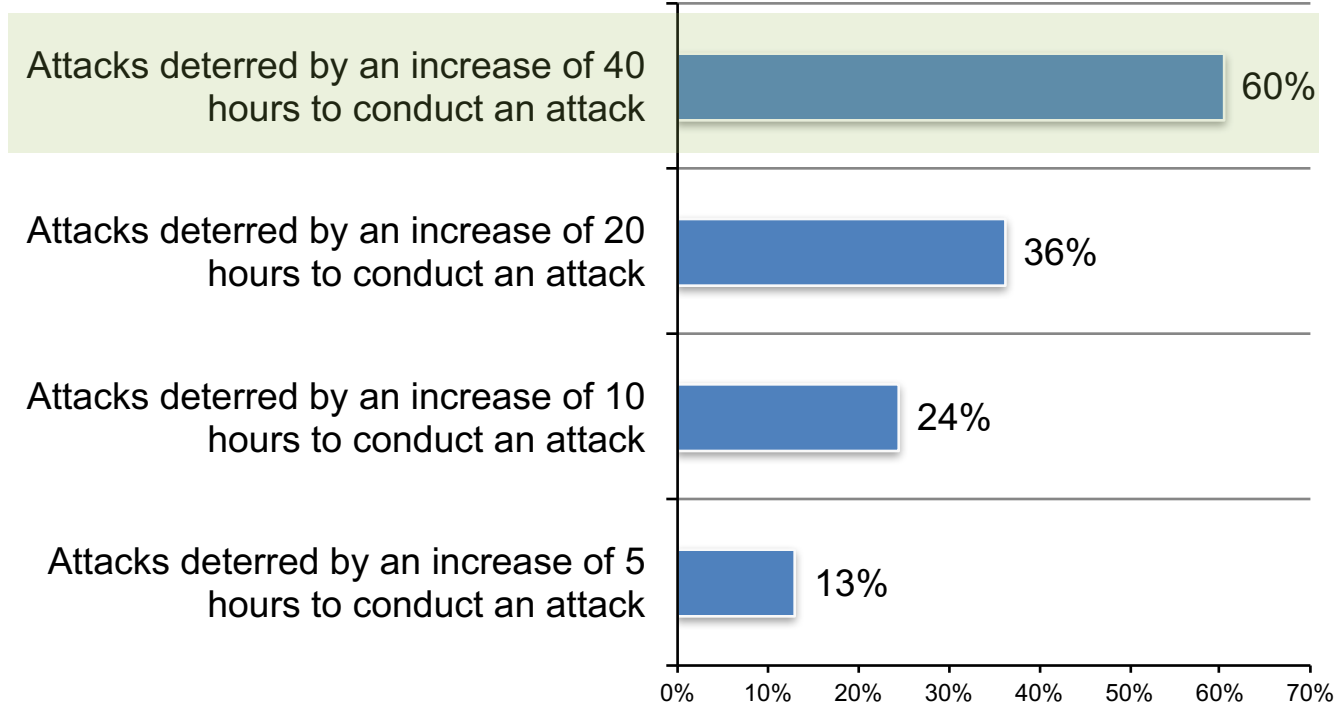
THREAT SHARING: INDUSTRY COOPERATES



FOUNDING MEMBERS



TIME IS OUR FRIEND



Increasing the time to breach an organization by less than 2 days **deters 60%** of attacks

5 THOUGHTS

1. Share intelligence with your security partners
2. Collaborate in industry communities
 - Industry – FS-ISAC
 - National – CISP
 - Vendor – Cyber Threat Alliance
3. We have the CPU power to turn the scales: the cloud
4. Kill the whole attack lifecycle, not just the attack binary
5. Integrated & automated security platforms are the enemy of the attacker

Palo Alto Networks Academy Overview



ACADEMY

■ Purpose

- The Palo Alto Networks Academy is designed to equip students with the next-generation cybersecurity knowledge they'll need to succeed in today's rapidly changing cyber-threat landscape

■ Who & Where?

- 160+ Authorized Academy Centers (AACs) in 20 countries (as of January 2017)
- Any degree-granting, nationally accredited university or college

■ Academy Benefits

- Faculty training (TTT) at no cost
- Training lab support at no cost
- Courseware at no cost
- PCNSE certification vouchers at 50% discount

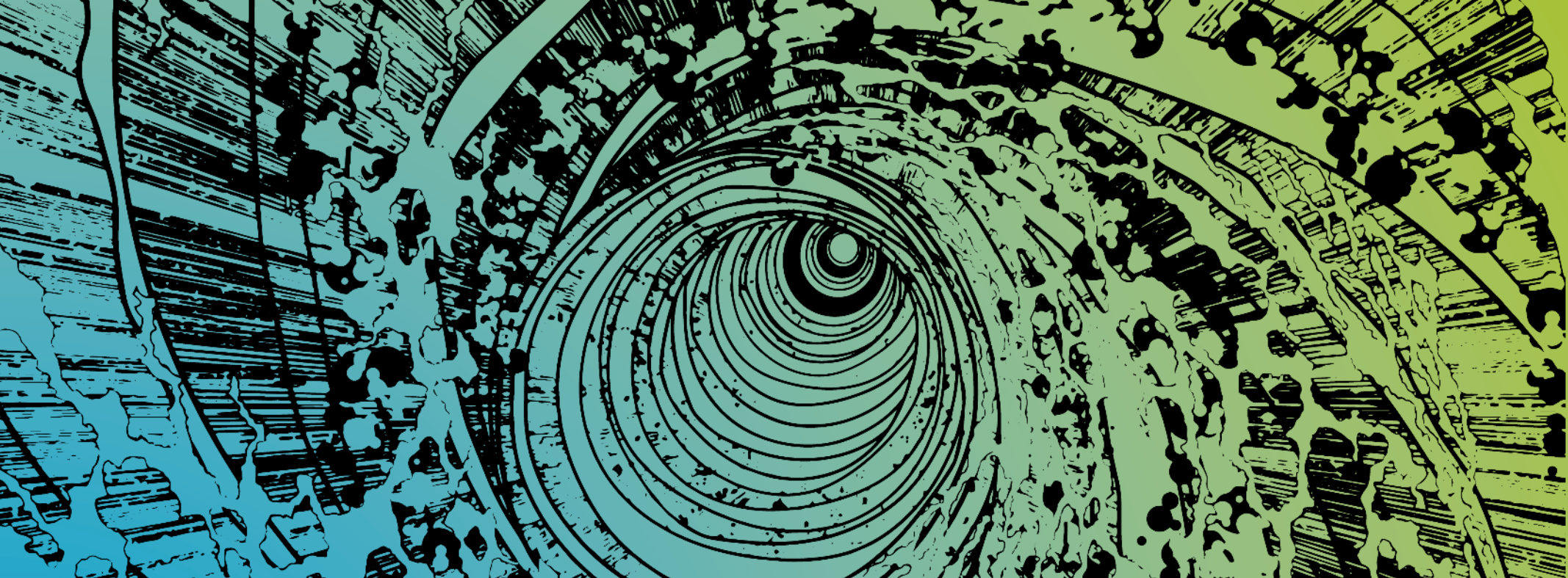
■ How?

www.paloaltonetworks.com/academy



Academy Colleges & Universities





THANK YOU



akopp@paloaltonetworks.com



@akopp92



LinkedIn

www.linkedin.com/in/arnaudkopp/



+33 6 09 16 75 66

 paloalto
NETWORKS®