



**Check Point**  
SOFTWARE TECHNOLOGIES LTD

**CPX  
360**

# SUPERCHARGE YOUR SOC

with InfinitySOC

Eytan Segal, Head of Product Management  
Avishai Duer, R&D Director

WELCOME TO THE FUTURE OF CYBER SECURITY

A customer story...



# A GLOBAL MANUFACTURING COMPANY

- HQ in EU
- 20K employees, €2B revenue
- 24x7 SOC



**FEBRUARY 23, 2019**

- Ryuk ransomware outbreak
- 500 systems are down
- Production is paralyzed

*Why did this happen???*

*(we'll skip the story on how we saved them...)*

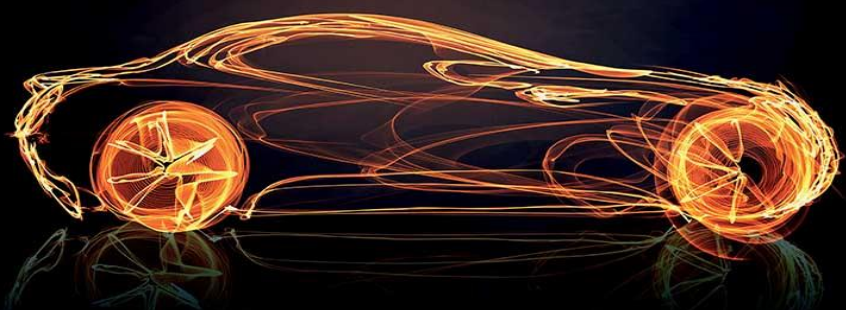
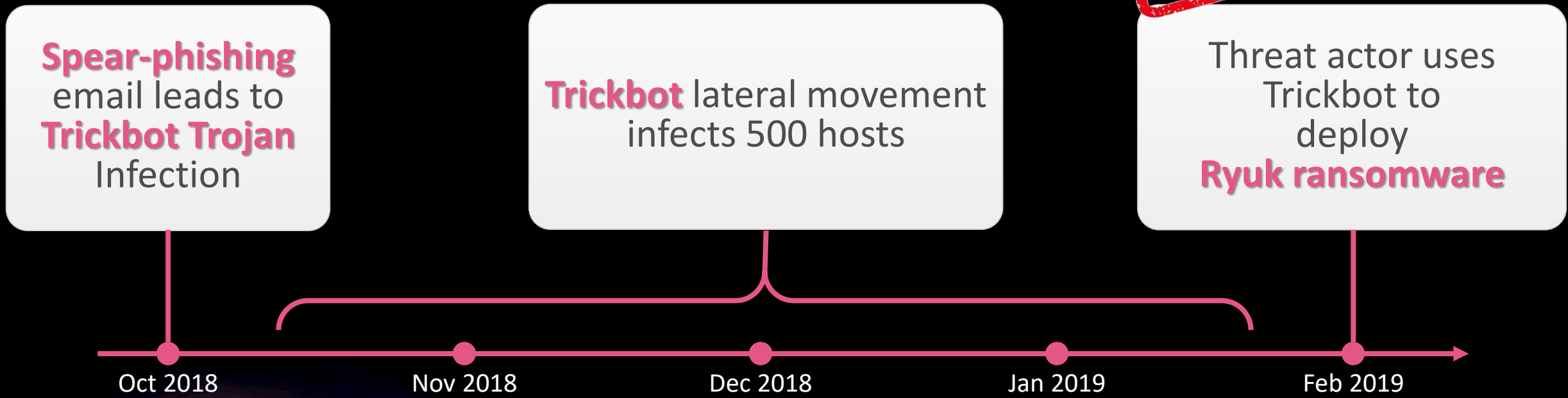
**EMERGENCY  
CALL**

**INCIDENT RESPONSE TEAM**  
  
**CHECK POINT**





# How did the SOC miss it?



# SOCs know they have a problem!

53% of SOC  
Rate their own operation as **immature**

Check Point survey, n=199



# SOC teams face formidable challenges

Too many alerts,  
too many false  
positives

Lack of insights &  
actionable  
information

Not enough skilled  
people

Result: critical attacks are missed, until it's too late



Check Point  
SOFTWARE TECHNOLOGIES LTD

Introducing



CHECK POINT

**INFINITY SOC** BETA

SUPERCHARGE YOUR SECURITY OPERATIONS

WELCOME TO THE FUTURE OF CYBER SECURITY

©2019 Check Point Software Technologies Ltd.



CHECK POINT

**INFINITY SOC** BETA



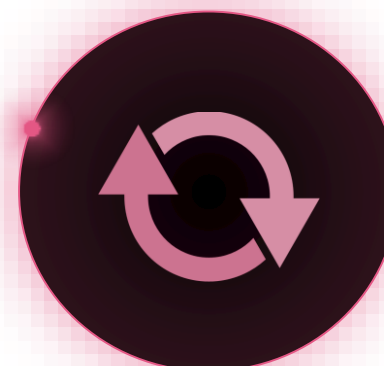
Check Point  
SOFTWARE TECHNOLOGIES LTD



Actionable  
Insights



Accelerate  
Investigation



Effective  
Response & Prevention

# BOOST INVESTIGATION AND RESPONSE





CHECK POINT

# INFINITY SOC<sup>BETA</sup>



Check Point  
SOFTWARE TECHNOLOGIES LTD



SIEM

Maintain  
analyst workflow



API

Automate & integrate



Web UI

Rich native experience  
in Infinity Portal

## INTEGRATES WITH YOUR SOC



CHECK POINT  
**INFINITY SOC** BETA



Actionable  
Insights



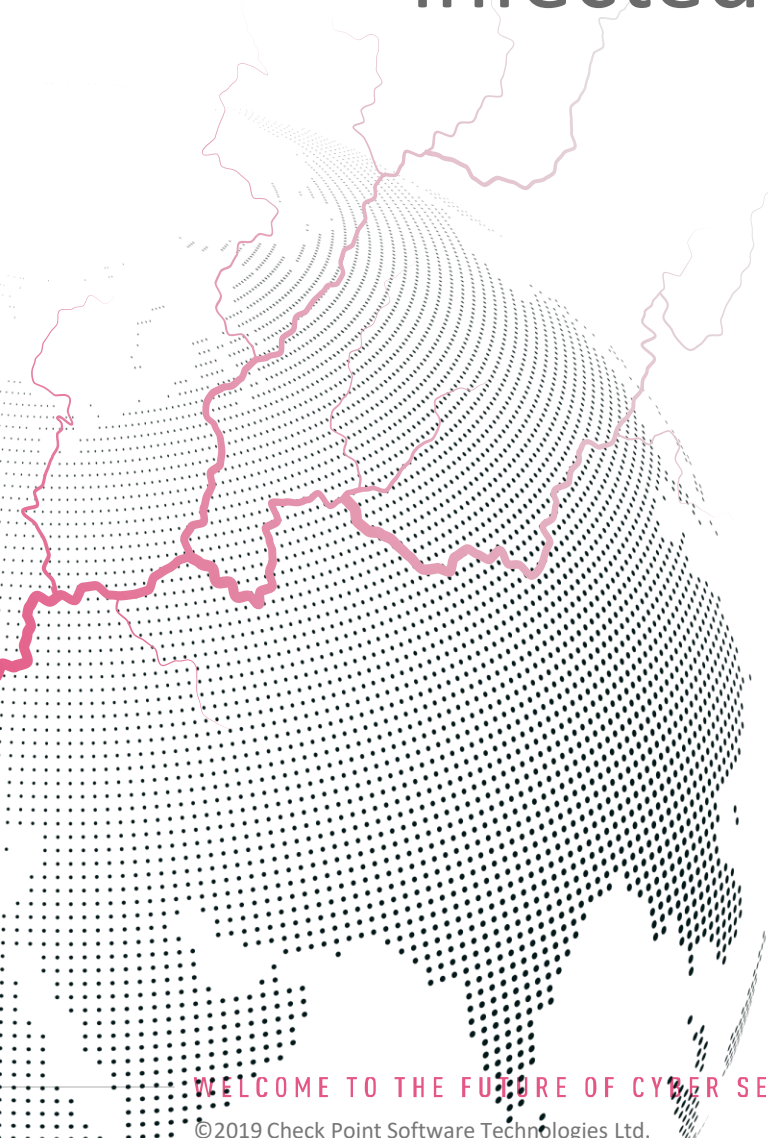
Accelerate  
Investigation



Effective  
Response & Prevention

# BOOST INVESTIGATION AND RESPONSE

# How do you **expose** a host that's infected with **stealth malware**?



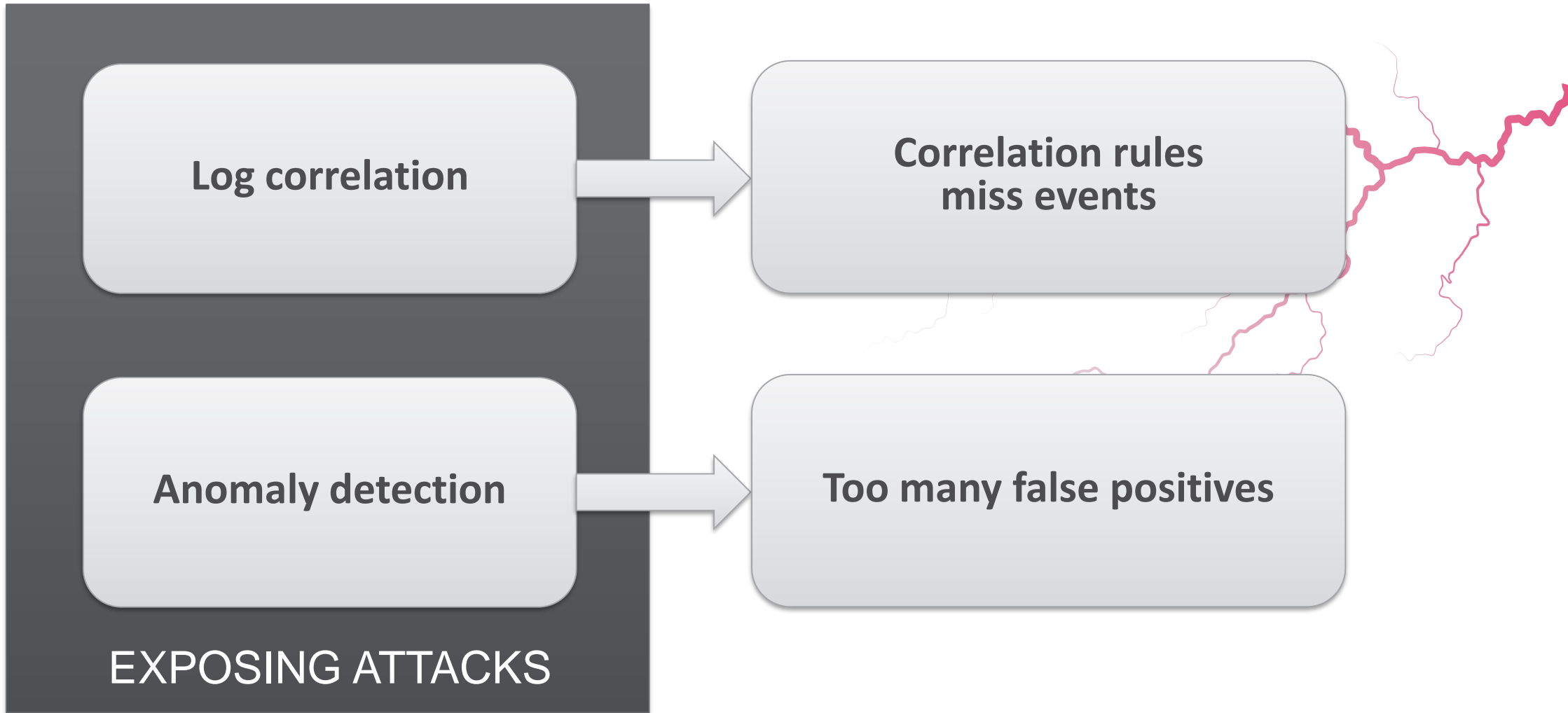
SIEM

50M logs/day

YOUR NETWORK

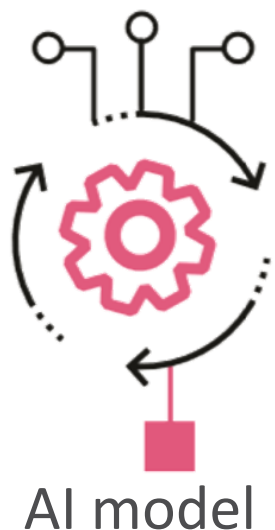
10,000 hosts

# Traditional approaches **fail**

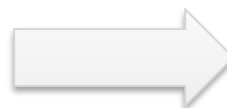




# Accurately exposing stealth attacks



1. Learn from ThreatCloud
2. Apply to customer events
3. Customer feedback loop

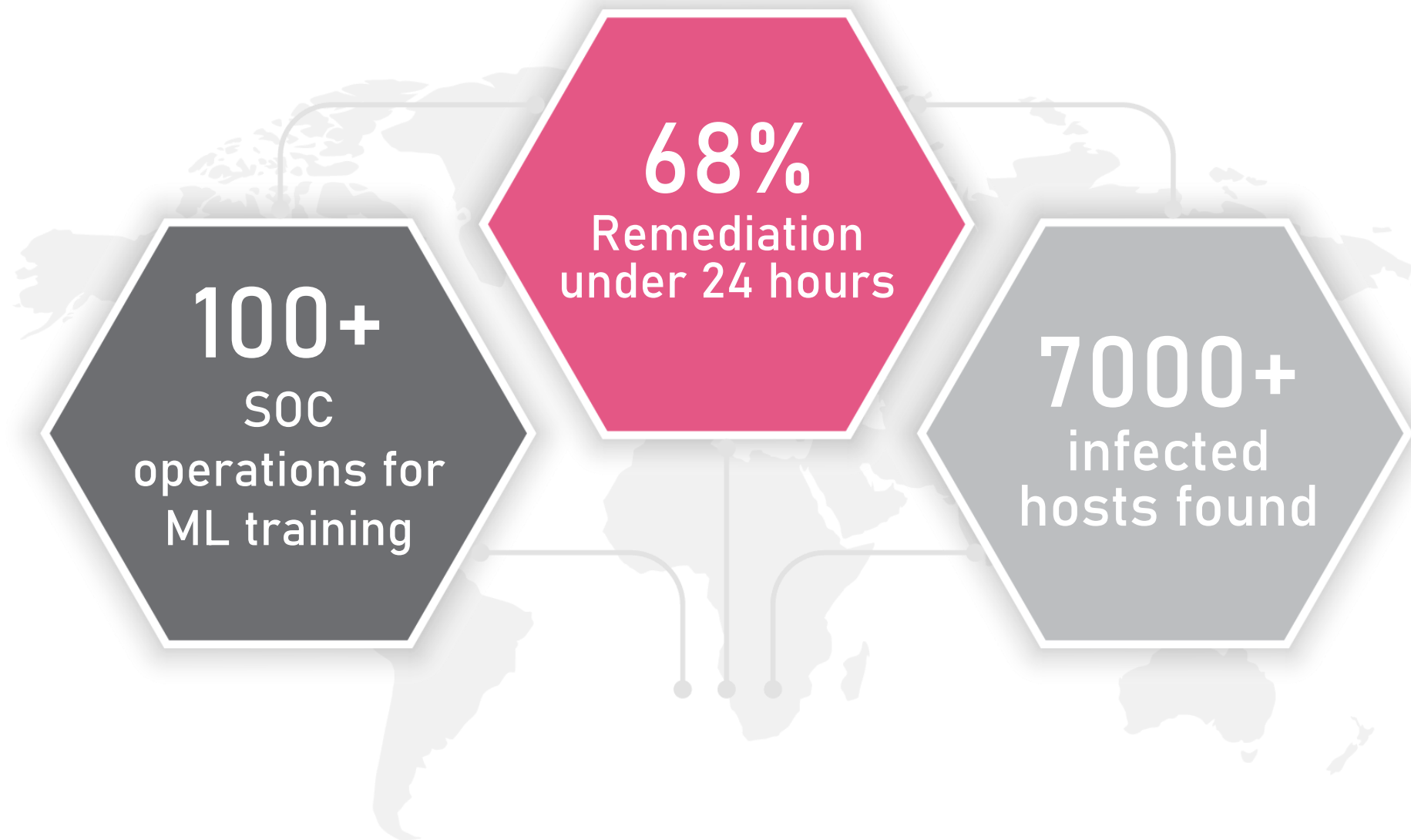


False Positives  
< 1%



**Expose**  
hidden attacks







# Harnessing AI for big data analysis

## 1. LEARN



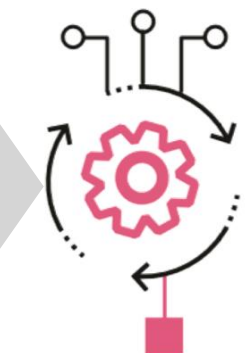
THREATCLOUD  
millions of events

events from  
**benign** hosts

events from  
**infected** hosts



Learn  
event patterns



AI model

Connection rate  
Connection time  
Repetitive connections  
Number of sessions  
Volume of data sent

...



# Harnessing AI for big data analysis

## 1. LEARN

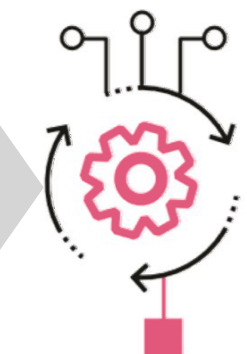


events from  
**benign** hosts

events from  
**infected** hosts



**Learn**  
event patterns



AI model

## 2. EXPOSE

Customer  
events



**Expose**  
hidden attacks



# Accurately exposing stealth attacks





# Accurately exposing stealth attacks



- Infected hosts
- Compromised cloud assets
- DNS tunneling
- APTs
- Targeted campaigns

False Positives < 1%



<p><b>1</b> 📶</p> <p>Inspected Gateways</p>	<p><b>171</b> 🖥️</p> <p>Hosts been attacked</p>	<p><b>17K</b> 🖥️</p> <p>Malicious activities has been inspected</p>	<p><b>17</b> 🦠</p> <p>Unique Malware Families Seen</p>	<p><b>46</b> 🦠</p> <p>Unique Indicator Of Compromise</p>
---	---	---	--	--

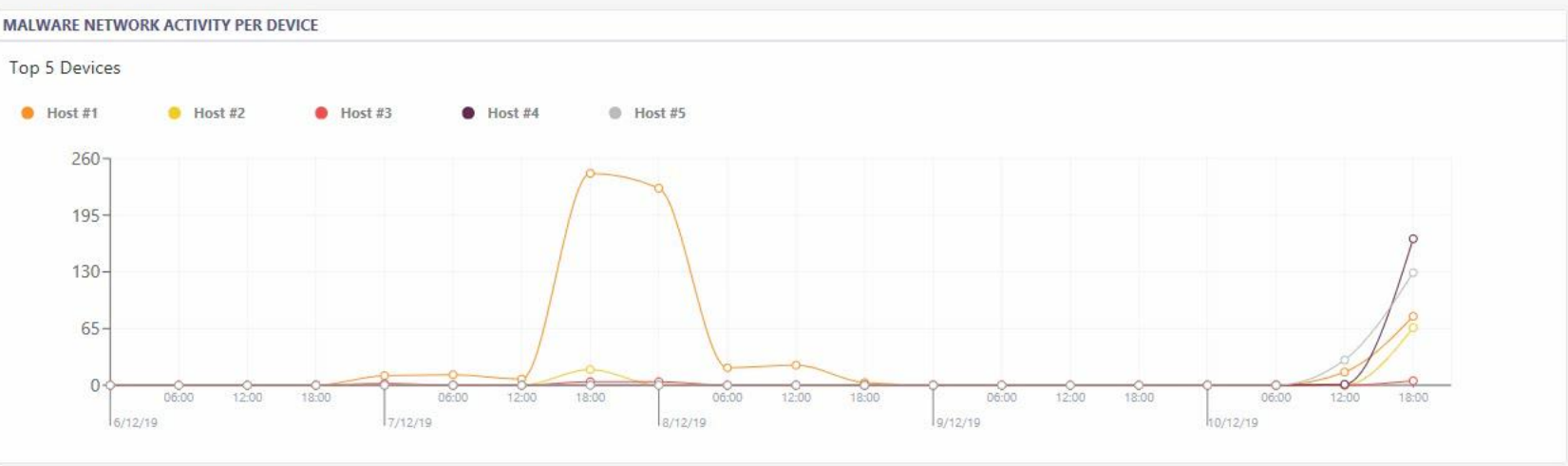
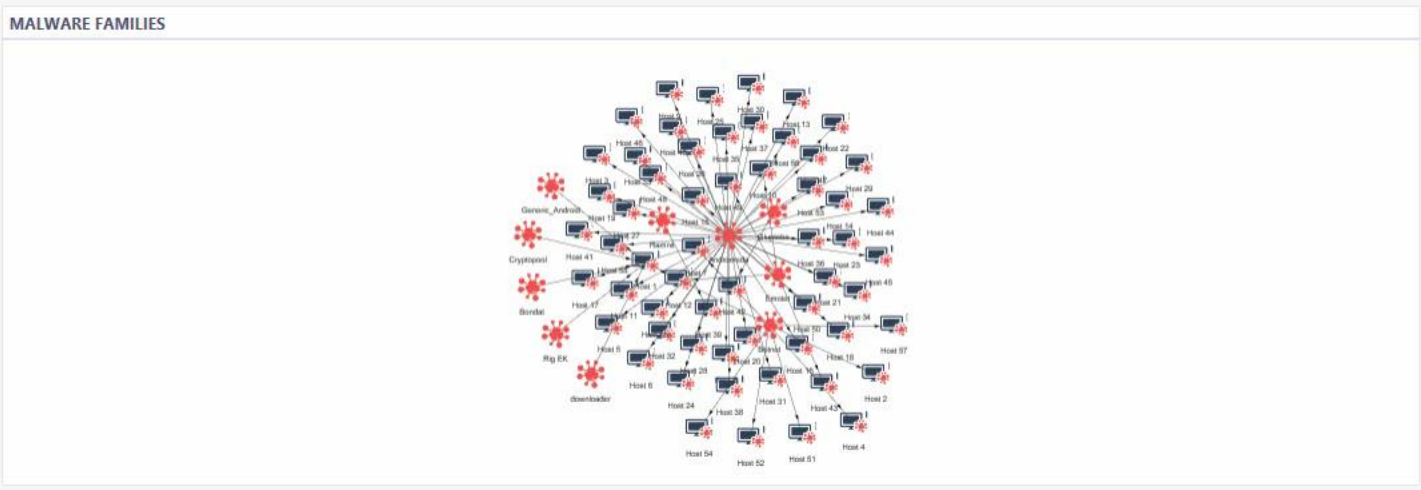
### INFECTED DEVICES

**58** 🖥️🦠

#### INFECTED DEVICES

Top 5 Devices

🖥️ <b>Host 1</b> (0f68b00b190f2c36bfab18757fd3f793)	Generic_Android
🖥️ <b>Host 2</b> (cb774a2cee6b5e9a86365cf774e7be2d)	Andromeda
🖥️ <b>Host 3</b> (1bc53b38ce7e5048fe02296b42b26a31)	Botnet
🖥️ <b>Host 4</b> (e7820ef2b250daf1346a71545403e0b2)	Andromeda
🖥️ <b>Host 5</b> (ac0cc4fa82faab5e54ea123947dccc81)	Andromeda





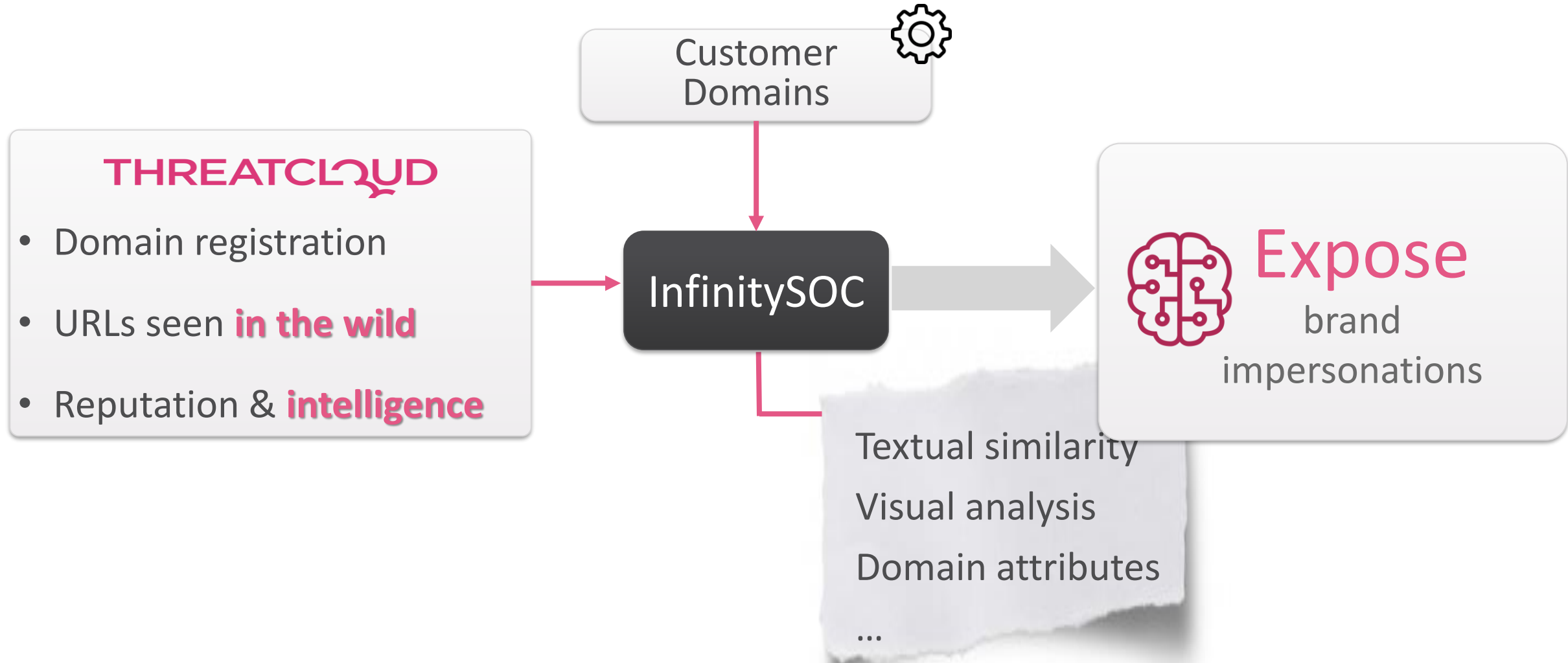
# What if an attack lives outside your network?

Brand  
impersonation

Phishing  
campaigns

Targeting  
customers

# Exposing **brand impersonation** attacks





Check Point<sup>®</sup>  
SOFTWARE TECHNOLOGIES LTD



Expose  
brand  
impersonations



# Expose

brand  
impersonations

- Uncover **real attacks**
- Automated **visual triage**
- Detailed **domain analytics**
- Domain **takedown service**



OVERVIEW

EVENTS

CONFIG

GLOBAL SETTINGS

Last Month Protected Domain Sort By Date


LOOKALIKE WEBSITES 3159

Filter By Severity All Low Medium High Show Live Websites Only

- Tag 23 Dec 2019 http://login-account.paypal.com paypal.com
- Tag 23 Dec 2019 http://paypal.topcarts.c... paypal.com
- Tag 23 Dec 2019 http://paypal.topcarts.c... paypal.com
- Tag 23 Dec 2019 http://paypal.com-updat... paypal.com
- Tag 23 Dec 2019 https://paypalability.co... paypal.com
- Tag 23 Dec 2019 http://paypalability.com paypal.com
- Tag 23 Dec 2019 https://paypalinvestigat... paypal.com
- Tag 23 Dec 2019 http://paypalconcerns.c... paypal.com
- Tag 23 Dec 2019 http://paypalinvestigate... paypal.com
- Tag 23 Dec 2019 http://paypalreversals.c... paypal.com

LOOKALIKE WEBSITES

502 HIGH SEVERITY 977 MEDIUM SEVERITY 1680 LOW SEVERITY

<p>http://login-account.paypal.engelca.com.br/03917</p> <p>Tag</p> <p>Index of /login-account.paypal/03917</p>	<p>http://paypal.topcarts.com/customer_center/customer-idpp0c340/myaccount/signin</p> <p>Tag</p> <p>Not Found</p>	<p>http://paypal.topcarts.com/customer_center/customer-idpp0c349</p> <p>Tag</p> <p>Not Found</p>	<p>https://paypalability.com/en</p> <p>Tag</p> 	<p>http://paypalability.com</p> <p>Tag</p> <p>404 Not Found</p>
<p>http://securepaypalaccount.hopto.org</p> <p>Tag</p> <p>Index of /</p>	<p>http://www.paypalaccounts.hopto.org/portal/secure/paypalaccounts/formation/learn-support/secure-emp</p> <p>Tag</p> <p>404 Not Found</p>	<p>http://kraegerama.de/system/paypal2018/customer_center/customer-idpp0c338</p> <p>Tag</p> <p>Not Found</p>	<p>https://paypal.secure2-limited-uk.com/webapps/login.php</p> <p>Tag</p> <p>404 Not Found</p>	<p>http://update-confirms.universalsignages.com/update-security-account-paypal</p> <p>Tag</p> <p>Not Found</p>
<p>http://paypal-costumers.myvnc.com</p> <p>Tag</p> <p>Not Found</p>	<p>http://paypal-costumers.myvnc.com/signin</p> <p>Tag</p> <p>ERROR</p>	<p>http://rhinocomp.co.uk/en/www.paypal.com</p> <p>Tag</p>	<p>http://paypal.servicecom.byethost8.com/86226900a494e1a15a53632f0f...</p> <p>Tag</p>	



CHECK POINT

# INFINITY SOC<sup>BETA</sup>



Check Point  
SOFTWARE TECHNOLOGIES LTD



Actionable  
Insights

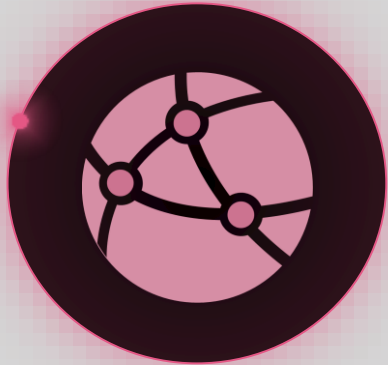
Expose attacks  
**in your network**

Expose attacks  
**outside your network**

## BOOST INVESTIGATION AND RESPONSE



CHECK POINT  
**INFINITY SOC** BETA



Actionable  
Insights



Accelerate  
Investigation



Effective  
Response & Prevention

# BOOST INVESTIGATION AND RESPONSE



# How can you **understand** what you're dealing with?



*The traditional approach...*

Spend **a lot of time**  
on complex manual investigation





# Accelerate investigations with **ThreatCloud**



# Leverage the power of ThreatCloud



# A portal into ThreatCloud

Check Point  
Research  
insights

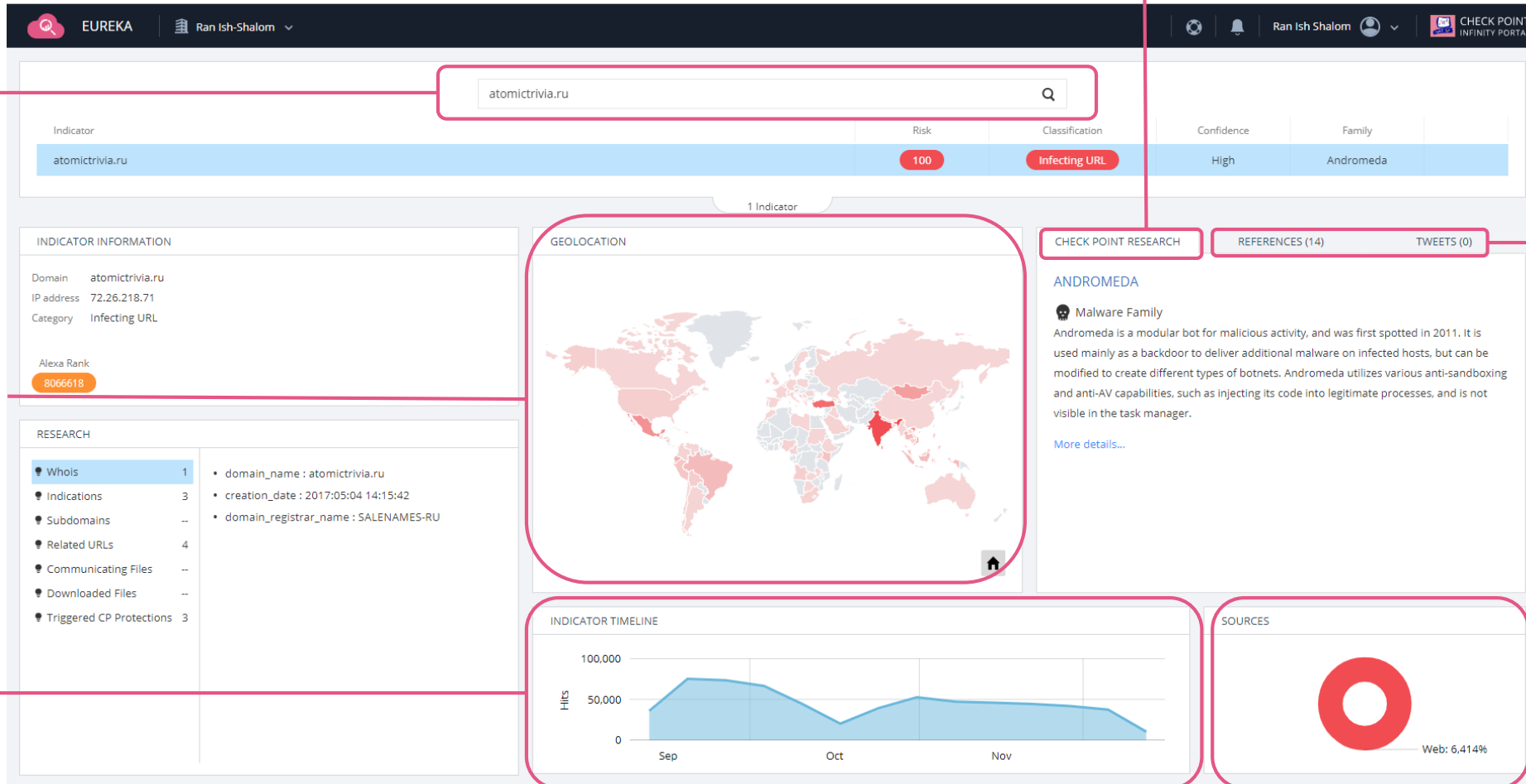
Search for  
any indicator

Geographical  
spread

Activity  
timeline

OSINT

Known  
attack  
surfaces



Search for any indicator: atomicrivia.ru

Indicator	Risk	Classification	Confidence	Family
atomicrivia.ru	100	Infecting URL	High	Andromeda

1 Indicator

**INDICATOR INFORMATION**

Domain: atomicrivia.ru  
IP address: 72.26.218.71  
Category: Infecting URL

Alexa Rank: 8066618

**RESEARCH**

- Whois: 1
- Indications: 3
- Subdomains: --
- Related URLs: 4
- Communicating Files: --
- Downloaded Files: --
- Triggered CP Protections: 3

• domain\_name : atomicrivia.ru  
• creation\_date : 2017:05:04 14:15:42  
• domain\_registrar\_name : SALENAMES-RU

**GEOLOCATION**

World map showing geographical spread of the indicator.

**CHECK POINT RESEARCH**

**ANDROMEDA**

Malware Family

Andromeda is a modular bot for malicious activity, and was first spotted in 2011. It is used mainly as a backdoor to deliver additional malware on infected hosts, but can be modified to create different types of botnets. Andromeda utilizes various anti-sandboxing and anti-AV capabilities, such as injecting its code into legitimate processes, and is not visible in the task manager.

[More details...](#)

**REFERENCES (14)**

**TWEETS (0)**

**INDICATOR TIMELINE**

Line graph showing Hits (0 to 100,000) over time (Sep, Oct, Nov).

**SOURCES**

Donut chart showing Web: 6.414%

Supercharge your investigation with contextualized threat intelligence





Paste here any suspicious URLs and/or Hashes to detect types of malware

Search for any indicators



login.lataminternet.com and 6 more

Indicator	Risk	Classification	Confidence	Family
b8348ffd646688fb47715043e364729c	100	Malware	High	Emotet

7 Indicators

### INDICATOR INFORMATION

MD5: b8348ffd646688fb47715043e364729c  
SHA-1: 983f4aebc84e20642a83ec6027eab5b66893c140  
SHA-256: 1767d73a0602c0c604666467b04824556afb811ec8a5ed9ad8b97cdfff89978d  
Tags: Not available

File Type	Size	First Seen	Last Seen	Virus Total
DOC	251 KB	Not available	Not available	Not available

### RESEARCH

Category	Count	Details
File Names	5	• *****.doc
Network activity	8	• 1767*73*0602*0*604666467*04824556***811**8*5* *9**g*97****89978*.doc
Execution parents	--	• ***** 2299188521 18 10 2019.doc
Archive parents	--	• PO95593369281936433.doc
Source URLs	--	• *** 713-4856415.doc
Email Subjects	4	



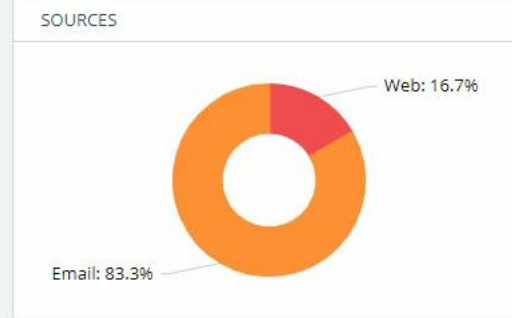
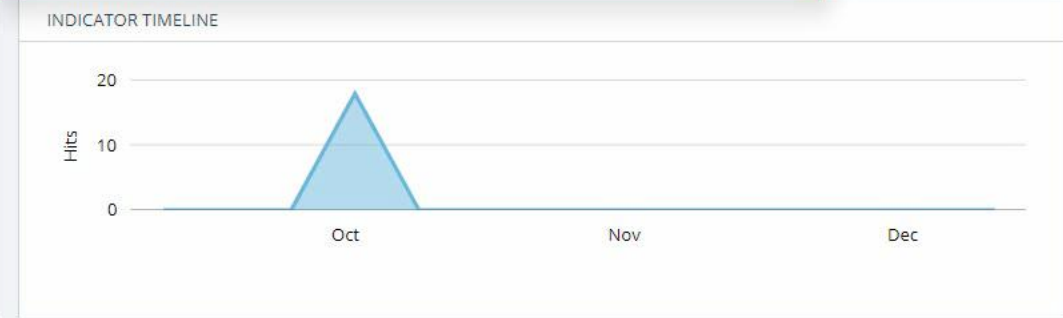
### EMOTET

Malware Family

Emotet is an advanced, self-propagating and modular Trojan that used to operate as a banking Trojan, and more recently is used as a distributor of other malware, most notably the Ryuk ransomware. Emotet uses multiple methods and evasion techniques for maintaining persistence and avoiding detection. Emotet can self-propagate, spreading itself through various channels, such as malicious attachments.

More details...

Geo information from ThreatCloud





login.lataminternet.com and 6 more

Indicator	Risk	Classification	Confidence	Family
differentia.ru	100	CnC Server	High	Andromeda

7 Indicators

### INDICATOR INFORMATION

Type: Domain  
 Domain: differentia.ru  
 IP address: 35.229.93.46  
 Category: CnC Server

Virus Total: 9 / 71  
 Alexa Rank: 3679306




### CHECK POINT RESEARCH

REFERENCES (16) TWEETS (2) GOOGLE (10)

#### ANDROMEDA

**Malware Family**

Andromeda is a modular bot for malicious activity, and was first spotted in 2011. It is used mainly as a backdoor to deliver additional malware on infected hosts, but can be modified to create different types of botnets. Andromeda utilizes various anti-sandboxing and anti-AV capabilities, such as injecting its code into legitimate processes, and is not visible in the task manager.

[More details...](#)

### RESEARCH

- Whois: 1
- Indications: 4
- Subdomains: 6
- Related URLs: 6
- Communicating Files: --
- Downloaded Files: --
- Triggered CP Protections: 3

**6 Malicious**

- differentia.ru/notfound.php
- differentia.ru/favicon.ico
- differentia.ru/index.html
- differentia.ru/diff.php
- differentia.ru
- differentia.ru/my.policy







# Analysts access Threat Emulation reports from InfinitySOC

**Urgent PO Septemer.pdf.exe**  
 Size: 1.33 MB | Type: EXE | Hash: ...

Verdict: Malicious | Action: Prevent | Confidence: High | Secure / Risk: Critical | Classification: Trojan

ATTACK VECTOR | 15/09/2019 15:45

From: attack@\*\*\*\*\*.com | Subject: undefined | To: customer@\*\*\*\*\*.com

**MALWARE FAMILY**

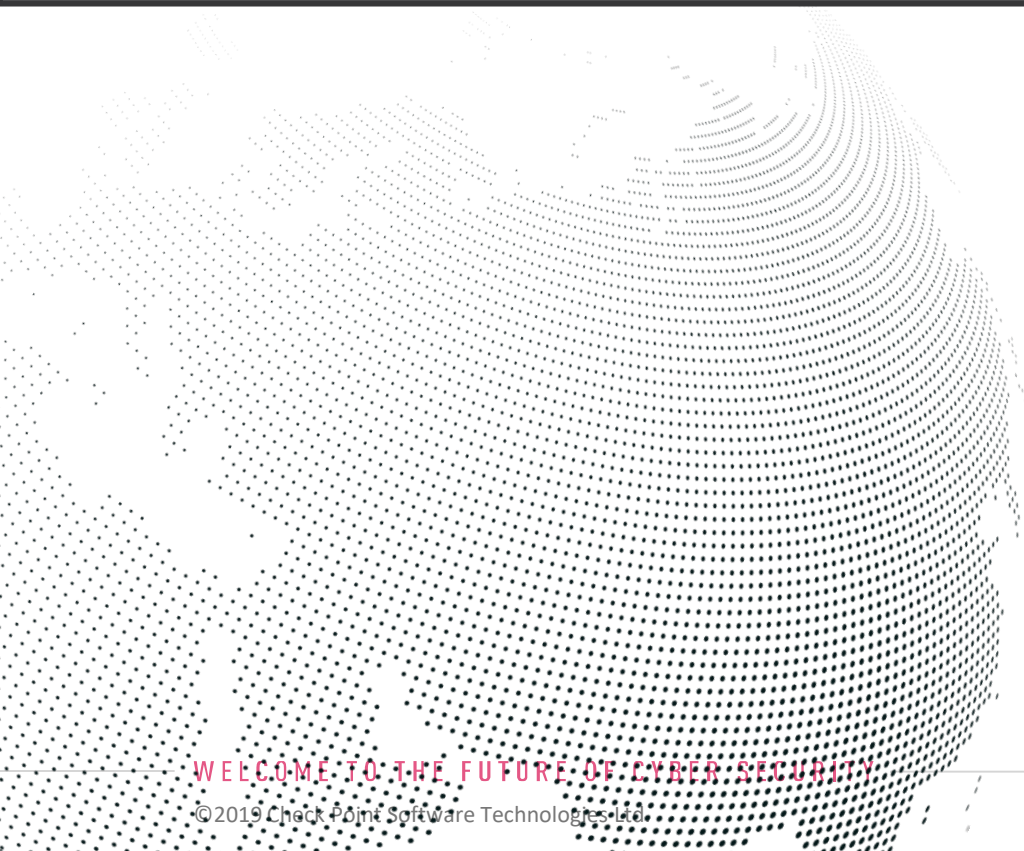
**AgentTesla**  
 AgentTesla is an advanced RAT which functions as a keylogger and password stealer and has been active since 2014. AgentTesla can monitor and collect the victim's keyboard input, system clipboard, and can record screenshots and software vulnerabilities. [Read more on Check Point Threatlog Intelligence Similarity Analysis](#)

**MITRE ATT&CK**

INITIAL ACCESS	EXECUTION	PERSISTENCE	PRIVILEGE ESCALATION	DEFENSE EVASION	CREDENTIAL ACCESS	DISCOVERY	LATERAL MOVEMENT	COLLECTION	EXFILTRATION & C2
	WMI	WMI Event Subscription		Disabling Security Tools	Credentials in Files	Security Software Discovery		Email Collection	
	Execution Through APIs	Registry Run Keys		Trusted Developer Utilities		Application Window Discovery		Data from Local System	
	Trusted Developer Utilities			Software Packing				Clipboard Data	
				File Deletion					



# Accelerate investigation with automated **endpoint forensics**





# AUTOMATED FORENSICS ANALYSIS

**ACTIONABLE  
INFORMATION**

**Interactive  
Attack Summary**

Instant visibility to  
what you need to  
know

**GENERATED  
AUTOMATICALLY**

**Triggered  
for All Events**

Avoids expensive  
manual analysis of  
raw forensic data





The image displays two overlapping screenshots of the SandBlast Forensics interface. The left screenshot shows a 'TREE VIEW' of processes, including 'ryuk.exe 1036' (Attack Start, Process Injection, Man in the Browser, Unsigned Process, User Execution...), 'net.exe 5928' (Dangerous Execution, Service Stop, Execution through API), 'net.exe 7120' (Dangerous Execution, Service Stop, Execution through API), 'cmd.exe 8588' (Execution through API, Command-Line Interface, Scripting), and 'cmd.exe 3180' (Execution through API, Command-Line Interface). The right screenshot shows a dashboard with 'ATTACK STATS' (ACTIVE status, Ryuk malware family, HIGH severity, Endpoint Behavioral Guard triggered by), 'ATTACK TYPES' (bot, infostealer, ransomware, trojan), 'ENTRY POINT' (Remote Logon Internal), 'BUSINESS IMPACT' (6 Credential Theft, 35 Data Changes, 1 Malicious Processes), and 'REMEDiation' (98% terminated processes). A 'HELP?' button is visible in the bottom left of the right screenshot.

# Endpoint Forensics demo



OVERVIEW



POLICY



COMPUTER MANAGEMENT



LOGS



PUSH OPERATIONS



ENDPOINT SETTINGS



THREAT HUNTING



GLOBAL SETTINGS

Last Week

Process Name IS powershell.exe

Parent Process Name IS winword.exe

Network Dest IP EXISTS



16 RESULTS FOUND



DETAILS

Parent Process MD5  
15e52f52ed2b8ed122fae897119687c4

Process Classification  
Benign

Network Dest IP  
81.171.3.211

Network Src IP  
10.0.0.115

Network URL  
http://myagentco.com/new/vkn/

URLClassification  
CnC Server

First Seen  
01/07/2020 1:20:08 PM

#	Machine Name	User Name	Process Name	ProcessMD5	Process Classification	Process
1	COKO-WIN10X64-2	dave	powershell.exe	65d86c34814c02569e...	Benign	
2	COKO-WIN10X64-2	dave	powershell.exe	65d86c34814c02569e...	Benign	
3	COKO-WIN10X64	dave	powershell.exe	65d86c34814c02569e...	Benign	
4	COKO-WIN10X64	dave	powershell.exe	65d86c34814c02569e...	Benign	
5	ANDY-WIN10	andy	powershell.exe	65d86c34814c02569e...	Benign	

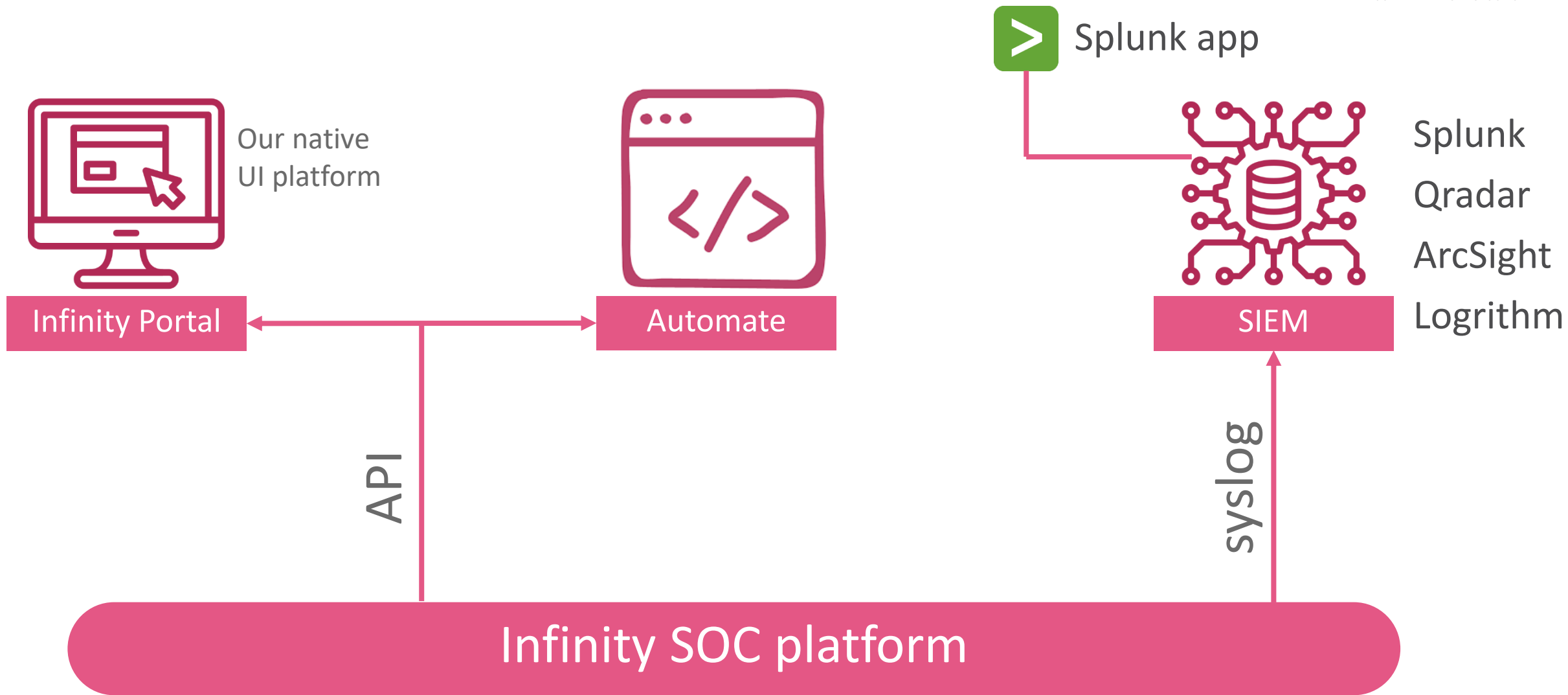




# Accelerate investigations within your **SIEM**



# We support your environment





# Accelerate investigation with InfinitySOC Splunk app



Check Point  
SOFTWARE TECHNOLOGIES LTD

Distill  
critical  
events

Threat  
Emulation  
reports

MITRE  
Att&ck  
analysis

## OPTIMIZED FOR SOC ANALYSTS

Apps

Search & Reporting

Check Point App for Splunk

+ Find More Apps

### Explore Splunk Enterprise



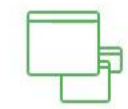
#### Product Tours

New to Splunk? Take a tour to help you on your way.



#### Add Data

Add or forward data to Splunk Enterprise. Afterwards, you may extract fields.



#### Splunk Apps [↗](#)

Apps and add-ons extend the capabilities of Splunk Enterprise.



#### Splunk Docs [↗](#)

Comprehensive documentation for Splunk Enterprise and for all other Splunk products.

Close

Choose a home dashboard

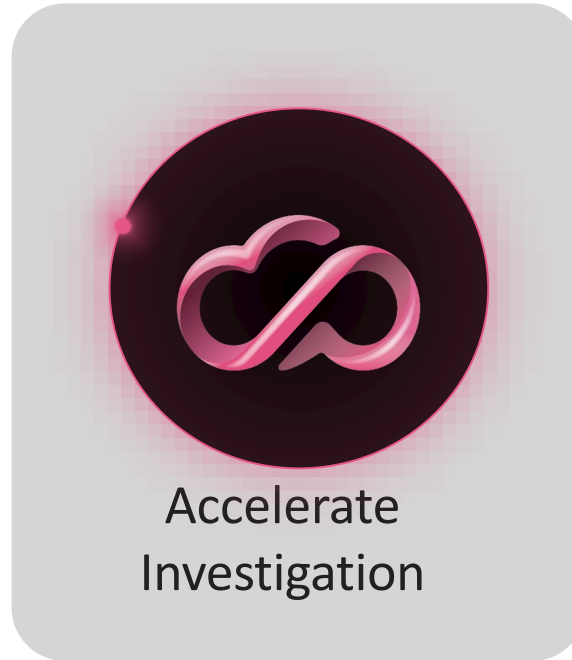


CHECK POINT

# INFINITY SOC<sup>BETA</sup>



Check Point  
SOFTWARE TECHNOLOGIES LTD



- ThreatCloud investigation
- Automated forensic analysis
- Threat hunting
- SIEM integration

## BOOST INVESTIGATION AND RESPONSE



CHECK POINT  
**INFINITY SOC** BETA



Actionable  
Insights



Accelerate  
Investigation



Effective  
Response & Prevention

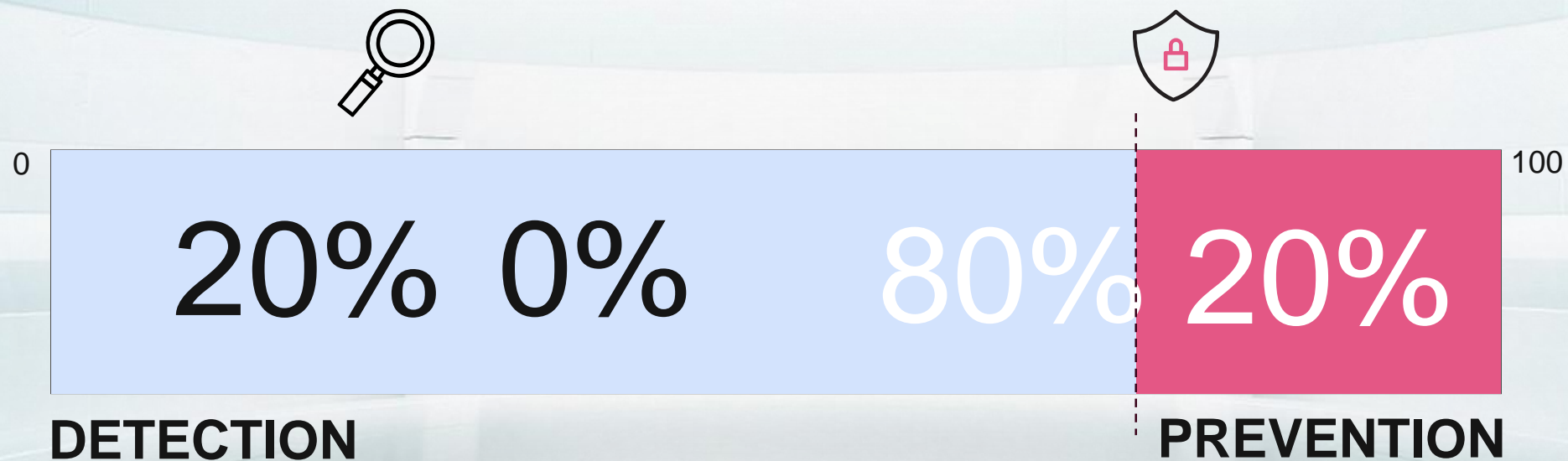
# BOOST INVESTIGATION AND RESPONSE



# SOC Containment & Remediation

AUTOMATE

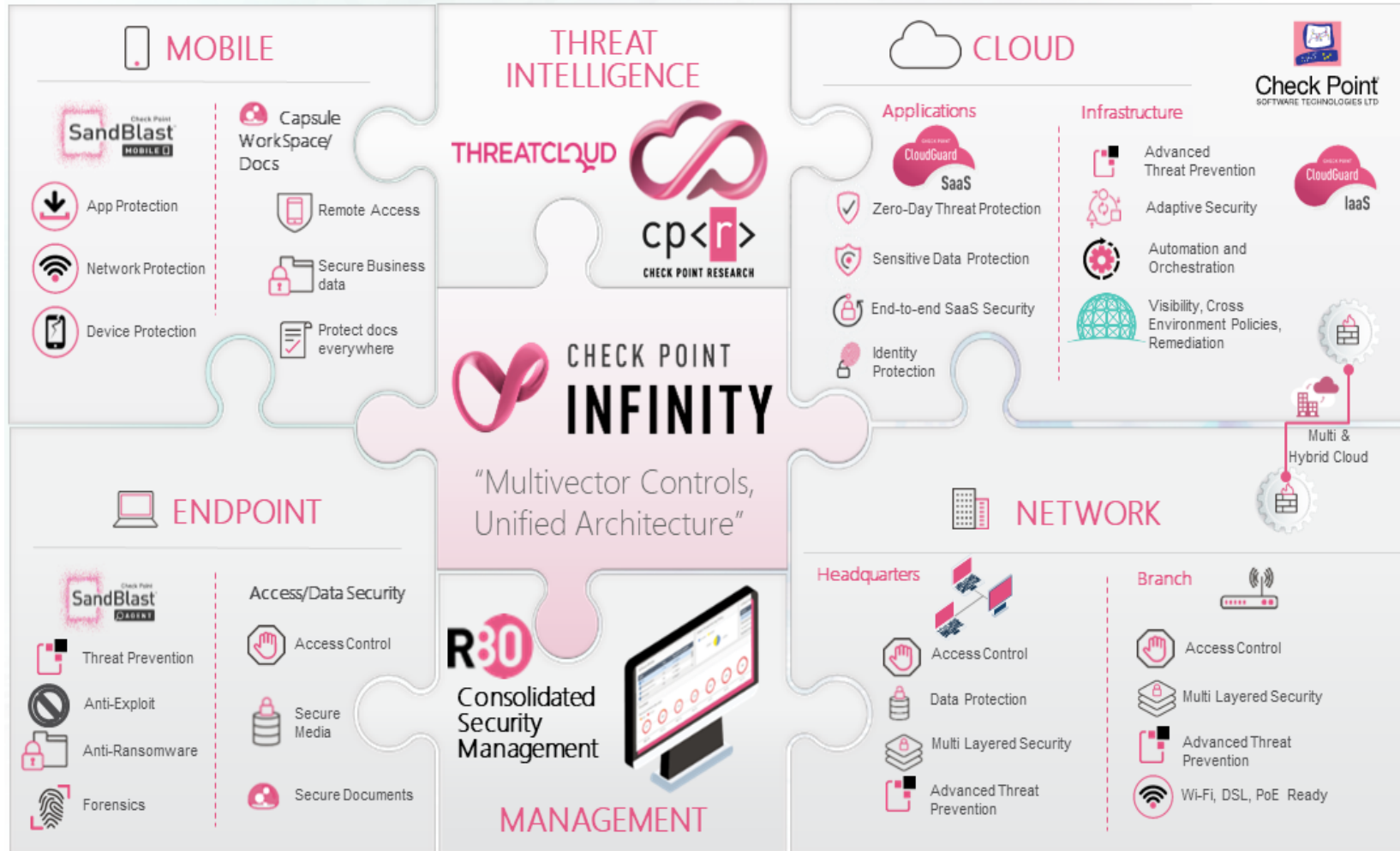
	Network & Cloud Security	Endpoint Security
<b>Isolate</b> infected hosts	✓	✓
<b>Contain:</b> Prevent C&C communications	✓	✓
<b>Contain:</b> Prevent lateral movement	✓	✓
<b>Recover</b> from ransomware		✓
<b>Remediate</b> infections		✓



# PREVENTION FIRST



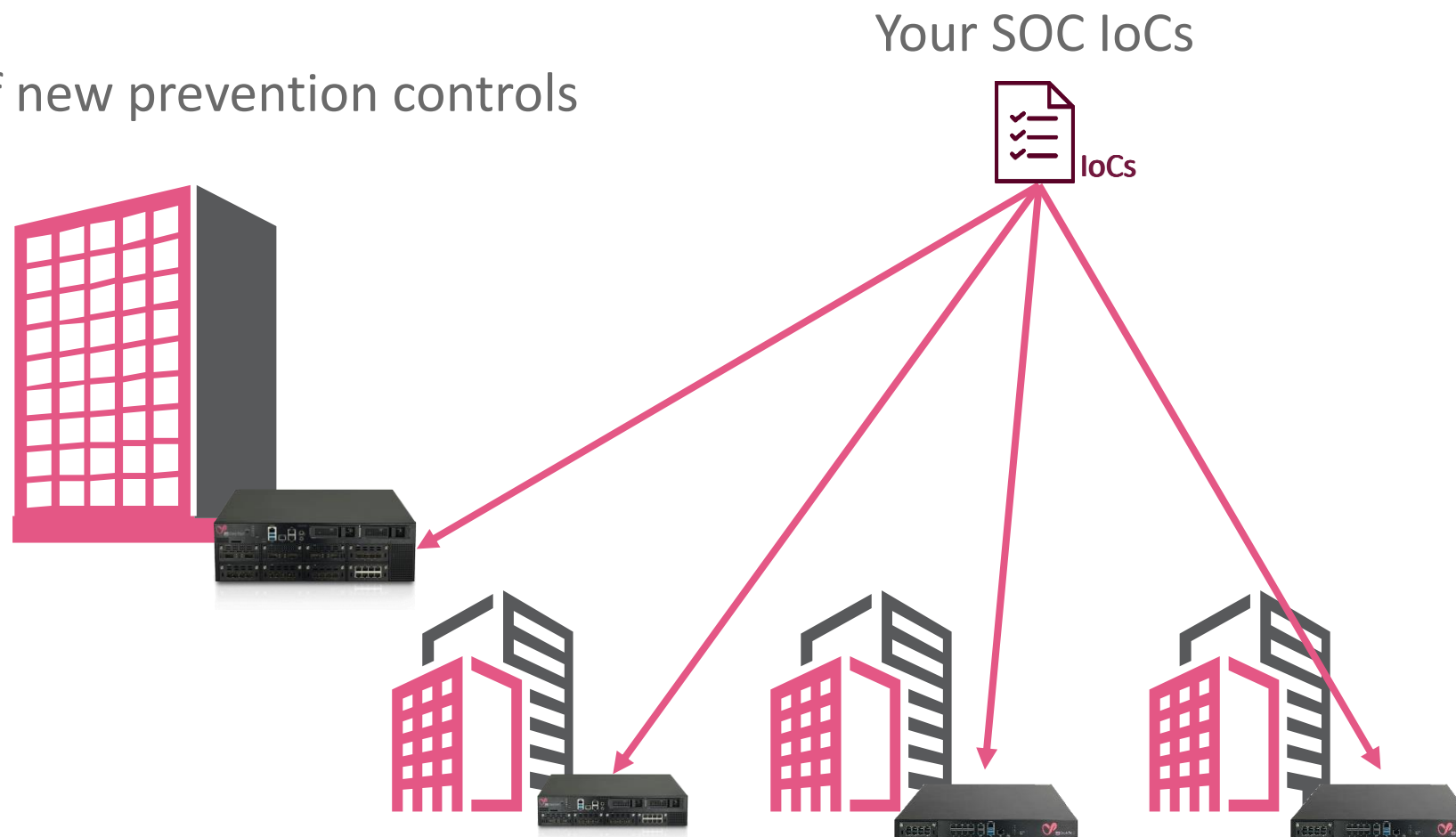
# Best Security starts with Best In Class Prevention



# IoC Enforcement

Simple indicator **dissemination** across organization

**Enforcement** of new prevention controls



LET'S SUMMARIZE





CHECK POINT

**INFINITY SOC**<sup>BETA</sup>

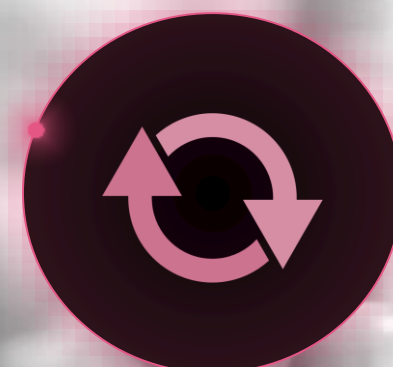
## BOOST INVESTIGATION AND RESPONSE



Actionable  
Insights



Accelerate  
Investigation



Effective  
Response & Prevention

**Join Infinity SOC EA**

[InfinitySoc@checkpoint.com](mailto:InfinitySoc@checkpoint.com)





CHECK POINT

**INFINITY SOC** <sup>BETA</sup>

SUPERCHARGE YOUR SECURITY OPERATIONS

