Changing the Game of Security Operations

How to beat the adversaries
(or at least try with a different approach).

November 8, 2021

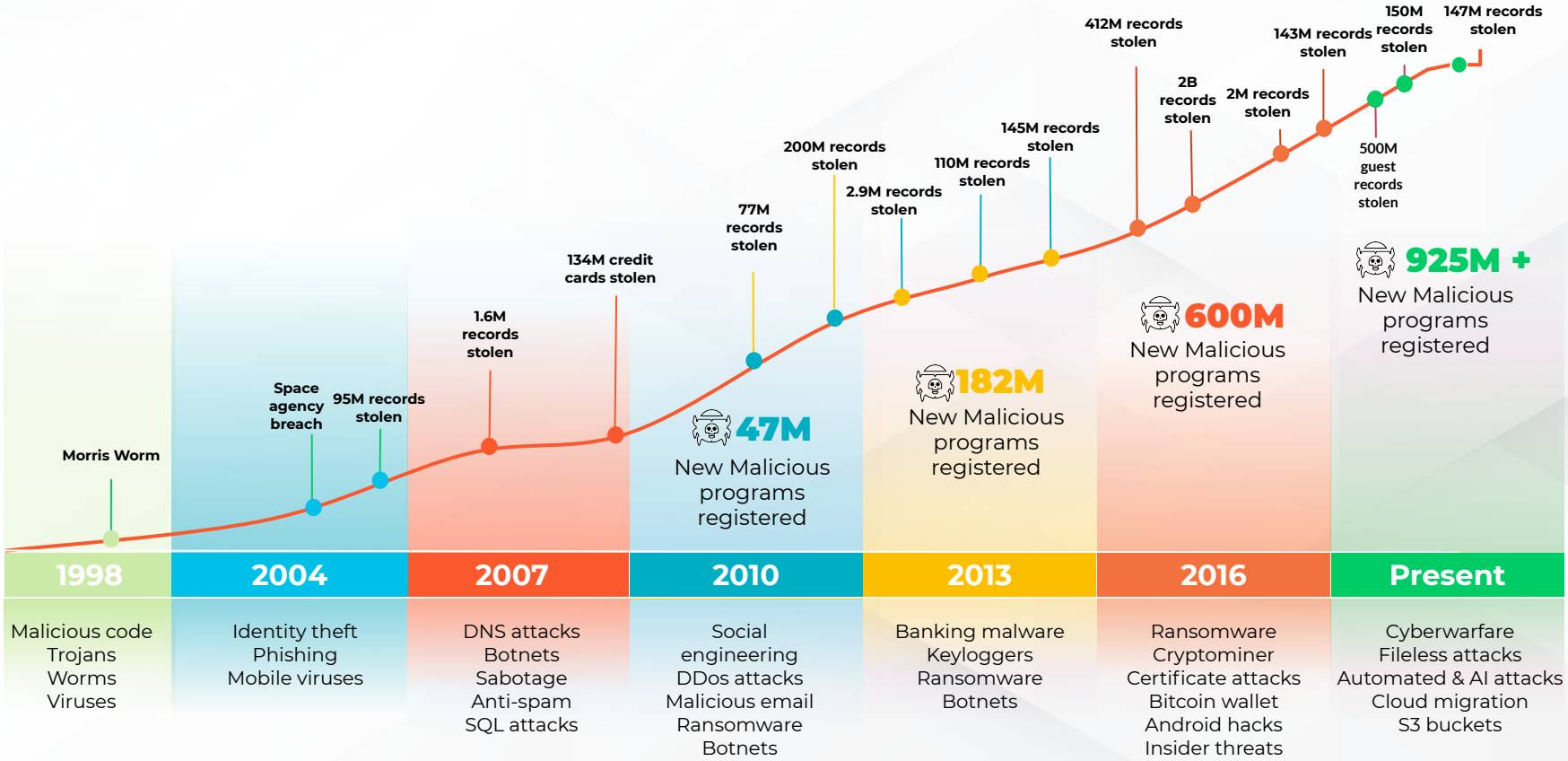
Sylvain Meras | Cortex Systems Engineer

paloalto® NETWORKS | Cybersecurity Partner of Choice

Threat Landscape

Observations made and shared by our Unit 42 Threat Researchers.

As threats escalate, SecOps is more important than ever



Ransomware Key Trends

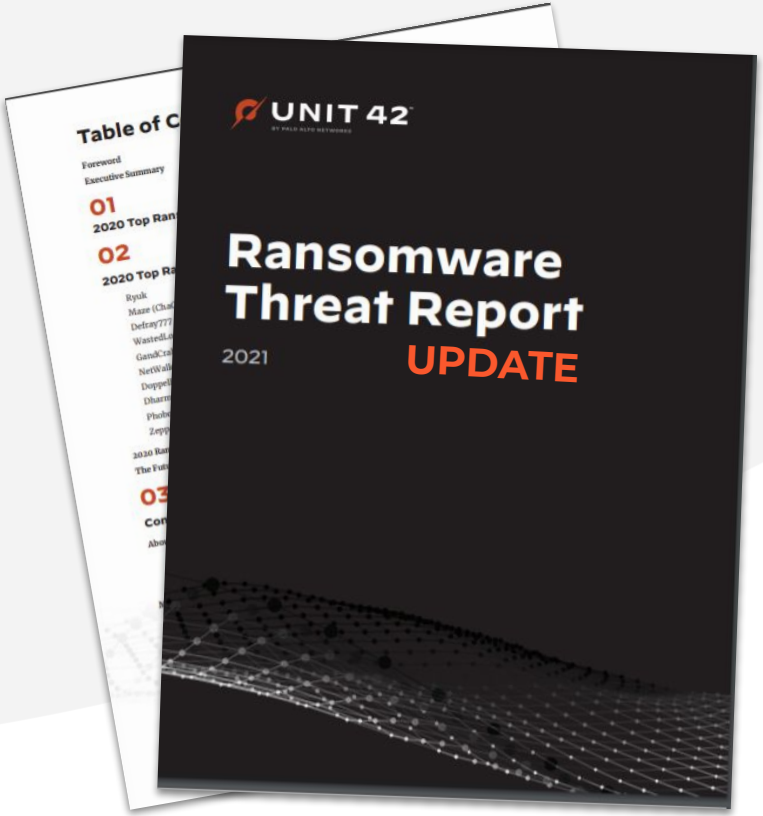
$5.3M average ransom demand in 1H21
up 518% from previous year

$570K average ransom paid in 2021
up 82% from previous year

$2M highest ransom paid in 2021

$50M highest ransom demand in 2021

Quadruple Extortion on the Rise



* Source: Unit 42 2021 Ransomware Threat Report

Key Insights Observed by Unit 42

Top targeted industries: Healthcare and Financial Services.
60% off all incidents we investigated.

Trendy Hacking Methods since 2019.
Ransomware attacks and Business Email Compromises (BEC).

The dark horse cyber risk: Insider threats.
+70% year over year. 57% of attacks were caused by employees leaving the company.

Great plans still fail.
Attackers capitalizing on organizations' inadvertent disclosure of data.
+ 45% of our inadvertent disclosure investigations involved sensitive data.

As long as there are ways to profit from cybercrime, threat actors will continue to find new methods to exploit vulnerable systems and processes.

* Source: Unit 42 2020 Incident Response & Data Breach Report

The pandemic has accelerated and increased the enterprise attack surface. Digital transformation is ~~coming~~ here. IT/OT convergence is ~~coming~~ here.

Hybrid work is here to stay

Users working from anywhere, anytime and across any devices and apps.

Shift to cloud is accelerating

Increasingly operating in hybrid, multi-cloud estates.

The distance between OT and IT has grown slimmer and slimmer.

OT and IT are converging and becoming increasingly the same.

Attackers are taking advantage of this larger attack surface

Rise of Nation State Attacks

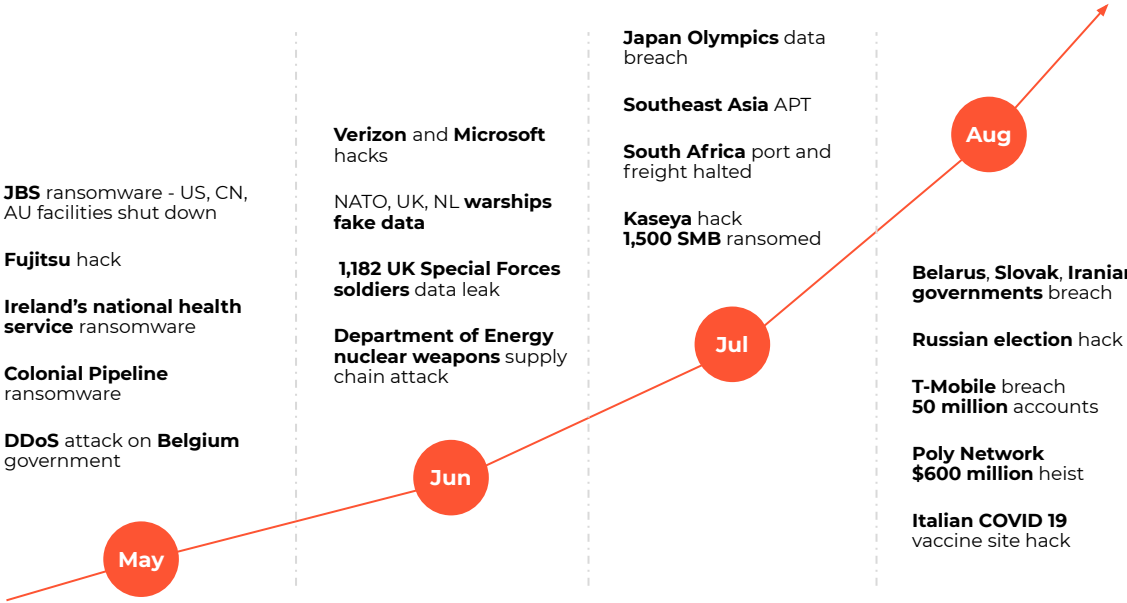
10+

Publicly attributed cyber attacks per month
In 2021

100%

Increase in Nation State cyber incidents
Since 2019

Significant cyber incidents



Sources: CSIS Significant Cyber Incidents; Nation States, Sep 2021; Cyberconflict and the web of Profit, by Dr Michael McGuire, Apr 2021

For more information please visit our Unit 42 website.

https://www.paloaltonetworks.com/unit42

Reinventing Security Operations

Building the Flywheel for the SOC.

Security Operations: The SOC's goal is to detect and respond to ALL threats

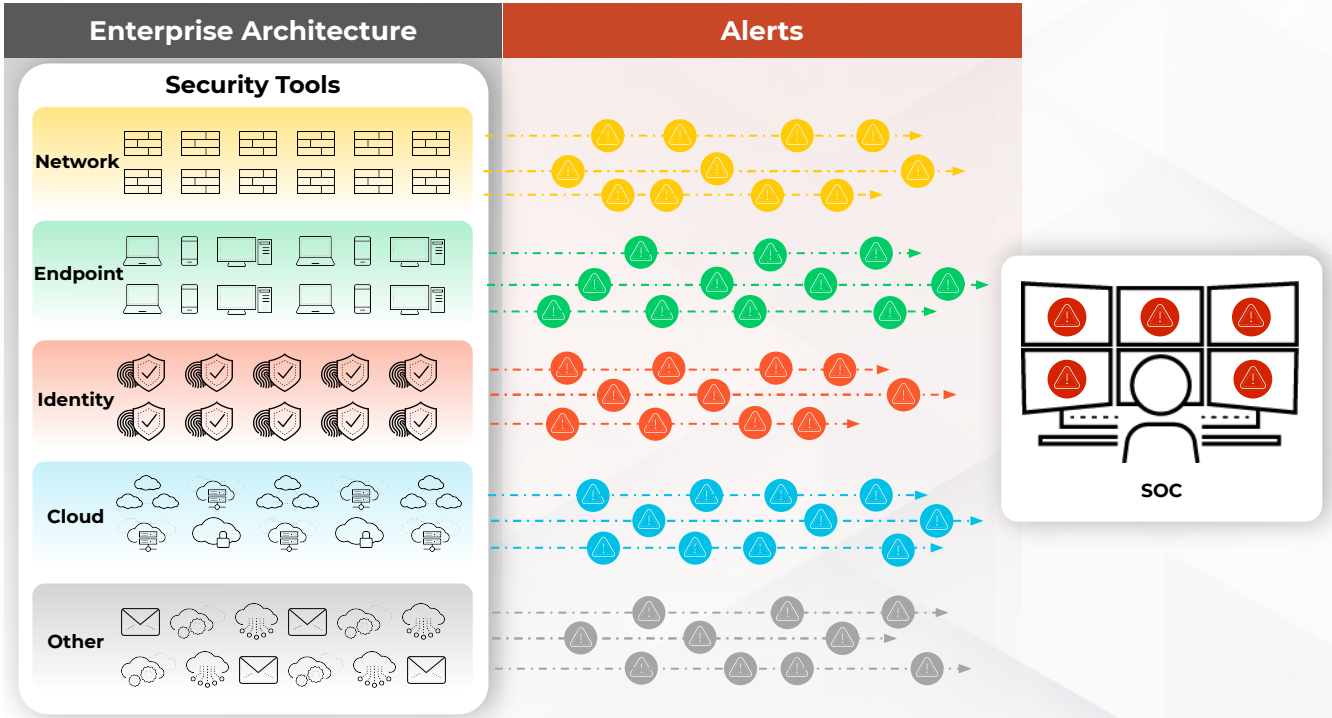
Alert prioritization

Investigation & response

Threat hunting

 |

Security Operations: Increasing volume of alerts is overwhelming most SOCs



TYPICAL INDUSTRY NUMBERS

~11K

Alerts / day; only 17% touched by automation

4+

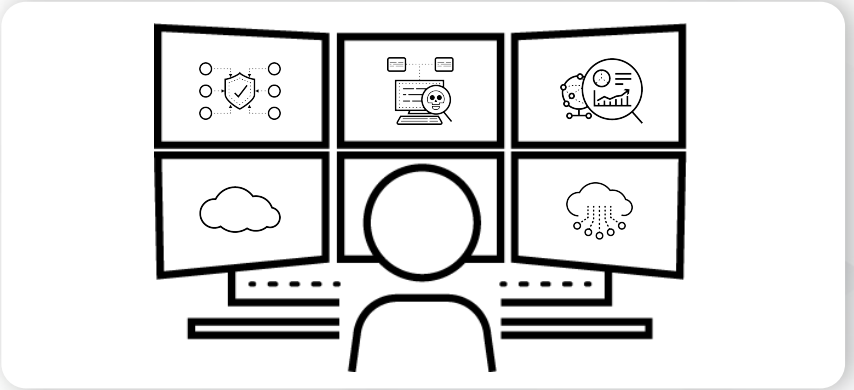
Days to investigate

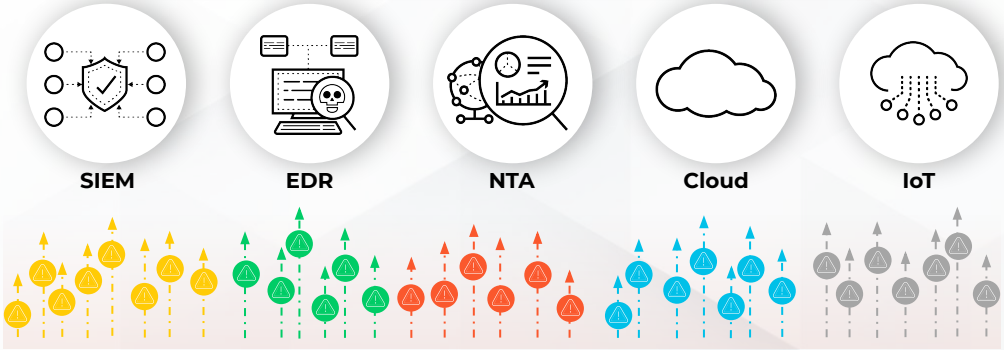
28%

Alerts ignored

Source: Forrester (The 2020 State of Security Operations), Demisto (The State of SOAR Report, 2018)

Security operations: “Single data source” approach is not solving the problem





TYPICAL INDUSTRY NUMBERS

~75

Security products to monitor assets

<30%

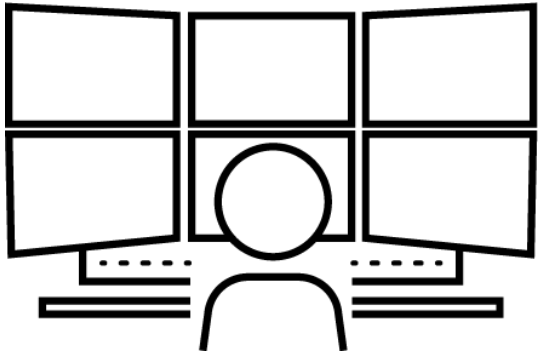
of SOC teams meet their KPI goals

287

Avg days to identify and contain a data breach

Source: CSO Online, Forrester (The 2020 State of Security Operations), IBM Security (Cost of a Data Breach Report 2021)

Our Approach: Providing the SOC with complete visibility, advanced AI/ML analytics and end-to-end automation



Attack Surface Management

eXtended
Prevention
Detection
Investigation
Response

Orchestration
Automation
Case Mgmt.
Threat Intell.
Mgmt.

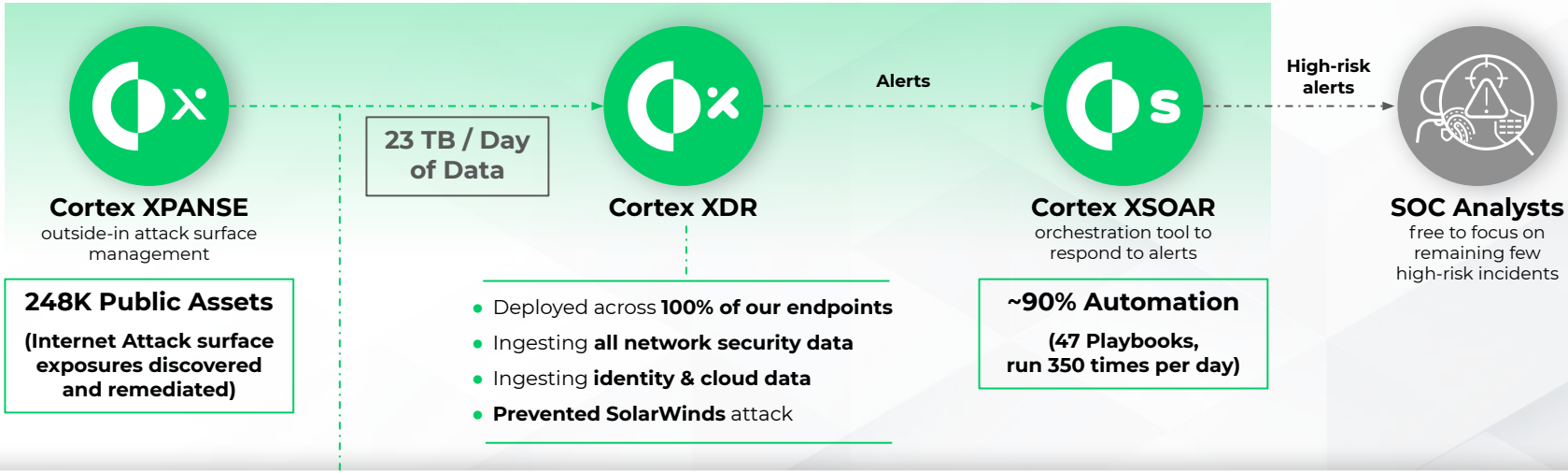
OUR GOALS

100%
Of attack surface is visible and analyzed

100%
Of attacks identified and stopped

Minutes
To respond to threats, not days

Palo Alto Networks SOC: Eating our own dog food

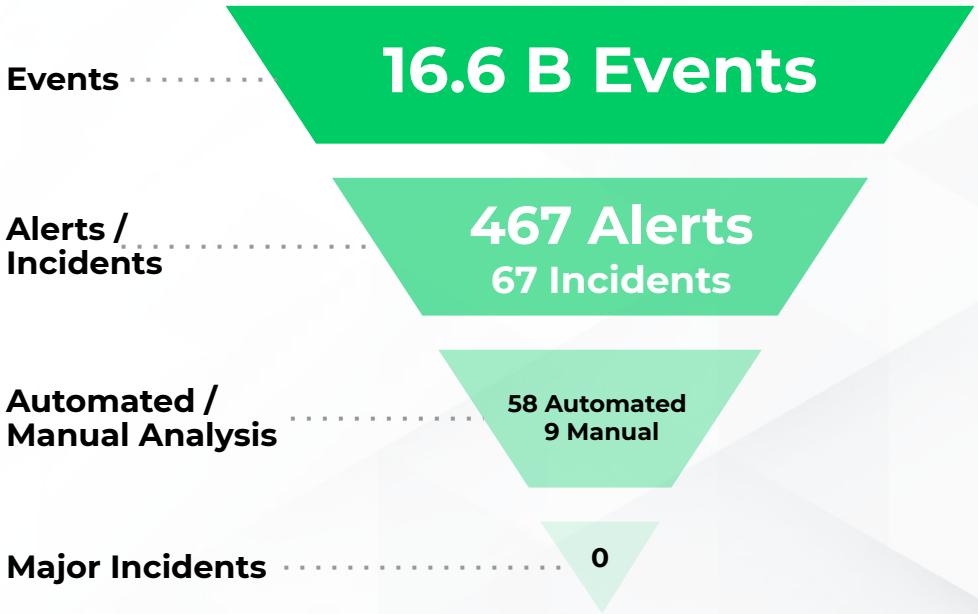


Comprehensive security

Network	Endpoint	Cloud
Prisma Access; NGFWs, VMs, and Security Services	Cortex XDR	Prisma SaaS; Prisma Cloud; Data Security
10K Employees	50K Endpoints	4.3 Million Cloud Assets

Palo Alto Networks SOC: Industry-leading 1 min response time

DAY IN THE LIFE OF THE PALO ALTO NETWORKS SOC



10
SECONDS

Mean Time to Detect

1
MINUTE

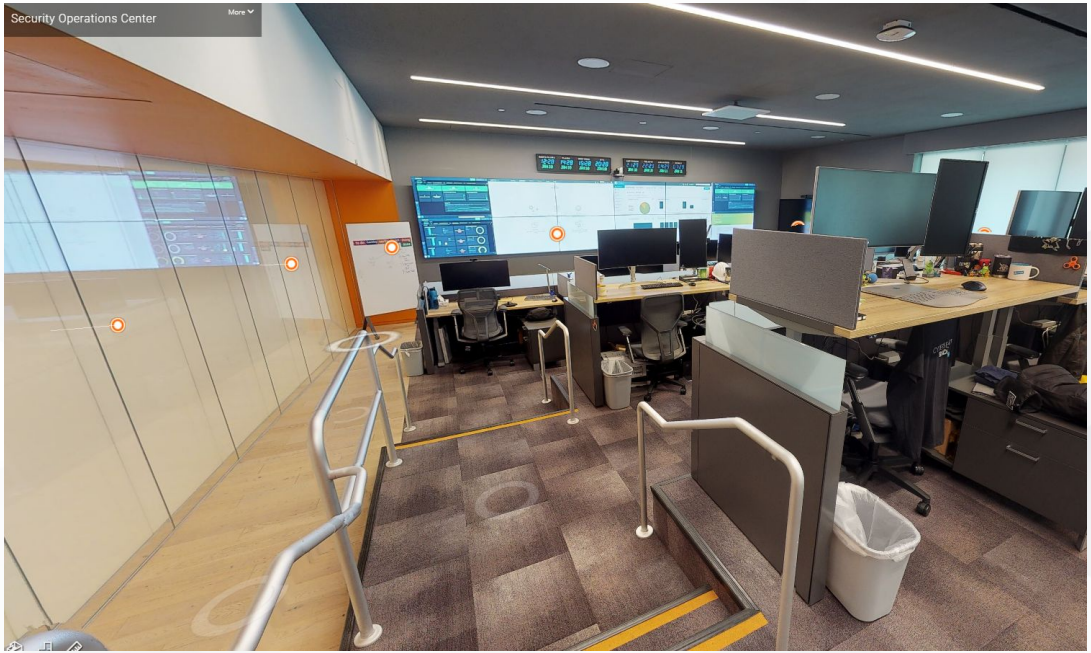
Mean Time to Respond
(High priority alerts)

Palo Alto Networks SOC: Take a virtual walkthrough tour of our SOC

- Matterport virtual walkthrough
- Externally accessible
- Select the orange dots for embedded videos of highlights from the team

https://my.matterport.com/show/?m=q3s3ktjhjC9

Or contact me to organize a live session with Matthew Mellen, our SOC Director.



 |

Threat Intelligence Management

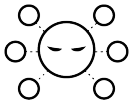
How to do clever things with smart data gathered about the adversaries.

 |

Current Threat Intelligence Platforms are an Incomplete Puzzle

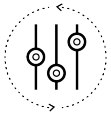
What is possible?

Static IOC scoring

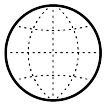


External intel aggregation

What is missing?



User-driven automation



Real-world context

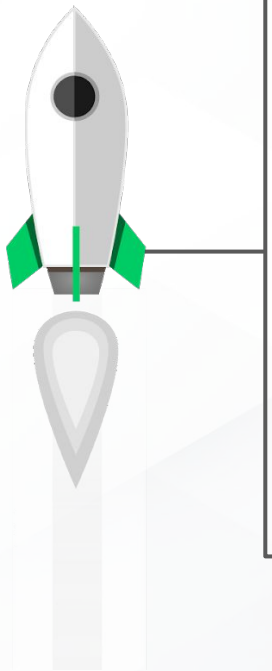
Why does it matter?

Gain confidence

Smarter incident response

Threat Intel Management Basic Concepts

Supercharged threat intelligence management

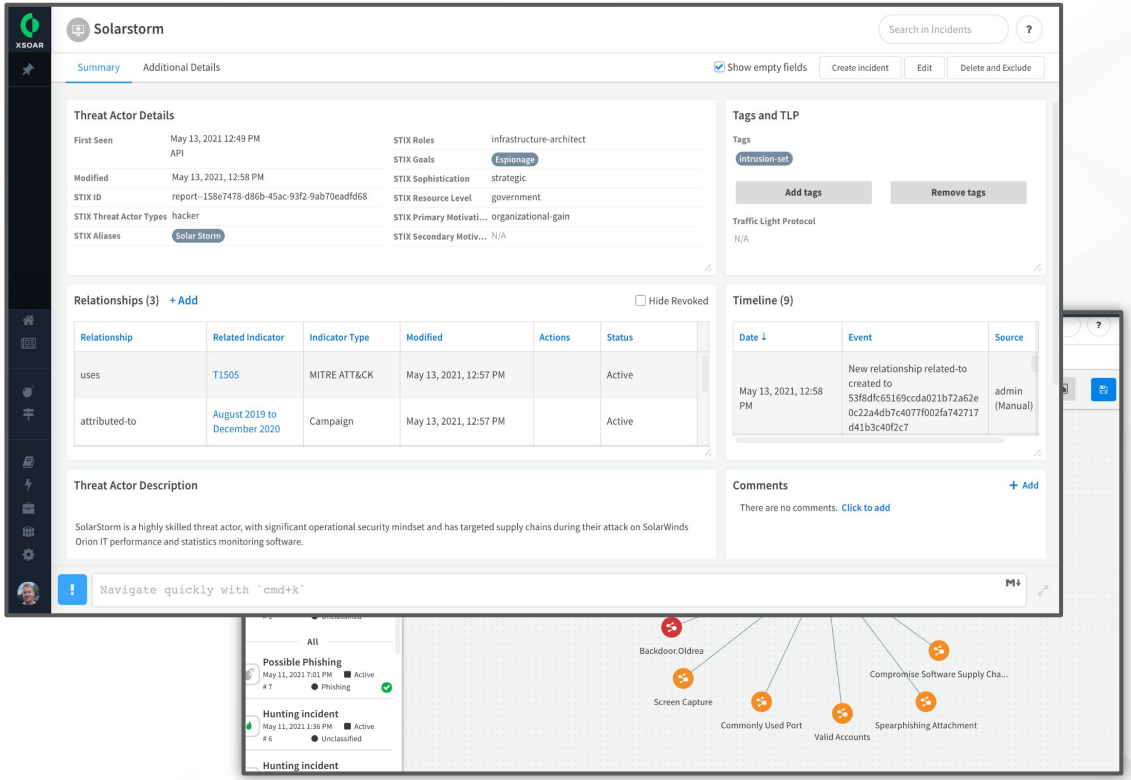


Centralized Threat Intel Library

Manage the Full Intelligence Lifecycle

Automate & Operationalize

Centralized Threat Intel Library



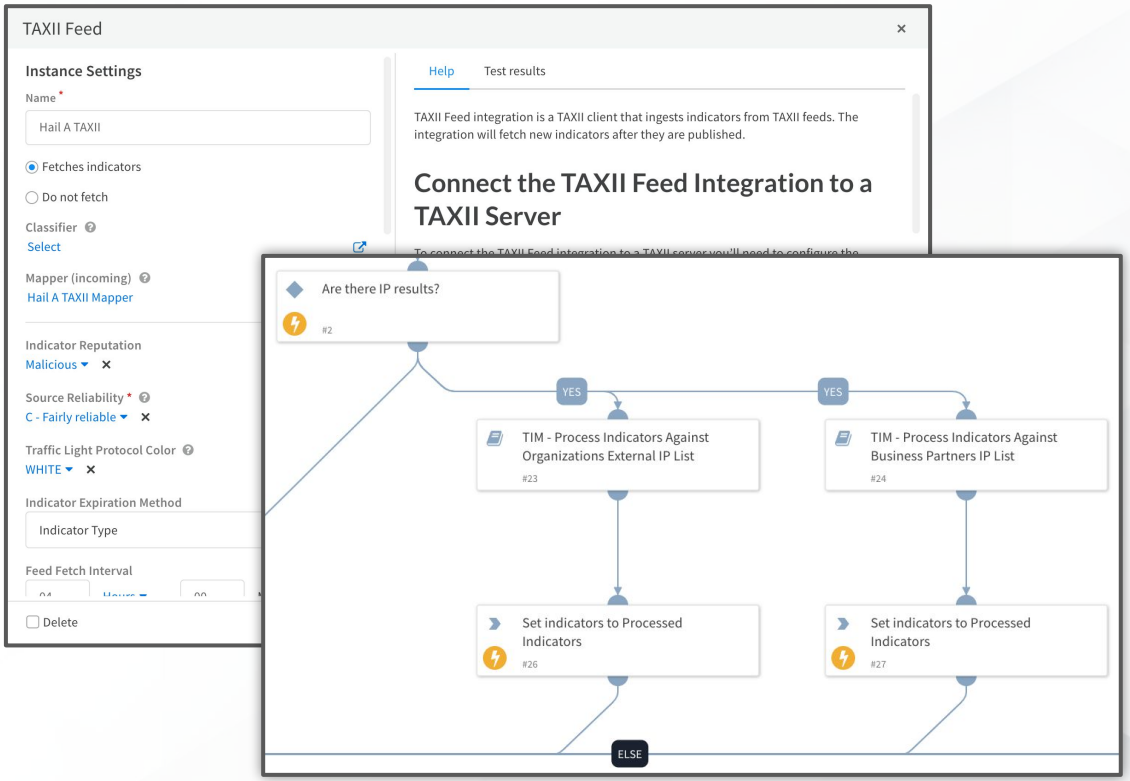
Gain unique visibility into cyber threat intelligence from the industry's largest footprint of network, endpoint, and cloud intel sources.

Gain a detailed understanding of your external threat landscape by enabling analysts to collaboratively build threat actor, campaign, and attack techniques profiles relevant to your industry.

Quickly incorporate additional intelligence via the Marketplace.

 |

Manage the Full Intelligence Lifecycle

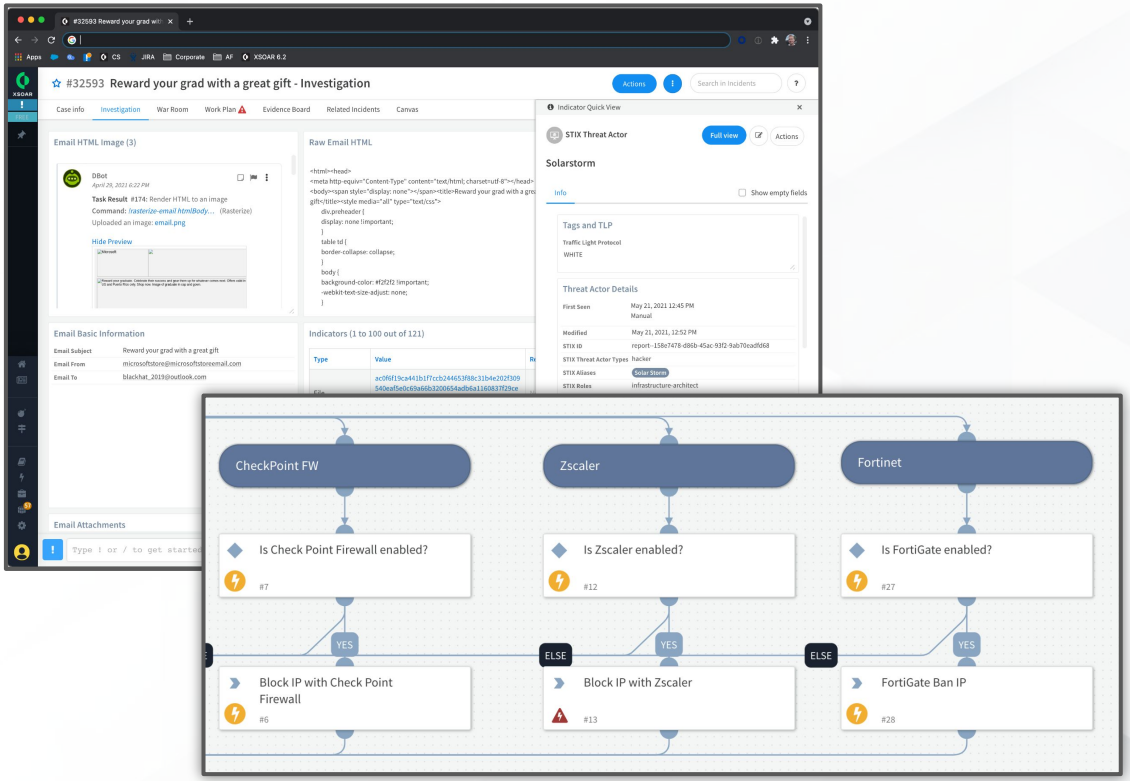


Collect, normalize, & de-dupe threat intelligence from open source, intelligence vendors, or custom feeds - all without writing a single line of code.

Identify the needle in the haystack by applying playbooks which automatically vet, enrich, & score intelligence.

Save time & safeguard against false positives by automatically expiring intelligence when it is no longer relevant.

Automate & Operationalize



Take automated action to immediately shutdown threats across your enterprise with purpose-built playbooks, based on proven SOAR capabilities.

Expand the scope of your investigations by easily sharing threat intelligence across internal teams and trusted organizations.

Gain confidence in your actions by enriching any detection, monitoring, or response tool with context from curated threat intelligence.

Weekly OSINT (Open Source Intelligence) Report

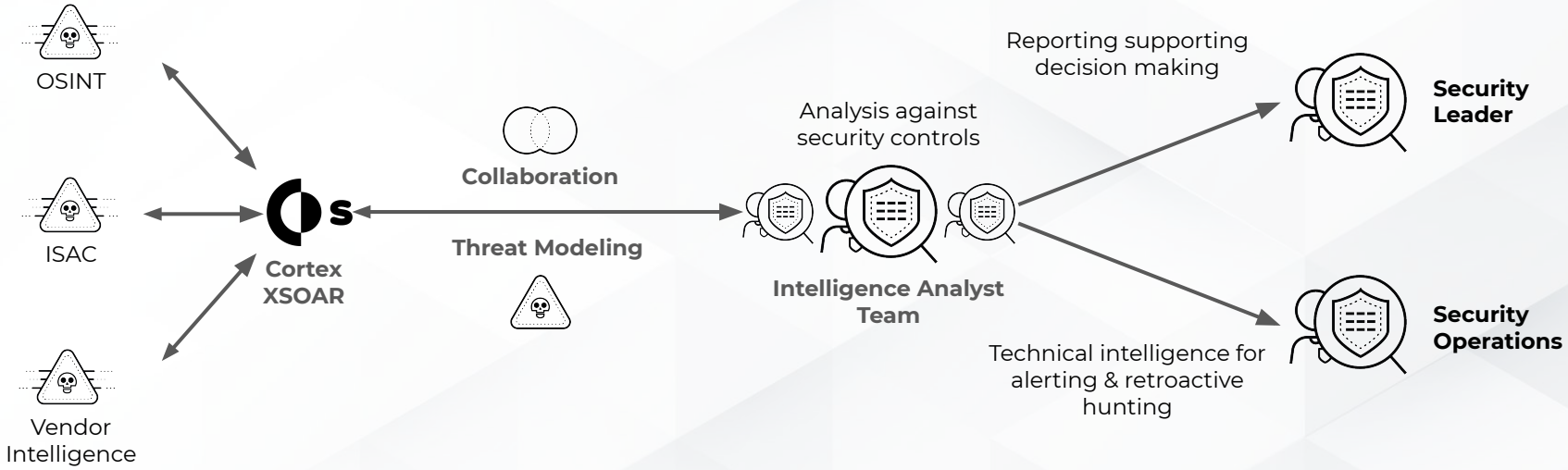
Intelligence Requirement: Keep IT employees educated regarding recent & emerging threats which target my industry vertical, provide analysis on why each threat is relevant to the business.
*** Bonus:** Advertise Threat Intelligence services to potential stakeholders.

COLLECT → ANALYZE → DISSEMINATE

 |

External Threat Landscape Modeling

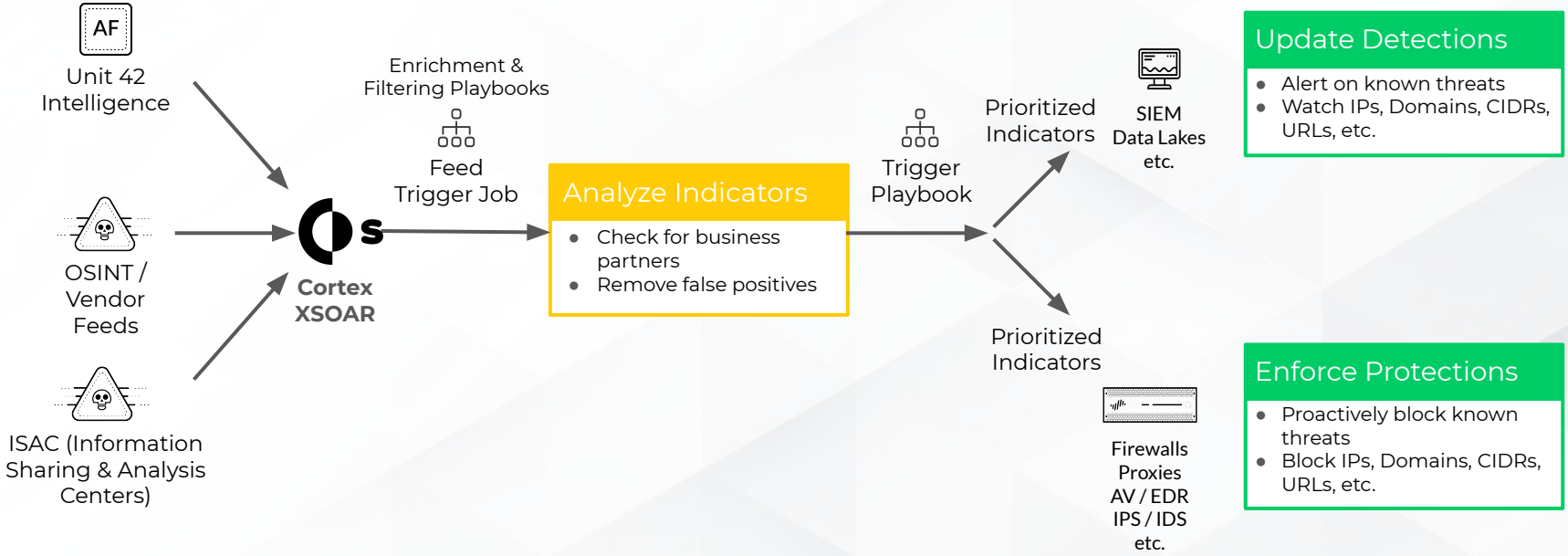
Threat Intelligence teams need to understand details of attacks and how their organization may be vulnerable. Threat Intel analysis begin profiling the attack, which will be foundational to understanding the risk of impact to their organization. The Intel team builds profiles of threat actors, identify if there are related attacks, identify which techniques and tools the threat actor used.
This information is shared to stakeholders including security operations and leadership.



COLLECT · · · · · ANALYZE · · · · · DISSEMINATE

Proactive blocking of threats

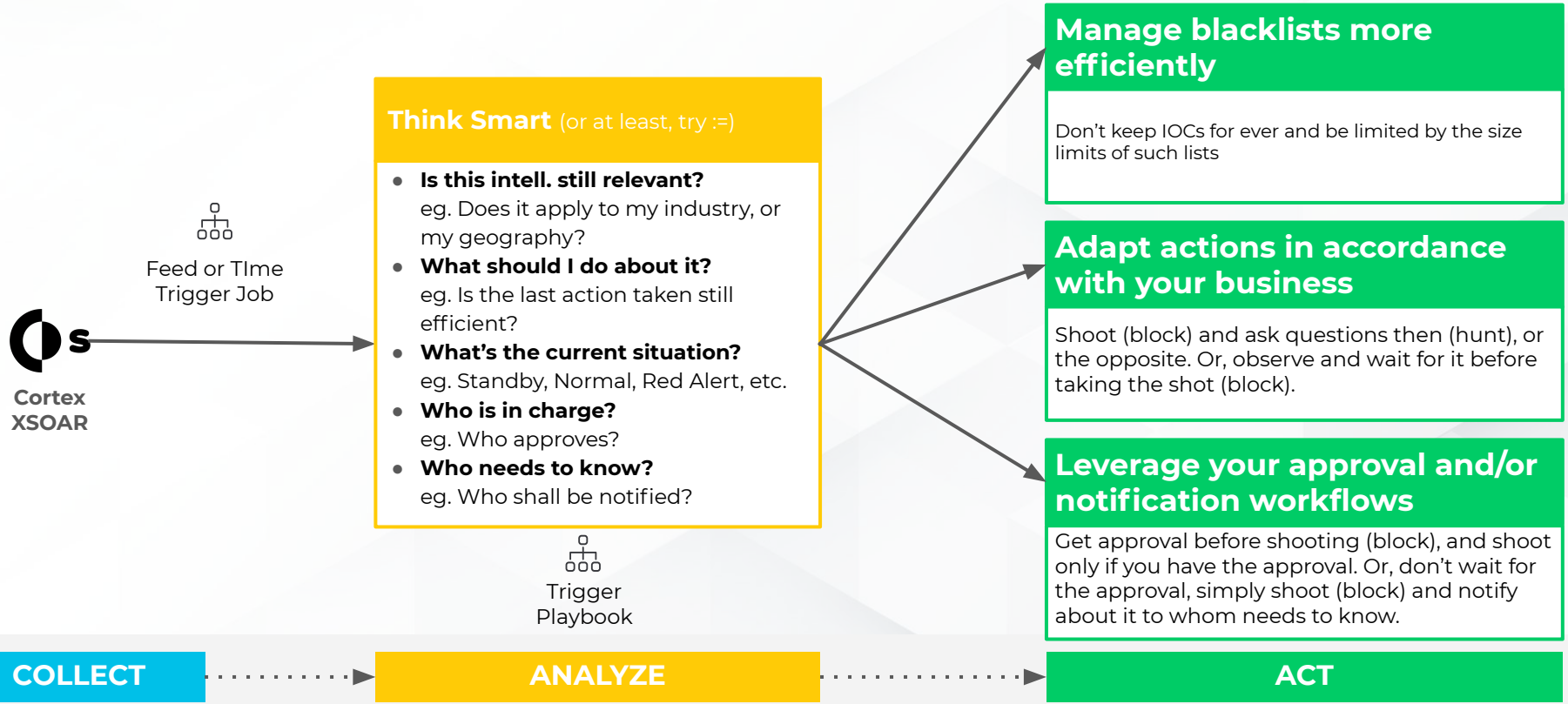
The security team needs to leverage threat intelligence to block or alert on known bad domains, IPs, hashes, etc (indicators). The indicators are being collected from many different sources which need to be normalized, scored, and analyzed before the customer can push to security devices such as SIEM & FireWall for alerting.



COLLECT → ANALYZE → DISSEMINATE

 |

TIM in action adapted to your context and your needs

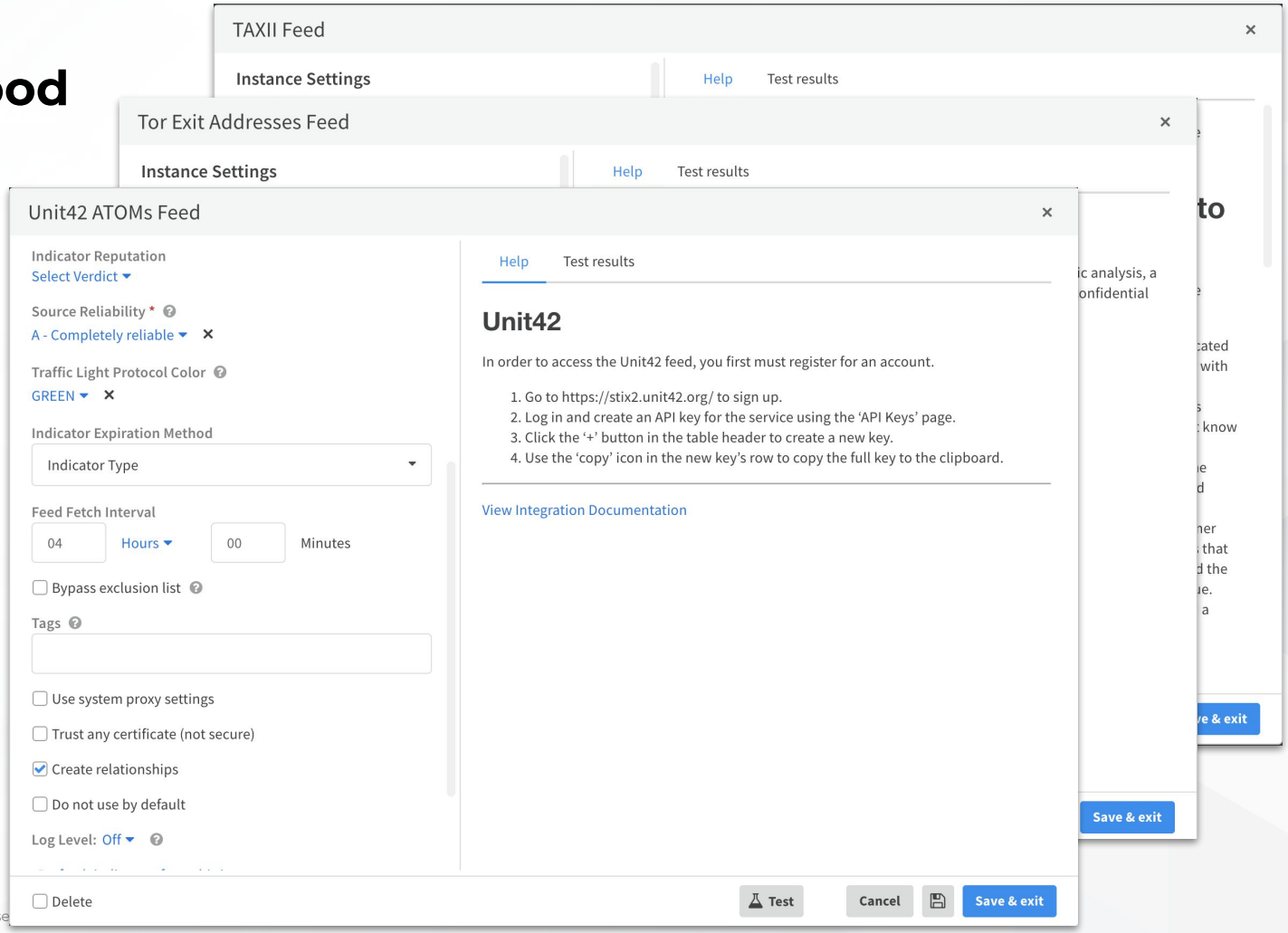


Under The Hood

Under The Hood

COLLECT

Setup Feed Integrations

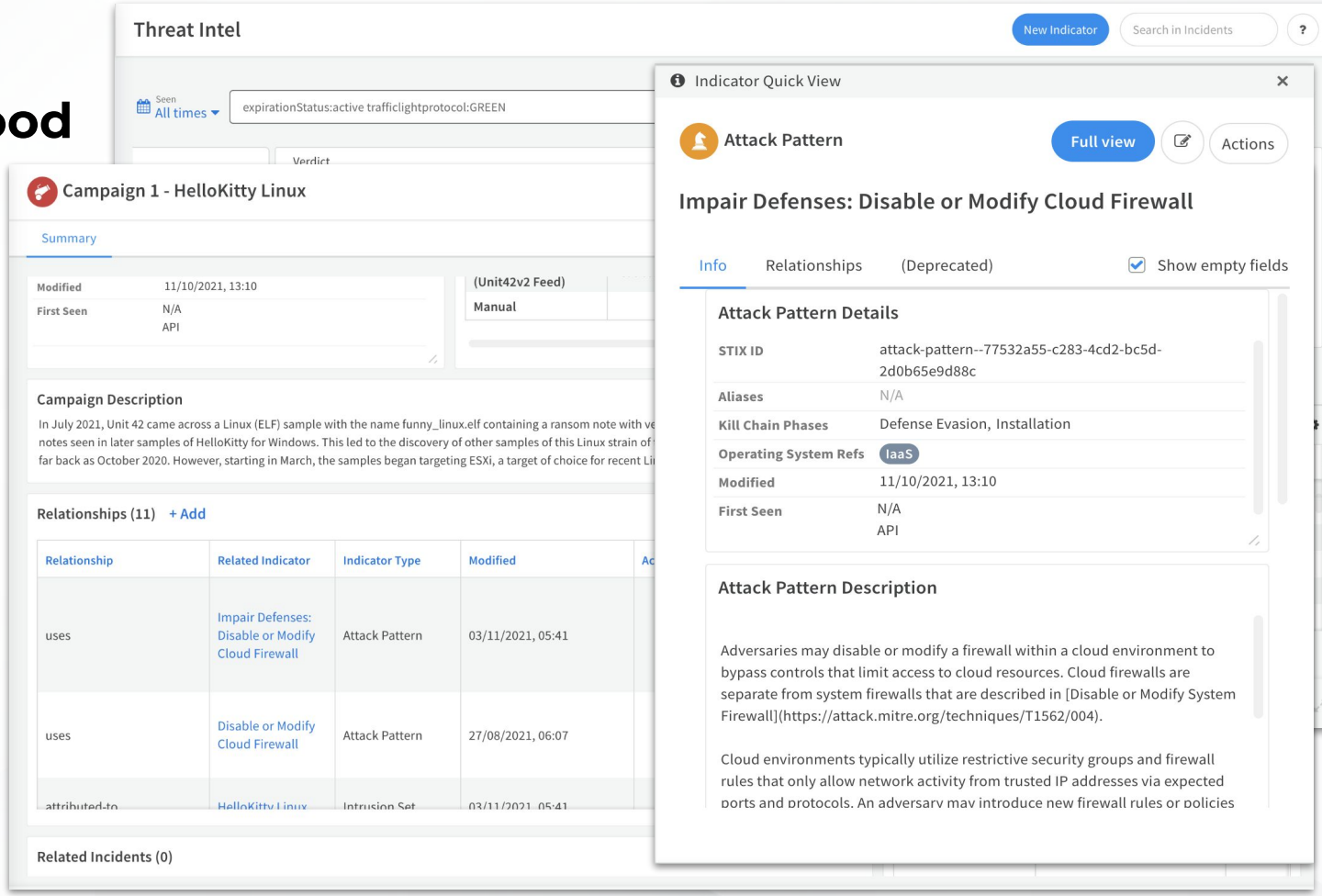


 |

Under The Hood

COLLECT

Bring and store Threat Intelligence in Cortex XSOAR repository.



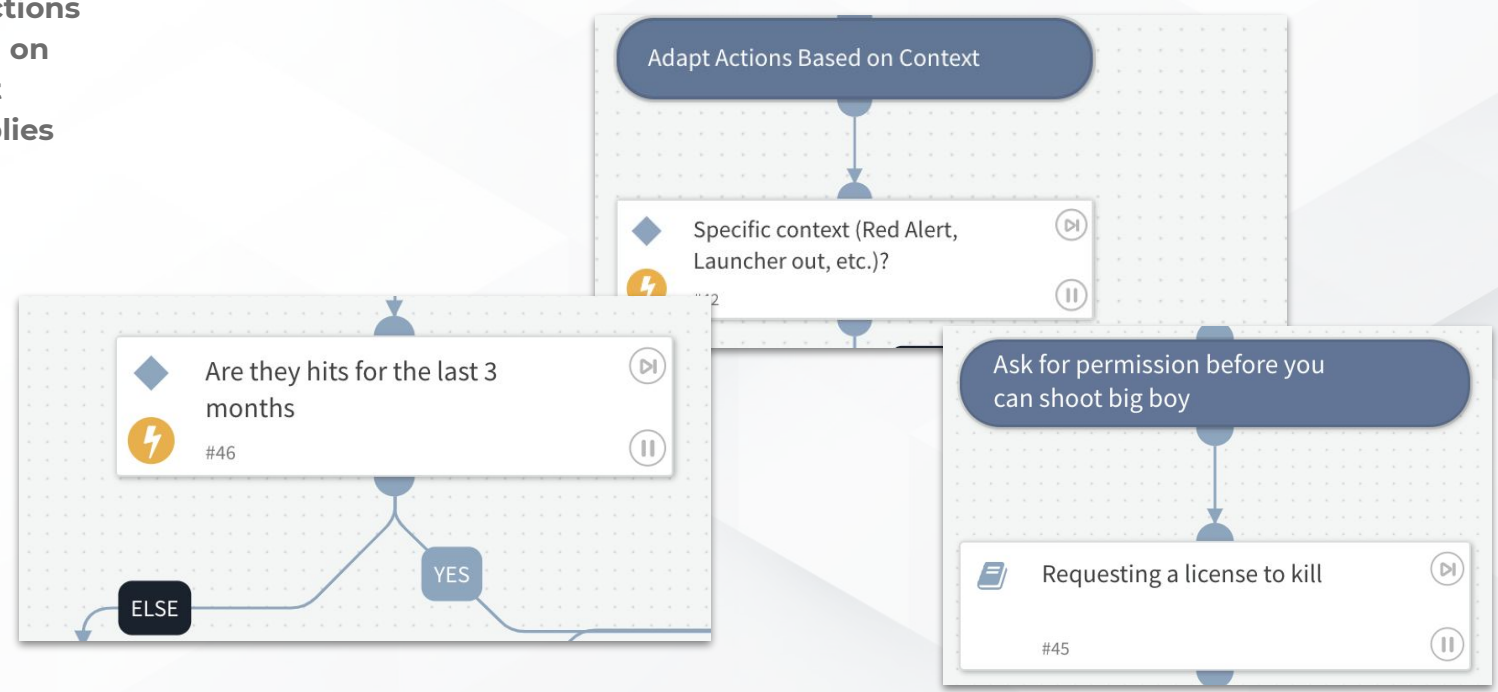
Under The Hood

ANALYZE

Influentiate the decisions and actions you made based on information that matters and applies to your context.

In-context relevant Threat Intelligence KPIs

Playbook Analysis / Decisions Build Block examples

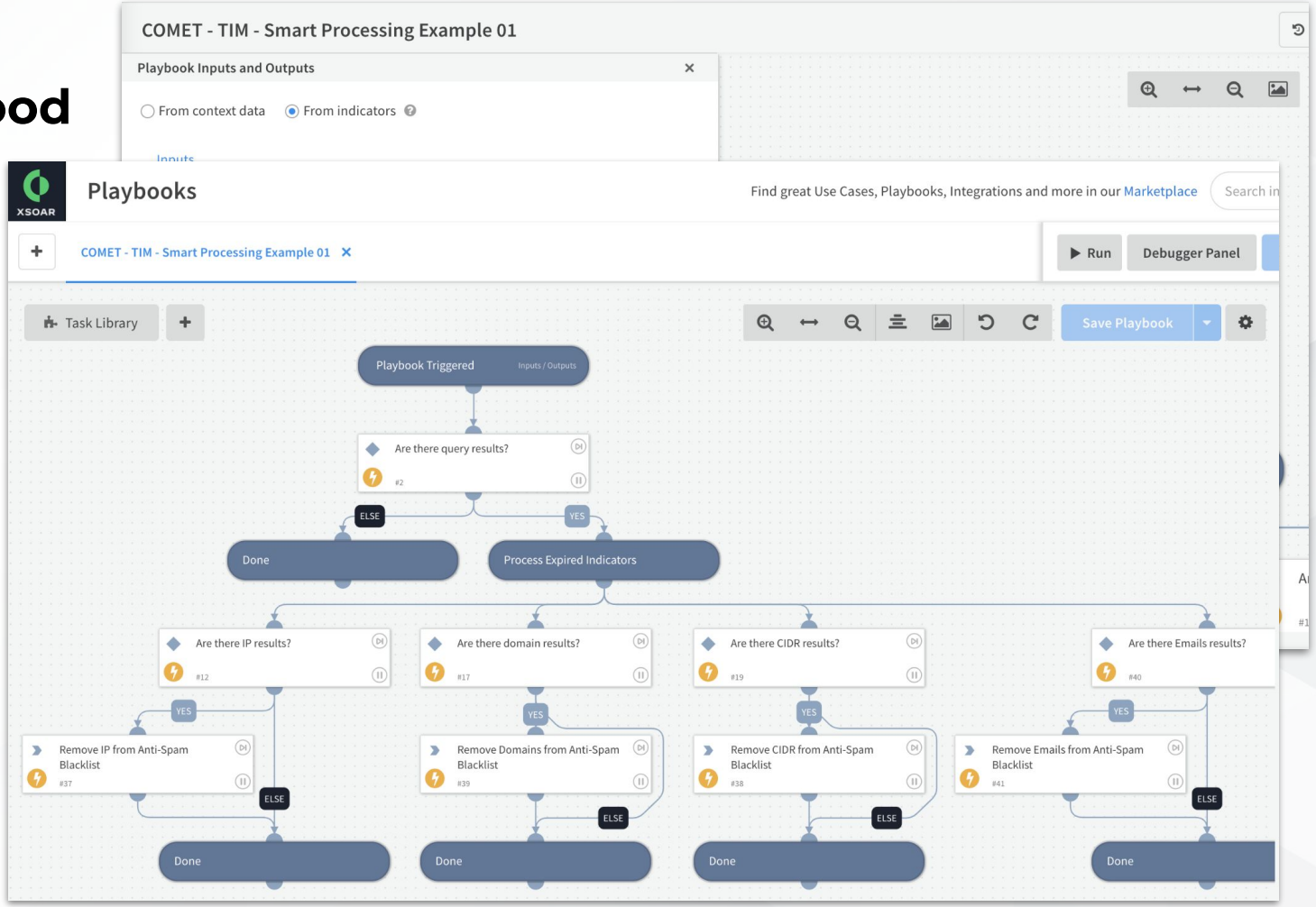


Under The Hood

ACT

Process Threat Intelligence at the speed and scale of the machine without loosing control.

Here how to simply purge blacklist from expired indicators.



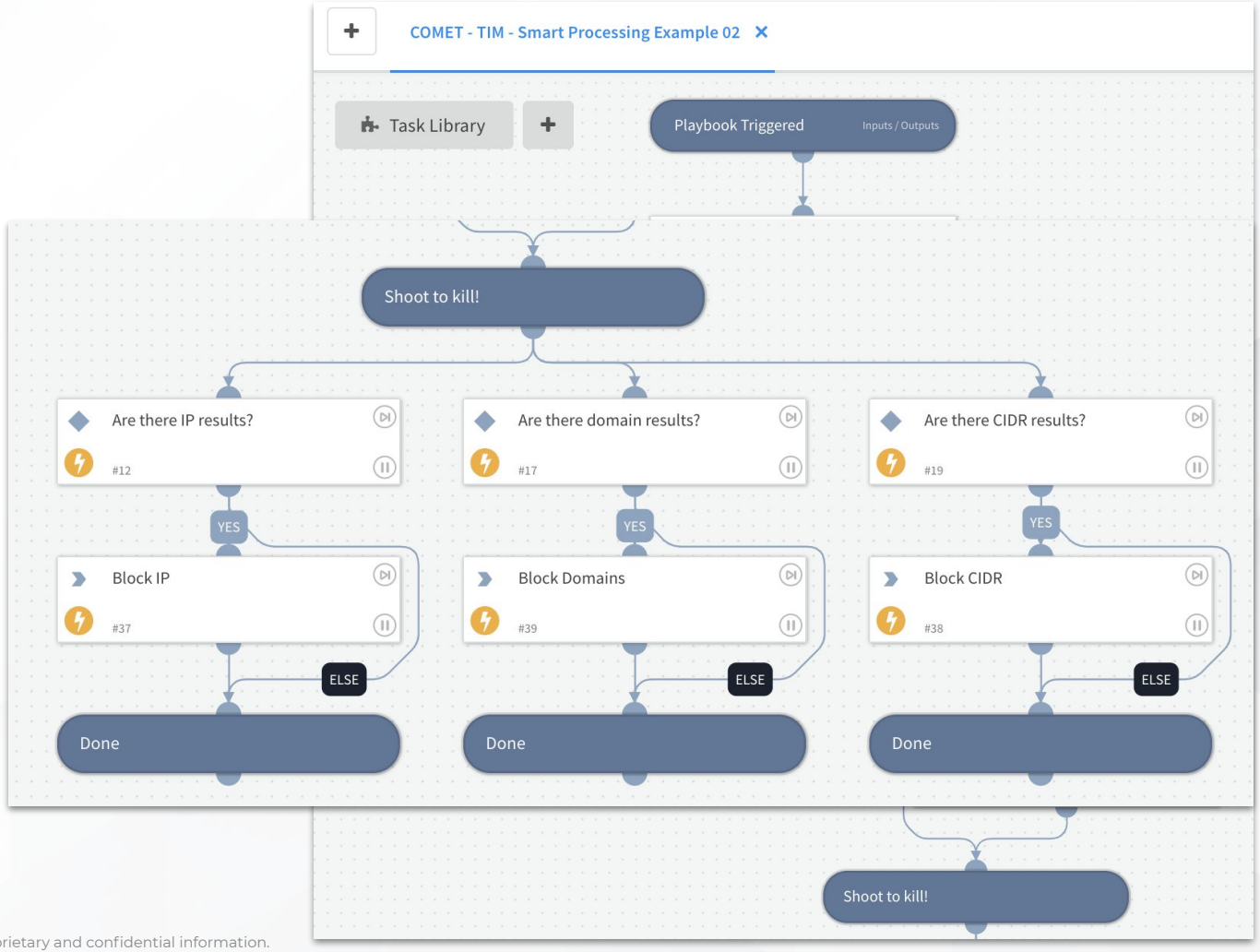
 |

Under The Hood

ACT

Process Threat Intelligence at the speed and scale of the machine without loosing control.

Here how to adapt your decision making based on your context.



 |

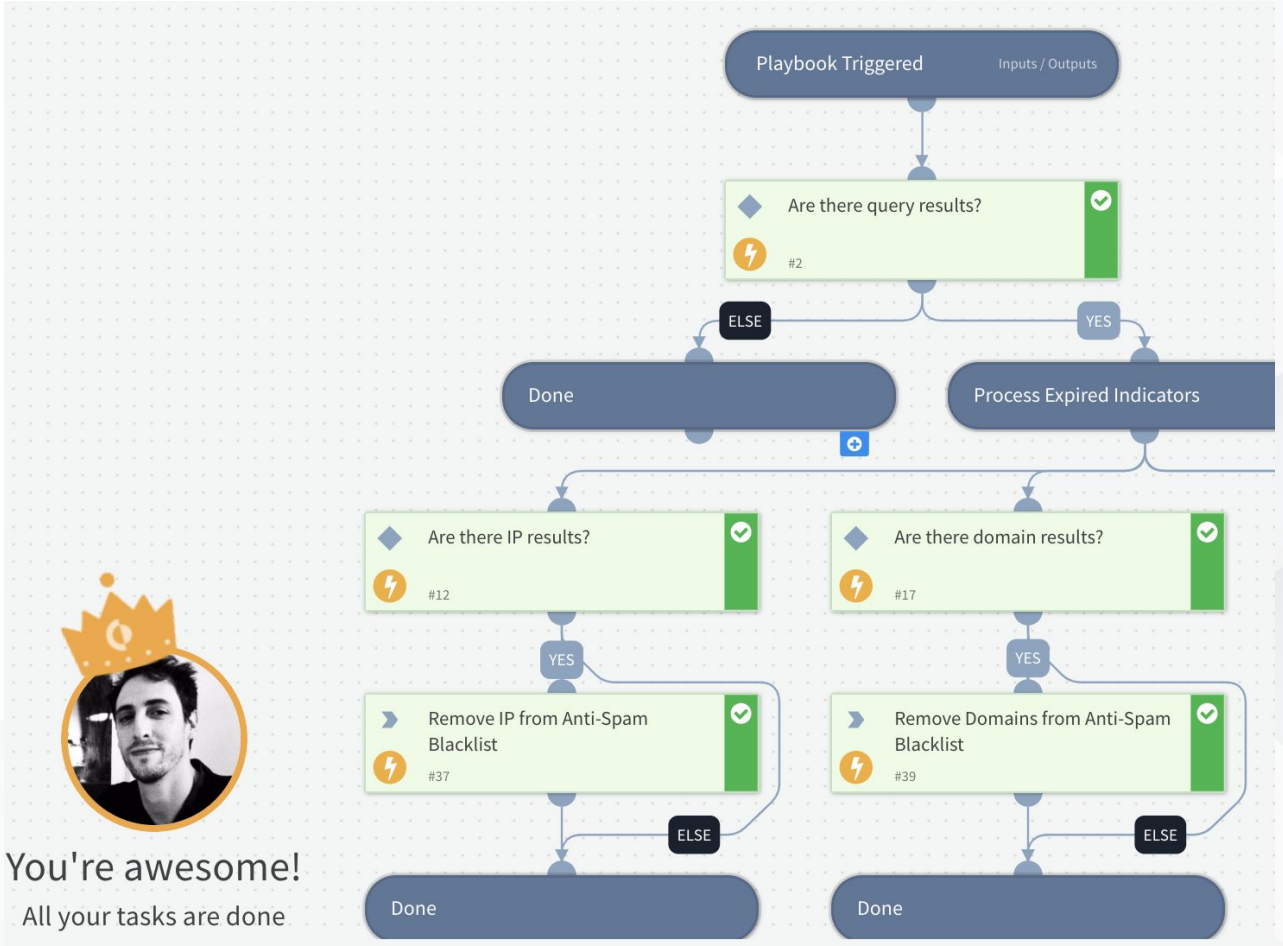
Under The Hood

COLLECT

ANALYZE

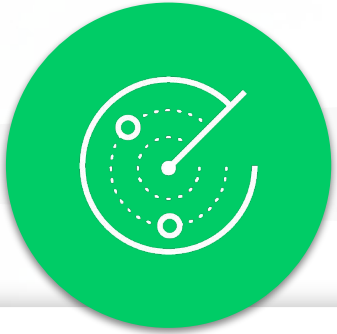
ACT

See your Threat Intelligence Management playbooks in motion.



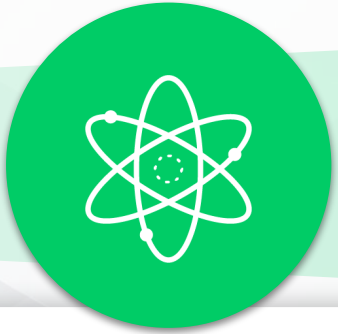
Wrap-Up

TIM or not to TIM, that should not be a question.



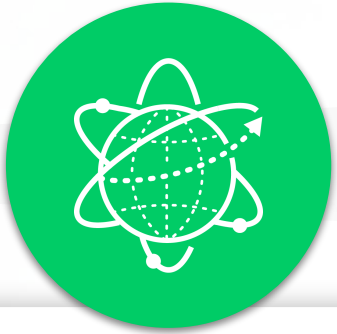
Being informed about Attackers, Threats, etc. is a good thing.

Doing something about it is even better.

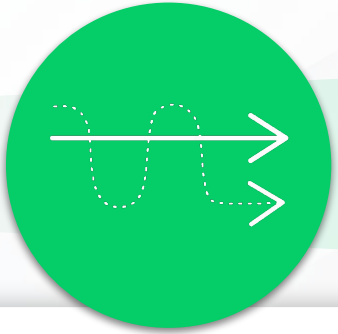


Doing something about it, while taking into account your context, is the best.

TIM & Strategic Reports / Analysis



Bring readable threats impact metrics to C-Level.



Compare yourself to your peers or other industries.

Follow your exposure level to threats year after year.

Let’s keep in touch

 |


CORTEX
paloalto
NETWORKS
Race Against Time
Are you ready for the next big cyberattack?
Every second counts. Join us for our simulation event, “Race Against Time.”
30th November from 4PM CET
22rd December from 4PM CET
26th of January from 4PM CET

Intelligence Driven.
Response Ready.

Under Attack?

unit42-investigations@paloaltonetworks.com

866-486-4842 (1-866-4-UNIT42)

Unit 42 Incident Response
Get in touch 24/7/365

paloalto® NETWORKS | UNIT 42™ BY PALO ALTO NETWORKS

paloalto NETWORKS | IGNITE21

WE'VE GOT NEXT

November 15-18, 2021

ignite.paloaltonetworks.com

We look forward to seeing you

 |


THANK YOU
paloalto NETWORKS
Cybersecurity
Partner of Choice