



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

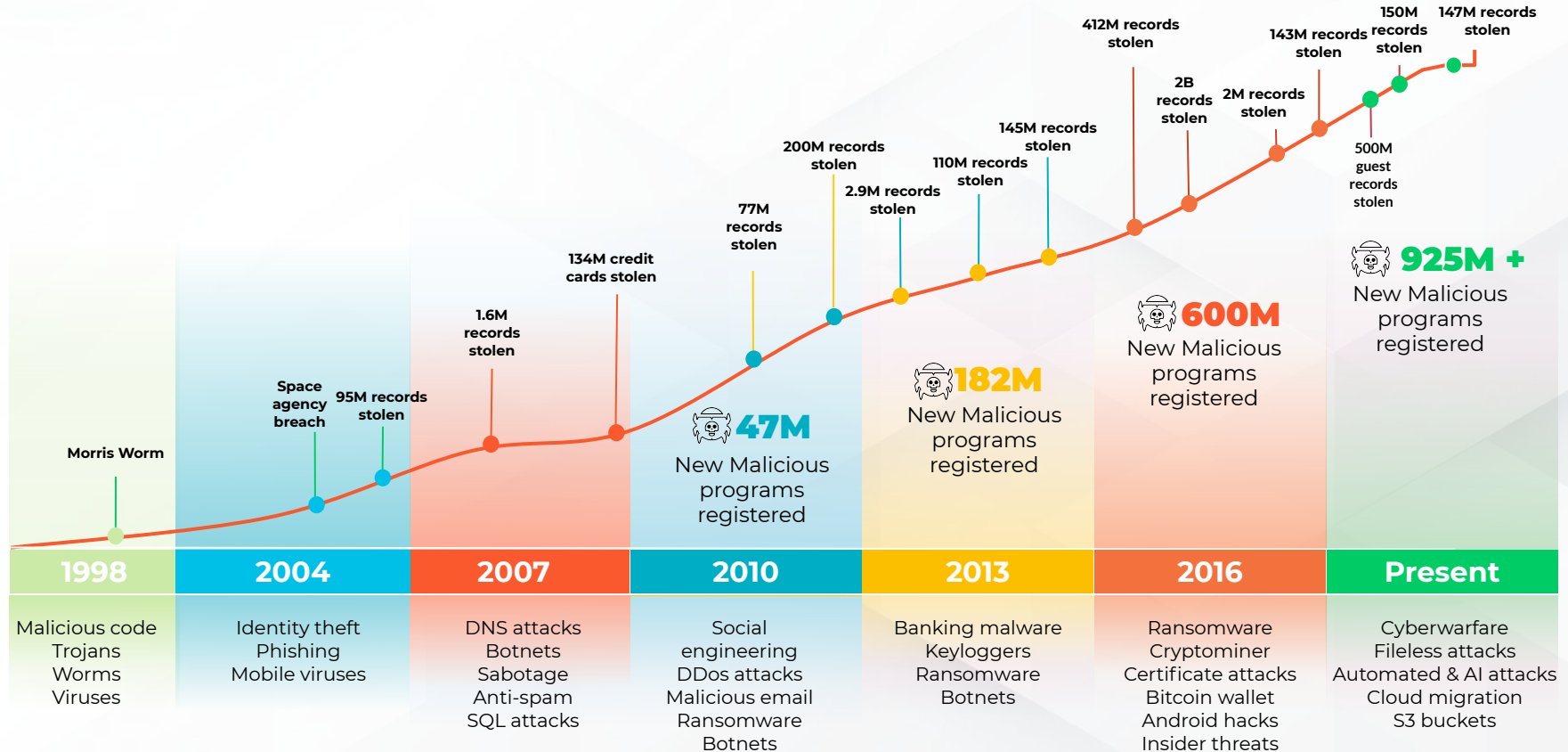
**Cybersecurity
Partner of Choice**



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

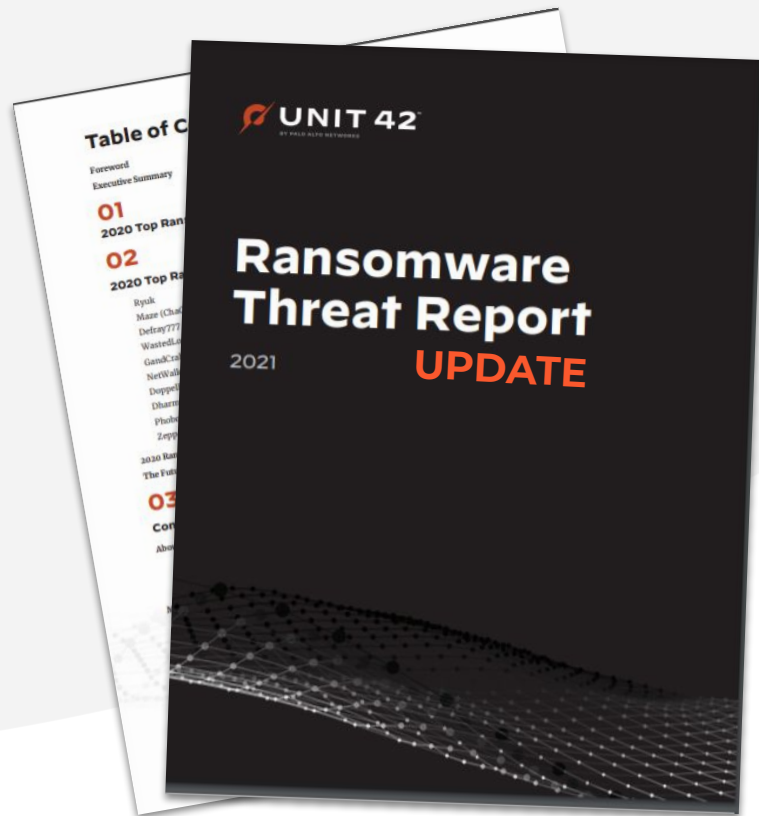
up 82% from previous year

\$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

JBS ransomware - US, CN, AU facilities shut down

Fujitsu hack

Ireland's national health service ransomware

Colonial Pipeline ransomware

DDoS attack on **Belgium** government

Verizon and **Microsoft** hacks

NATO, UK, NL warships fake data

1,182 UK Special Forces soldiers data leak

Department of Energy nuclear weapons supply chain attack

Japan Olympics data breach

Southeast Asia APT

South Africa port and freight halted

Kaseya hack
1,500 SMBransomed

Belarus, Slovak, Iranian governments breach

Russian election hack

T-Mobile breach
50 million accounts

Poly Network
\$600 million heist

Italian COVID 19 vaccine site hack

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>



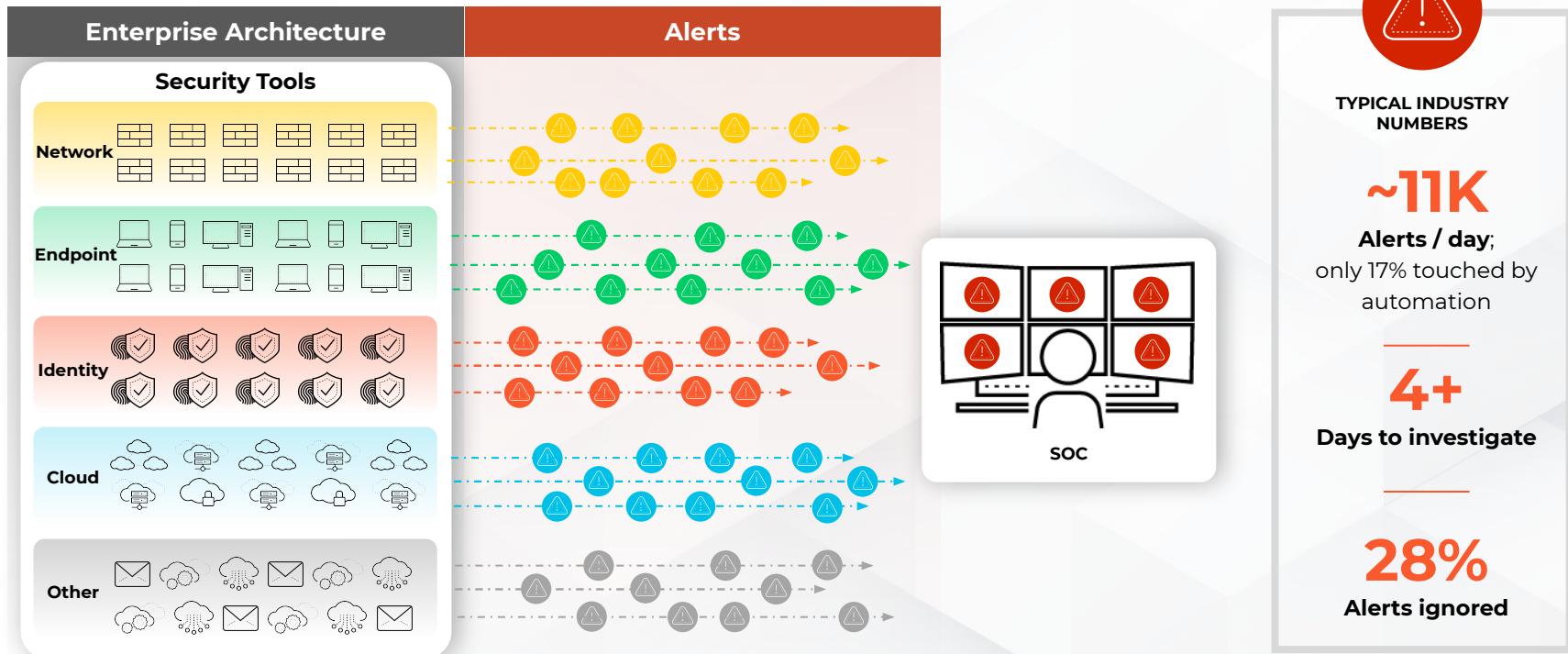
Reinventing Security Operations

Building the Flywheel for the SOC.

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

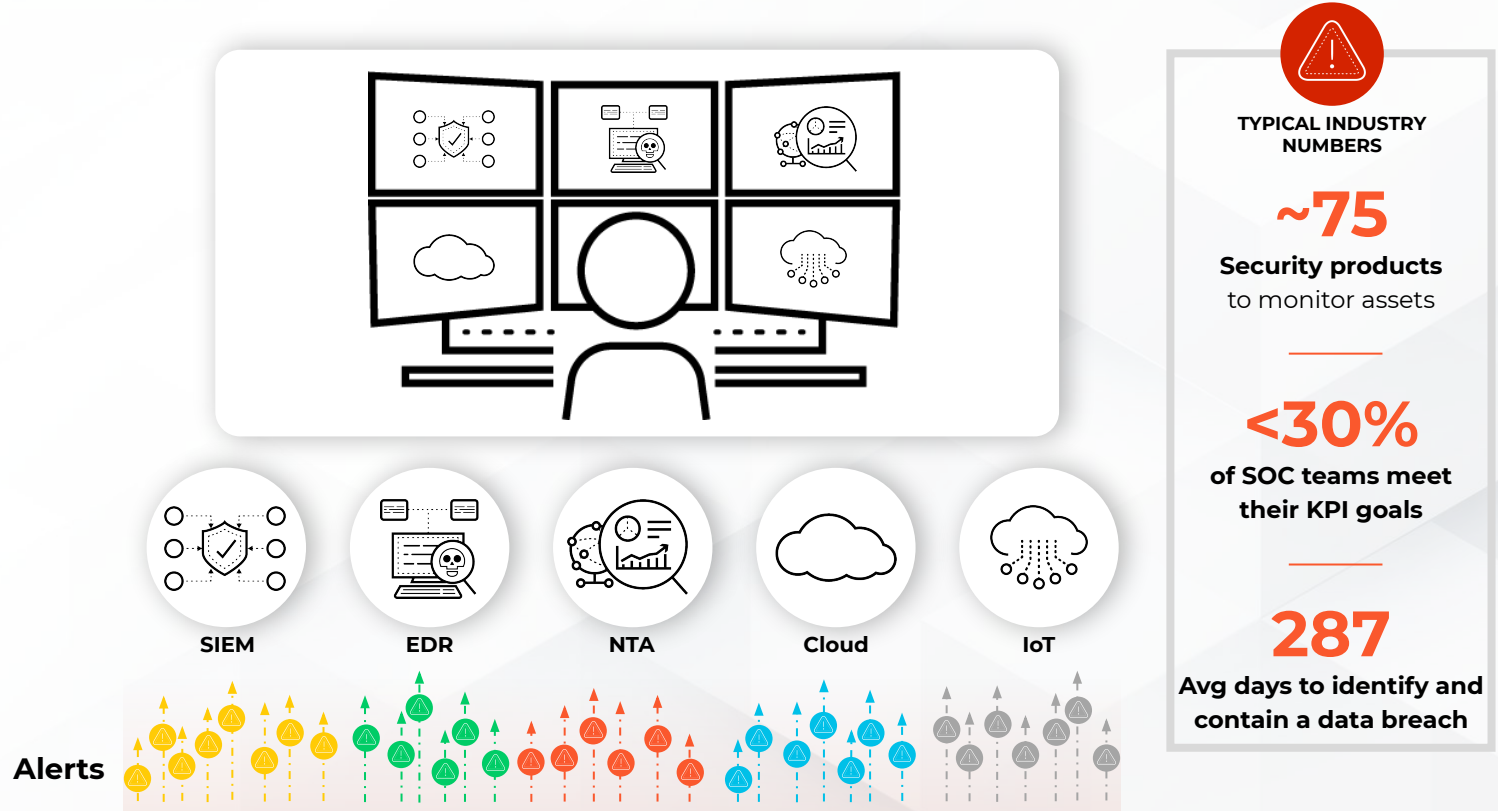


Security Operations: Increasing volume of alerts is overwhelming most SOC's



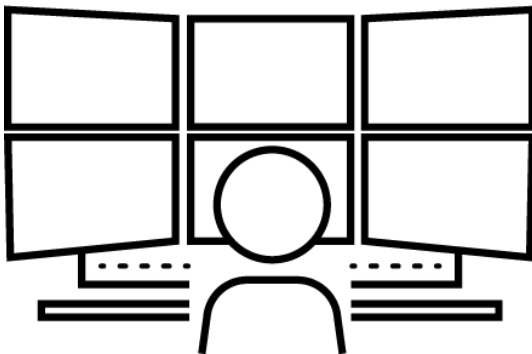
Source: Forrester (The 2020 State of Security Operations), Demisto (The State of SOAR Report, 2018)

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



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**

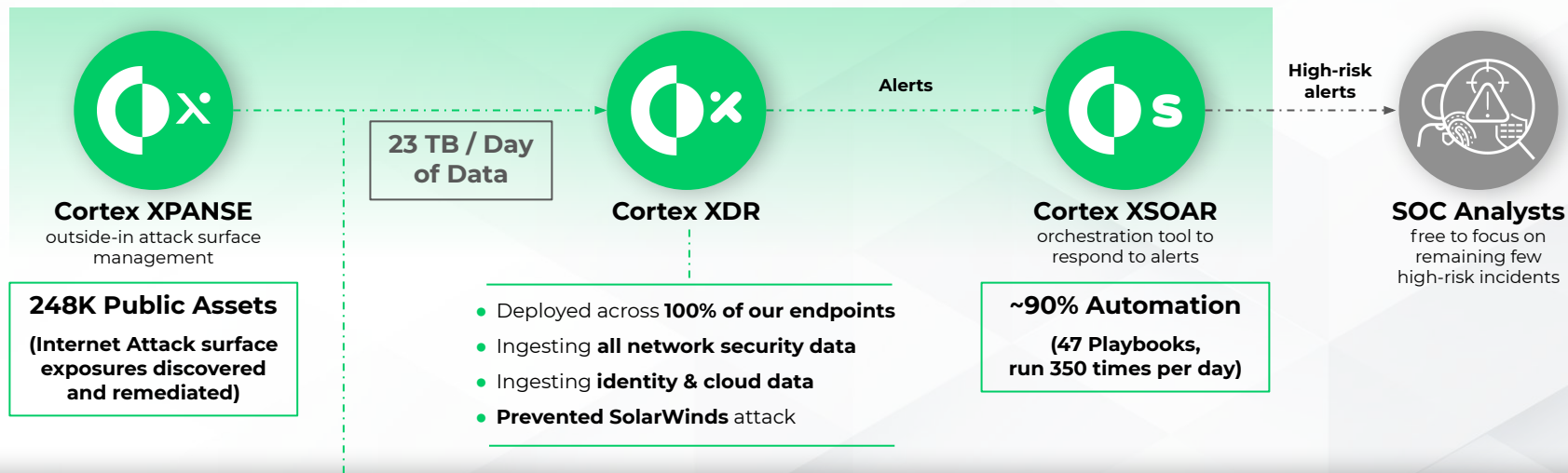
100%

**Of attacks identified
and stopped**

Minutes

**To respond to
threats, not days**

Palo Alto Networks SOC: Eating our own dog food



Comprehensive security

Network



Prisma Access



NGFWs,



VMs,



and Security Services

10K Employees

Endpoint



Cortex XDR

50K Endpoints

Cloud



Prisma SaaS



Prisma Cloud



Data Security

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

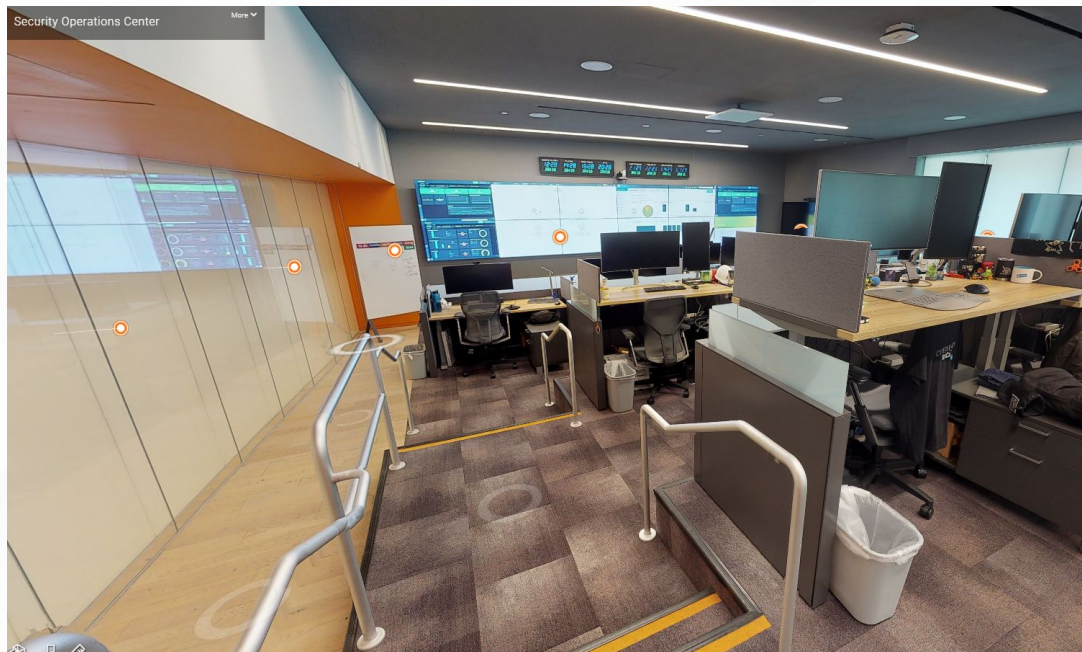


Palo Alto Networks SOC: Take a virtual walkthrough tour of our SOC

- 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.



A woman with short dark hair, wearing a white blazer over a dark collared shirt, is looking down at a tablet computer she is holding with both hands. She is in a warehouse or industrial setting, with large cardboard boxes visible in the background. The lighting is warm and slightly dim. A semi-transparent dark grey horizontal band is overlaid across the middle of the image, containing the main title and subtitle. The title 'Threat Intelligence Management' is in large white font, with a small orange horizontal line above the 'e' in 'Intelligence'. The subtitle 'How to do clever things with smart data gathered about the adversaries.' is in a smaller orange font below the title. The page number '17' and copyright information are in the bottom left corner.

Threat Intelligence Management

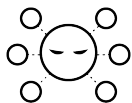
How to do clever things with smart data gathered about the adversaries.

Current Threat Intelligence Platforms are an Incomplete Puzzle

What is possible?

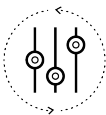


Static IOC
scoring

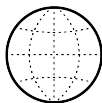


External intel
aggregation

What is missing?

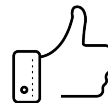


User-driven
automation



Real-world
context

Why does it matter?



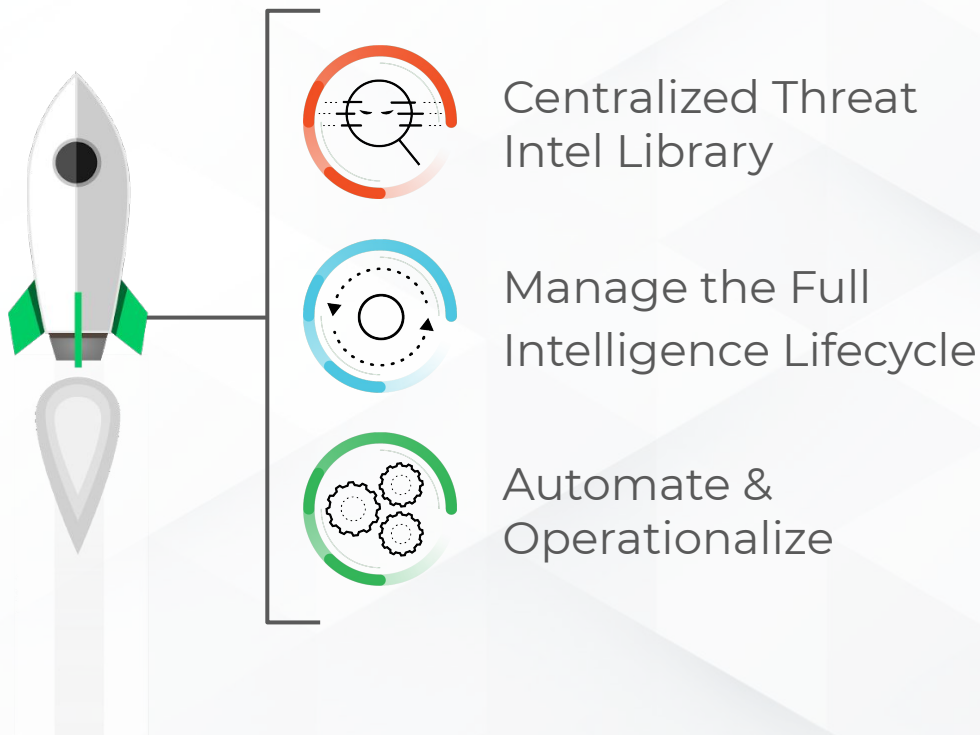
Gain confidence



Smarter incident
response

Threat Intel Management Basic Concepts

Supercharged threat intelligence management





Centralized Threat Intel Library

Solarstorm

Search in Incidents

Summary Additional Details

☑ Show empty fields Create incident Edit Delete and Exclude

Threat Actor Details

First Seen	May 13, 2021 12:49 PM	STIX Roles	infrastructure-architect
Modified	May 13, 2021, 12:58 PM	STIX Goals	Espionage
STIX ID	report-158e7478-d86b-45ac-93f2-9ab70eadf668	STIX Sophistication	strategic
STIX Threat Actor Types	hacker	STIX Resource Level	government
STIX Alliances	Solar Storm	STIX Primary Motivati...	organizational gain
		STIX Secondary Motiv...	N/A

Relationships (3) + Add

Hide Revoked

Relationship	Related Indicator	Indicator Type	Modified	Actions	Status
uses	T1505	MITRE ATT&CK	May 13, 2021, 12:57 PM		Active
attributed-to	August 2019 to December 2020	Campaign	May 13, 2021, 12:57 PM		Active

Threat Actor Description

SolarStorm is a highly skilled threat actor, with significant operational security mindset and has targeted supply chains during their attack on SolarWinds Orion IT performance and statistics monitoring software.

Tags and TLP

Tags

Intrusion-Set

Add tags Remove tags

Traffic Light Protocol

N/A

Timeline (9)

Date ↓	Event	Source
May 13, 2021, 12:58 PM	New relationship related-to created to 53f8d4c65169ccda021b72a62e0c22a4db7c4077f002fa742717d41b3c40f2c7	admin (Manual)

Comments

+ Add

There are no comments. [Click to add](#)

Navigate quickly with `cmd+k`

Backdoor Oldrea

Screen Capture

Commonly Used Port

Valid Accounts

Compromise Software Supply Cha...

Spearphishing Attachment

Possible Phishing

Hunting incident

Hunting incident

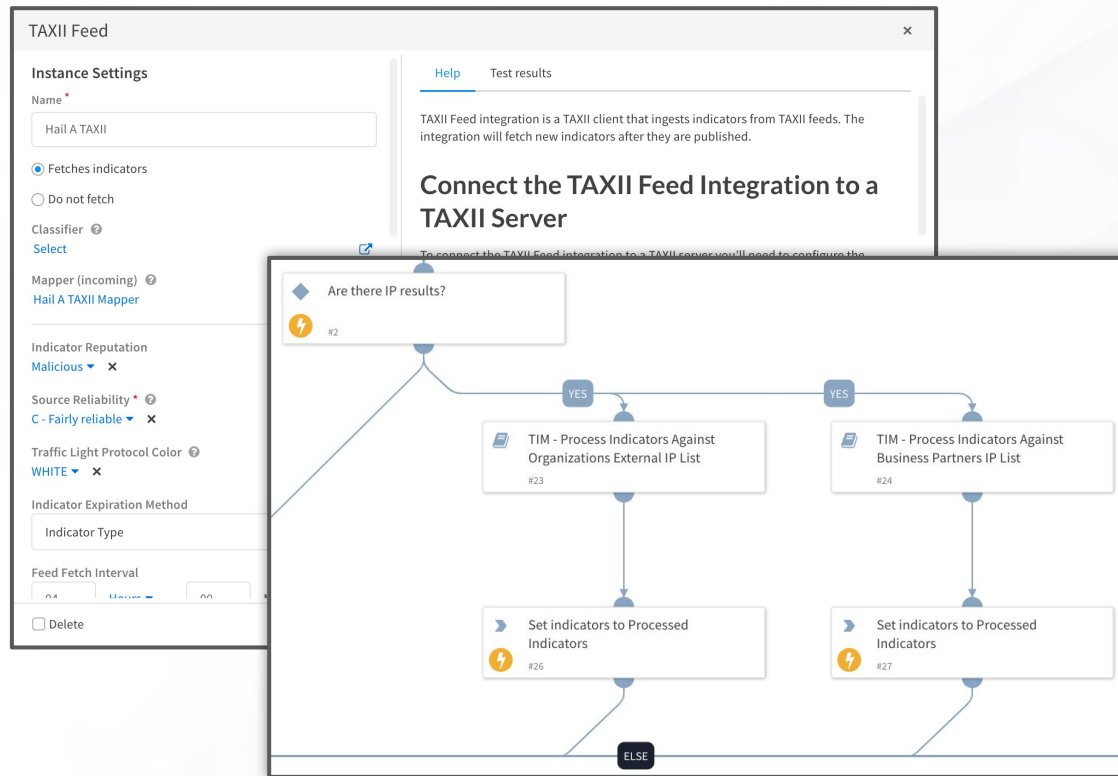
Gain unique visibility into cyber threat intelligence from the industry's largest footprint of network, endpoint, and cloud intel sources.

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

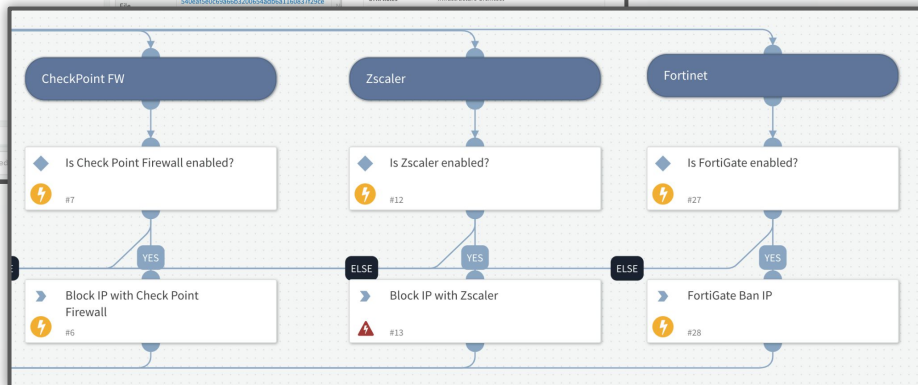
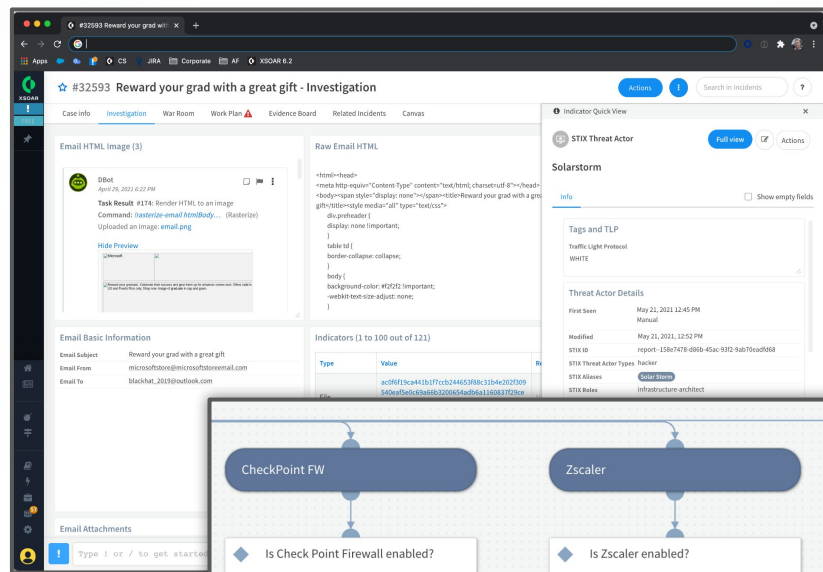


Collect, normalize, & de-dupe threat intelligence from open source, intelligence vendors, or custom feeds - all without writing a single line of code.

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.

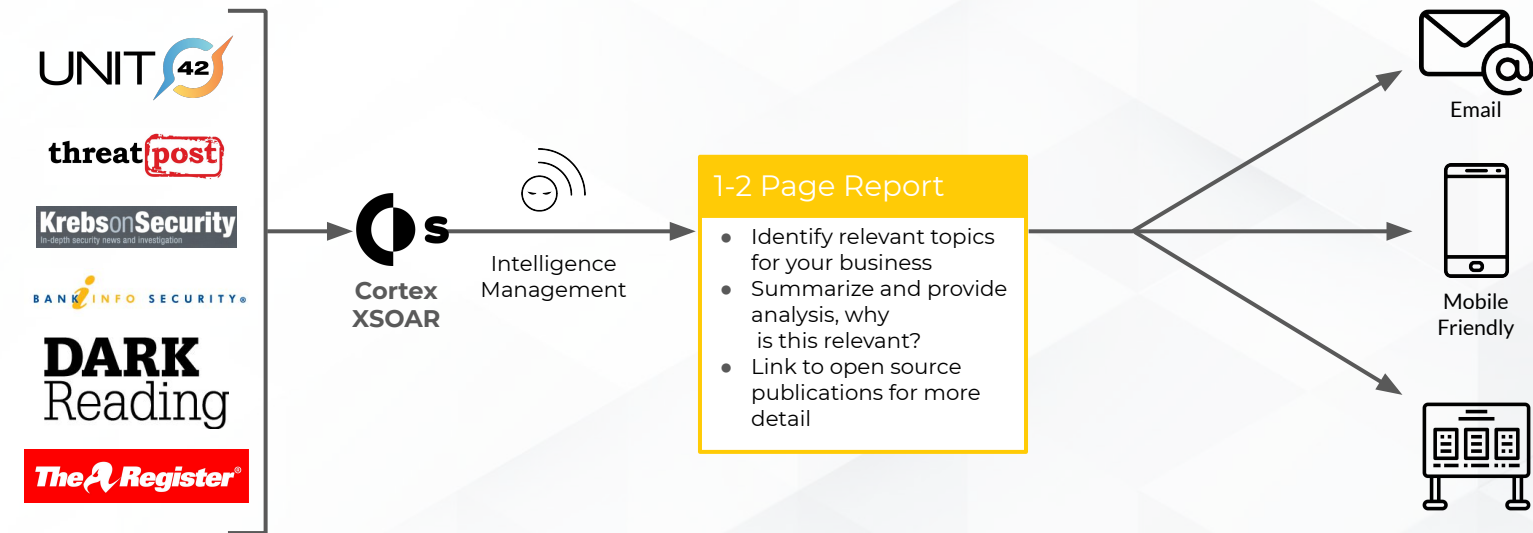
Expand the scope of your investigations by easily sharing threat intelligence across internal teams and trusted organizations.

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

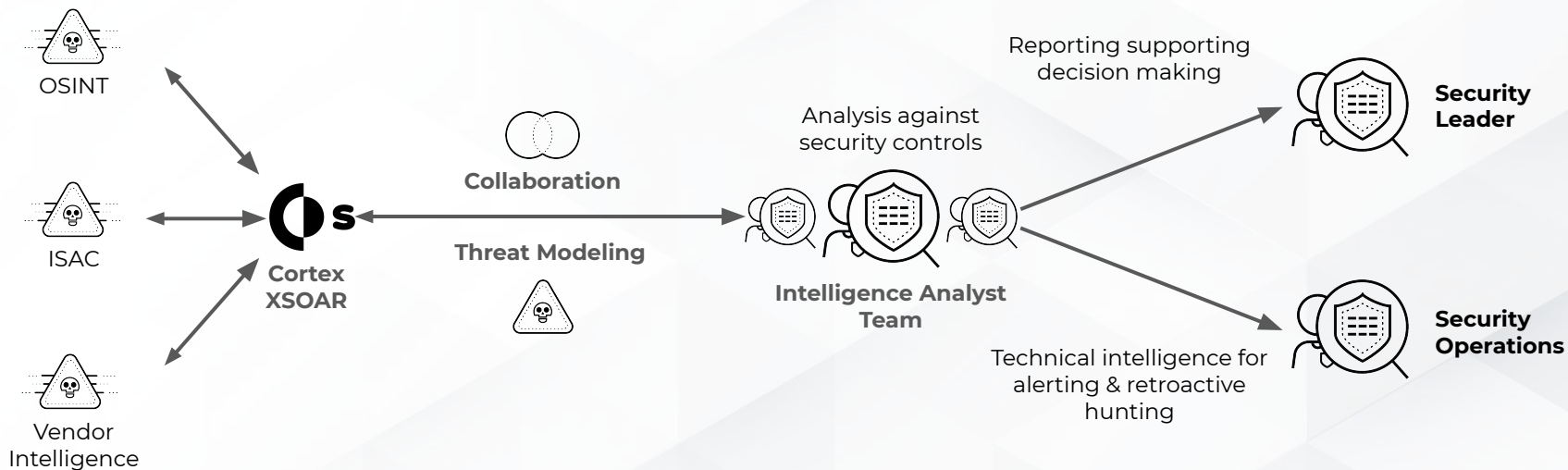
Intelligence Requirement: Keep IT employees educated regarding recent & emerging threats which target my industry vertical, provide analysis on why each threat is relevant to the business.

*** Bonus:** Advertise Threat Intelligence services to potential stakeholders.



External Threat Landscape Modeling

Threat Intelligence teams need to understand details of attacks and how their organization may be vulnerable. Threat Intel analysis begins 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.



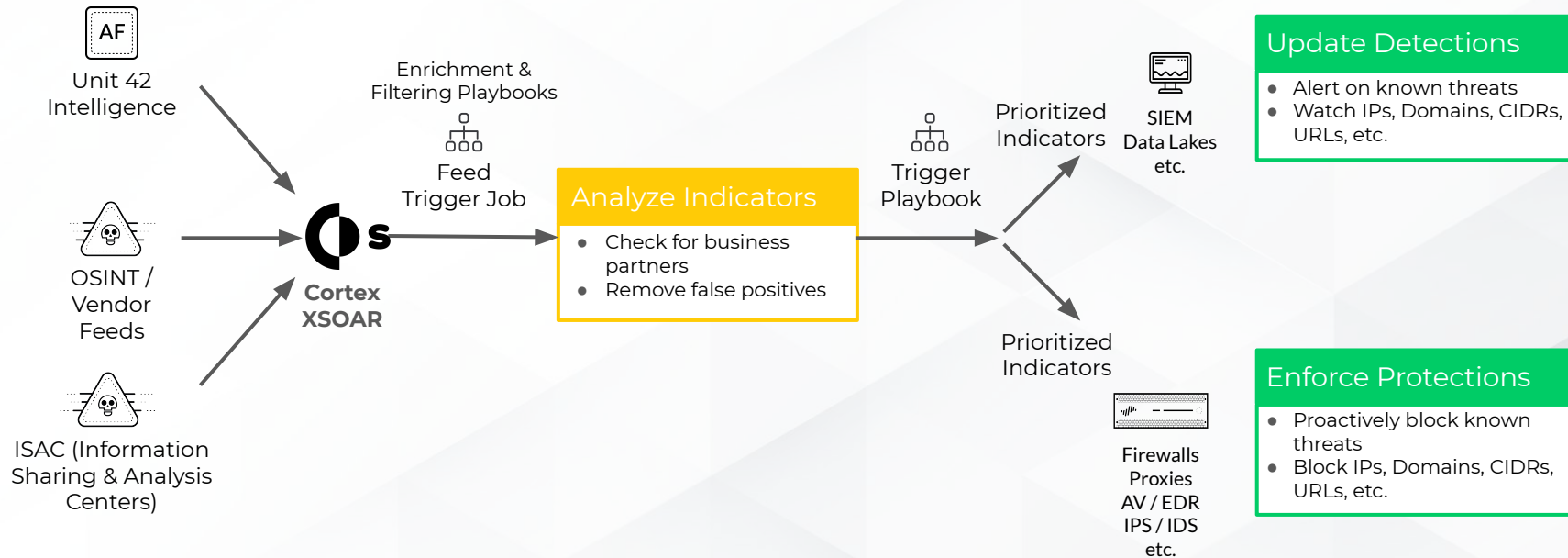
COLLECT

ANALYZE

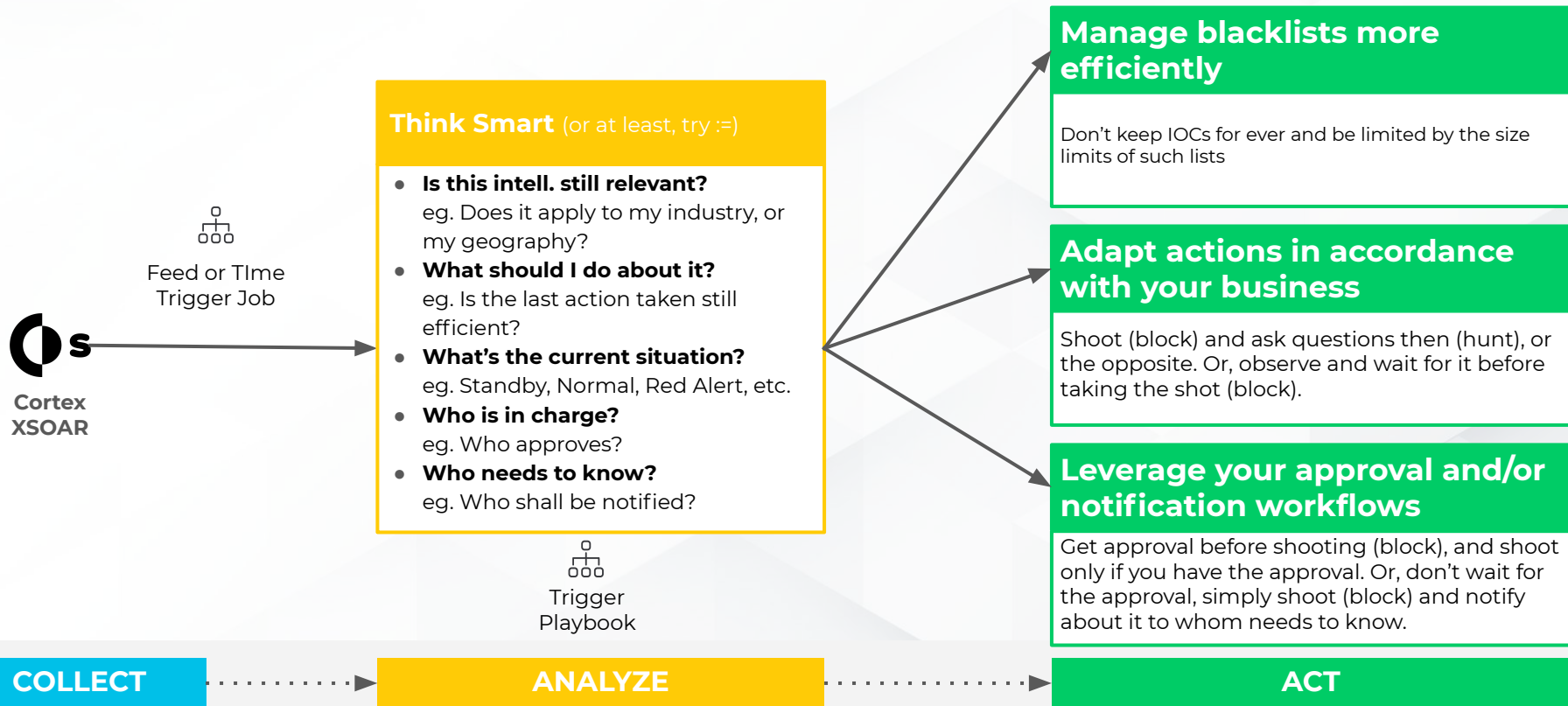
DISSEMINATE

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.



TIM in action adapted to your context and your needs



Under The Hood

Under The Hood

COLLECT

Setup Feed Integrations

TAXII Feed

Instance Settings

Help

Test results

Tor Exit Addresses Feed

Instance Settings

Help

Test results

Unit42 ATOMs Feed

Indicator Reputation

Select Verdict

Source Reliability

A - Completely reliable

Traffic Light Protocol Color

GREEN

Indicator Expiration Method

Indicator Type

Feed Fetch Interval

04

Hours

00

Minutes

Bypass exclusion list

Tags

Use system proxy settings

Trust any certificate (not secure)

Create relationships

Do not use by default

Log Level: Off

Delete

Test

Cancel

Save & exit

Unit42

In order to access the Unit42 feed, you first must register for an account.

1. Go to <https://stix2.unit42.org/> to sign up.
2. Log in and create an API key for the service using the 'API Keys' page.
3. Click the '+' button in the table header to create a new key.
4. Use the 'copy' icon in the new key's row to copy the full key to the clipboard.

[View Integration Documentation](#)

Save & exit

Under The Hood

COLLECT

Bring and store
Threat Intelligence in
Cortex XSOAR
repository.

Threat Intel

[New Indicator](#)

Seen
All times

expirationStatus:active trafficlightprotocol:GREEN

Verdict



Campaign 1 - HelloKitty Linux

Summary

Modified 11/10/2021, 13:10
First Seen N/A
API

(Unit42v2 Feed)

Manual

Campaign Description

In July 2021, Unit 42 came across a Linux (ELF) sample with the name funny_linux.elf containing a ransom note with notes seen in later samples of HelloKitty for Windows. This led to the discovery of other samples of this Linux strain of far back as October 2020. However, starting in March, the samples began targeting ESXi, a target of choice for recent Lin

Relationships (11) + Add

Relationship	Related Indicator	Indicator Type	Modified	Ac
uses	Impair Defenses: Disable or Modify Cloud Firewall	Attack Pattern	03/11/2021, 05:41	
uses	Disable or Modify Cloud Firewall	Attack Pattern	27/08/2021, 06:07	
attributed-to	HelloKitty Linux	Intrusion Set	03/11/2021, 05:41	

Related Incidents (0)

Indicator Quick View



Attack Pattern

[Full view](#)[Actions](#)

Impair Defenses: Disable or Modify Cloud Firewall

[Info](#)[Relationships](#)[\(Deprecated\)](#)☒ Show empty fields

Attack Pattern Details

STIX ID attack-pattern--77532a55-c283-4cd2-bc5d-2d0b65e9d88c

Aliases N/A

Kill Chain Phases Defense Evasion, Installation

Operating System Refs [laaS](#)

Modified 11/10/2021, 13:10

First Seen N/A
API

Attack Pattern Description

Adversaries may disable or modify a firewall within a cloud environment to bypass controls that limit access to cloud resources. Cloud firewalls are separate from system firewalls that are described in [Disable or Modify System Firewall](https://attack.mitre.org/techniques/T1562/004).

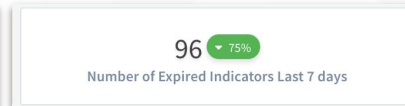
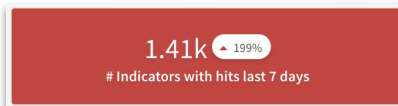
Cloud environments typically utilize restrictive security groups and firewall rules that only allow network activity from trusted IP addresses via expected ports and protocols. An adversary may introduce new firewall rules or policies

Under The Hood

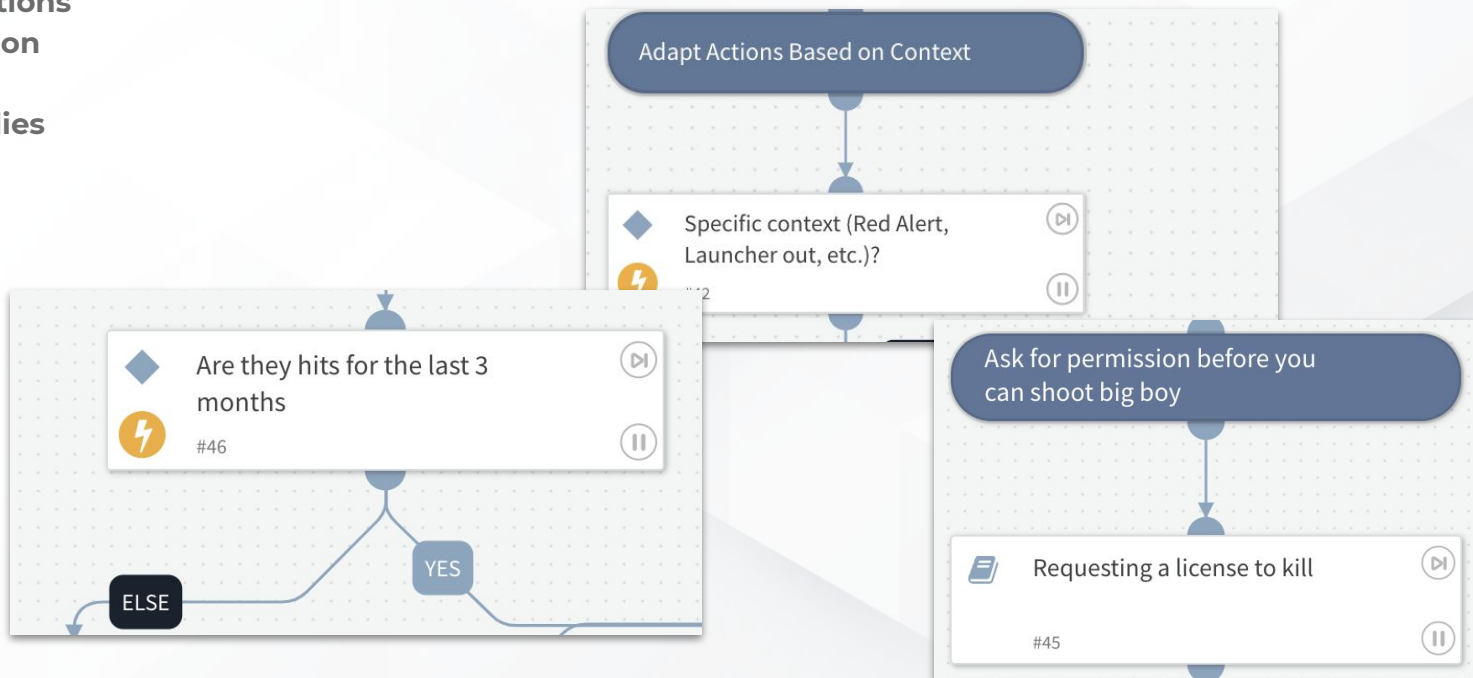
ANALYZE

Influential 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

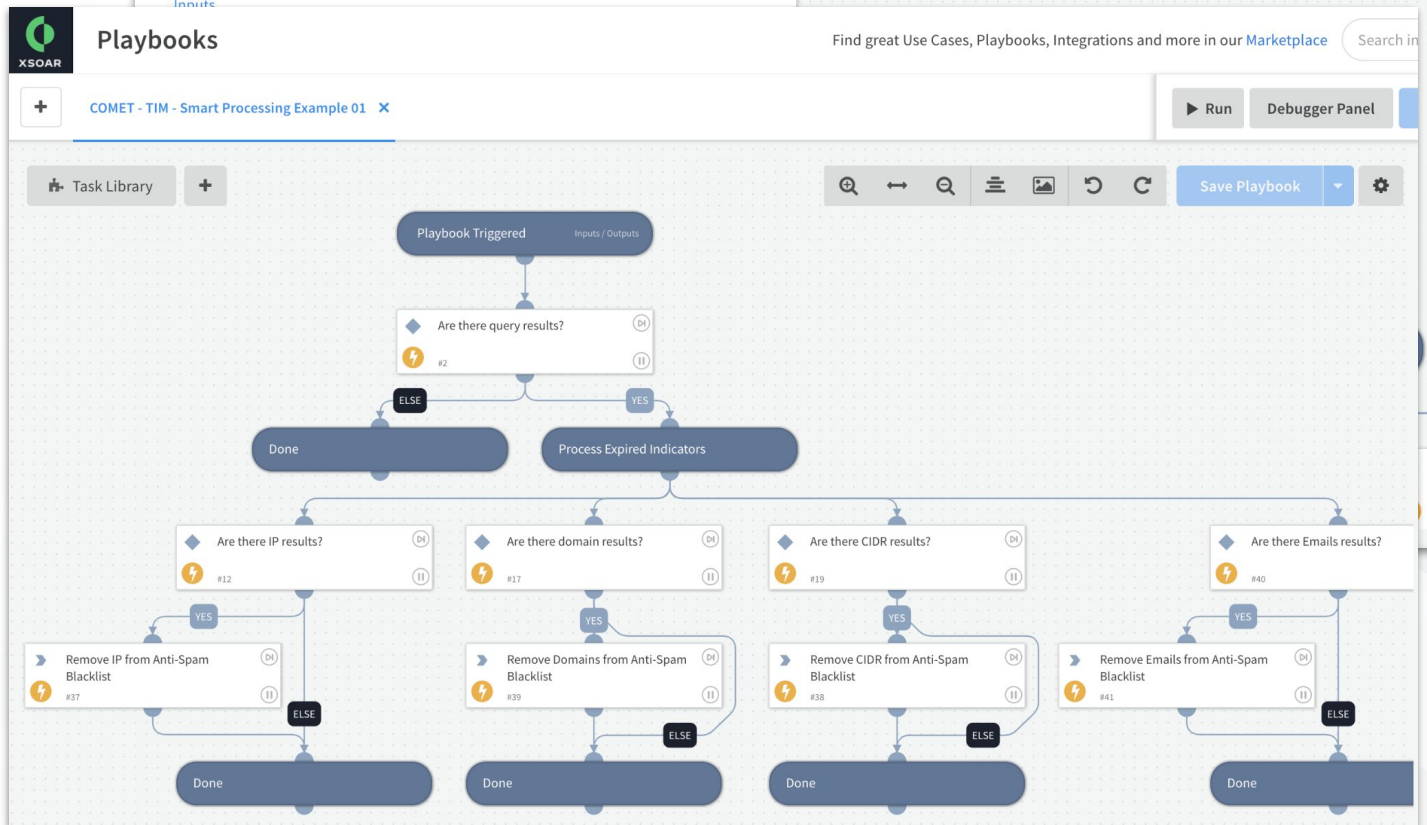


Under The Hood

ACT

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

Here how to simply purge blacklist from expired indicators.

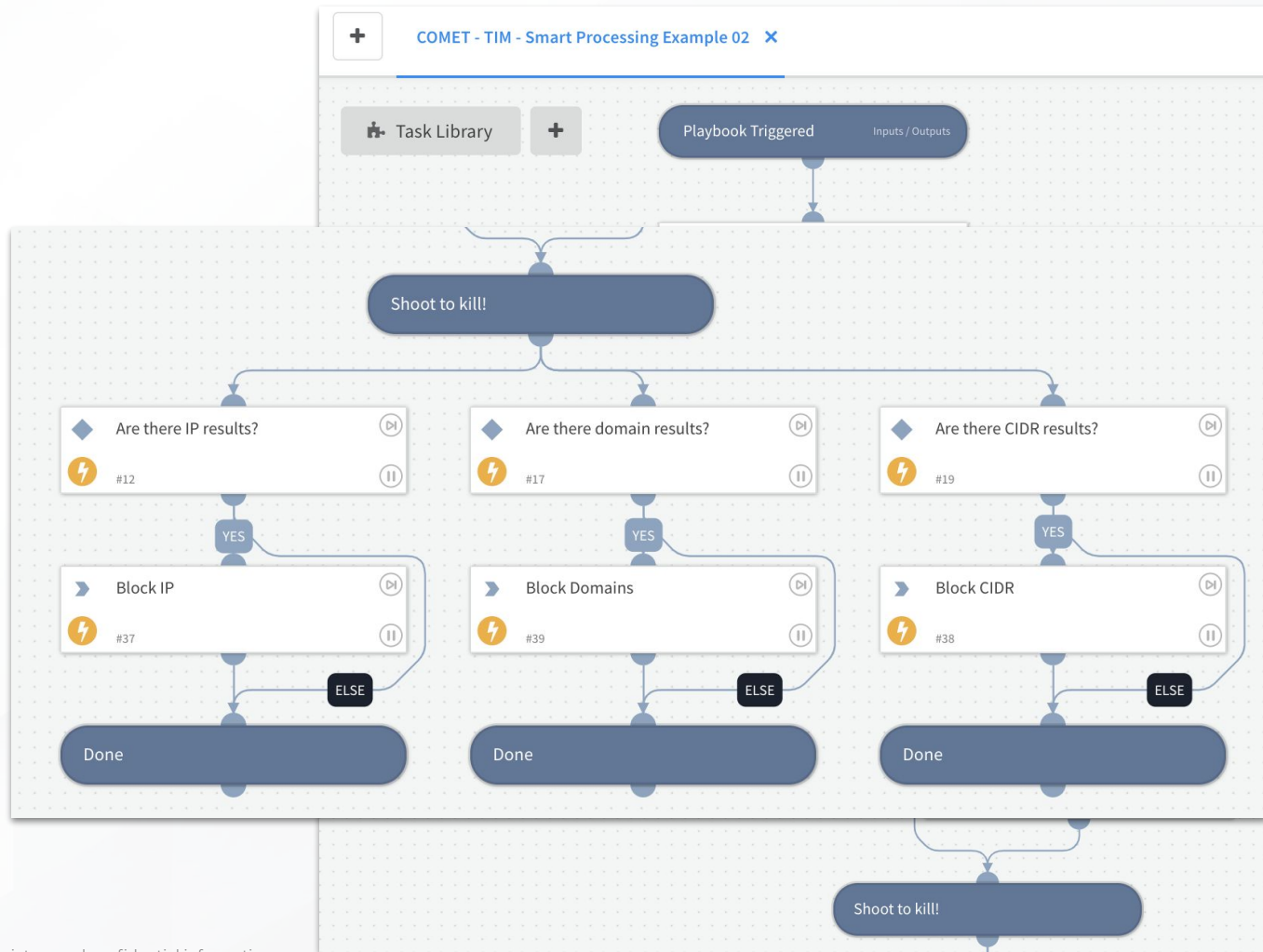


Under The Hood

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

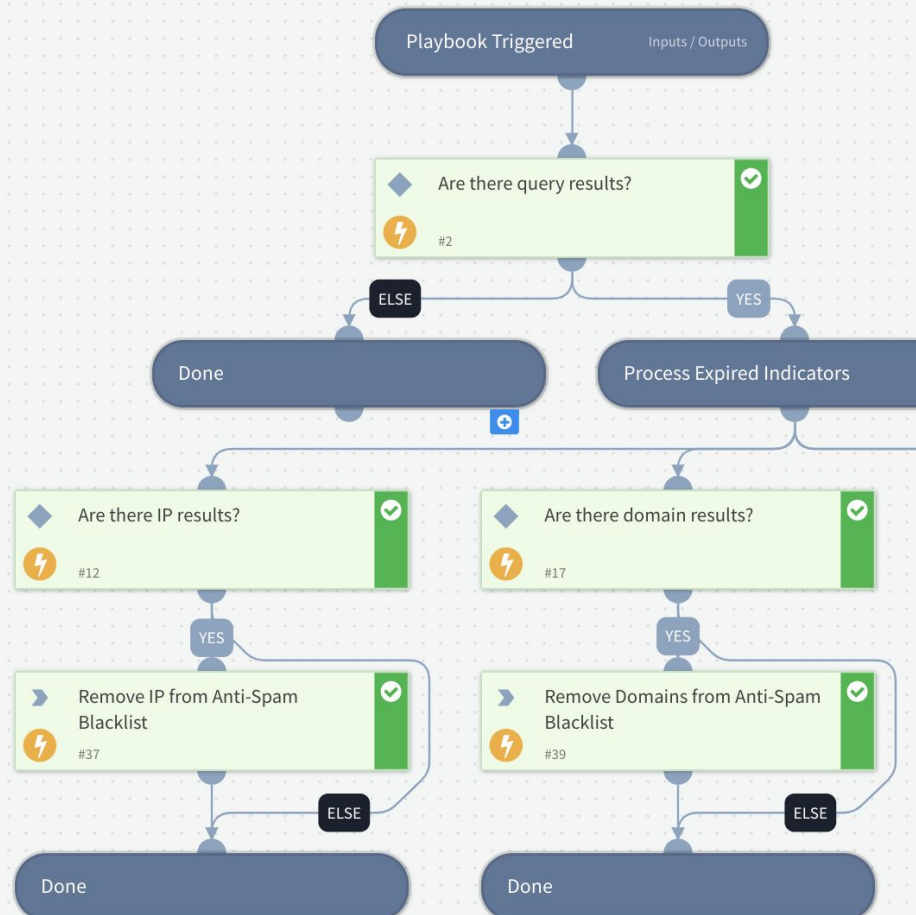
ACT

See your
Threat
Intelligence
Management
playbooks in
motion.



You're awesome!

All your tasks are done



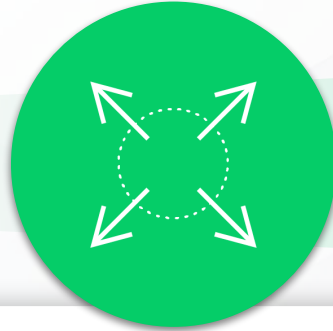


Wrap-Up

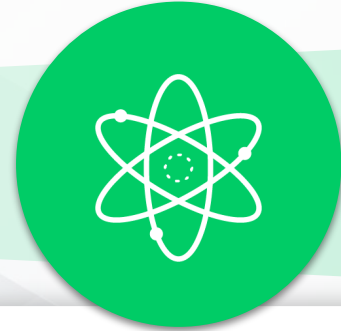
TIM or not to TIM, that should not be a question.



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

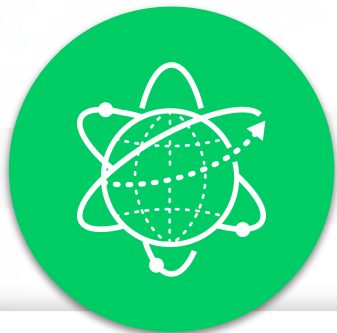


Doing something about it is even better.

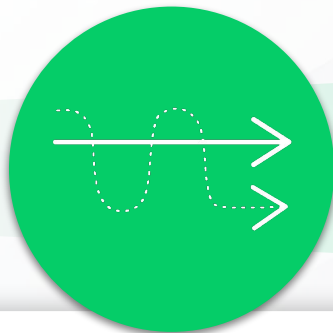


Doing something about it, while taking into account your context, is the best.

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

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





IGNITE21

WE'VE GOT NEXT

November 15-18, 2021

ignite.paloaltonetworks.com

We look forward to seeing you





Q&A



THANK YOU



paloalto[®]
NETWORKS

Cybersecurity
Partner of Choice