

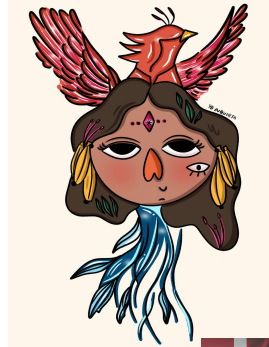
Cyber Gobierno - Tarea 1



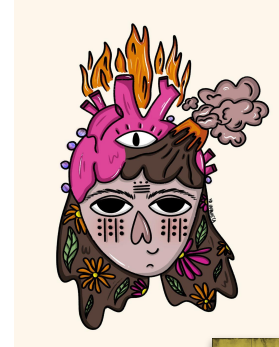
Panama



Colombia



Republica
Dominicana



Ecuador



Gobierno de seguridad

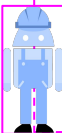
Cyber Gobierno

Inteligencia de Amenazas

Security Operations Center (SOC)

Modernizar Nuevo AI SOC

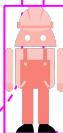
- 1 - Detección Mejorada
- 2 - Proteger contra amenazas importantes
- 3 - Automatizar la Respuesta a Incidentes con Inteligencia AI
- 4 - IT Nacional crítica que se ejecuta en plataformas digitales



Seguridad Digital

Ciberseguridad AI

Proteja la infraestructura contra malware, criptominería, denegación de servicio distribuida, API de web scraping, **envenenamiento de datos** y los nuevos ataques AI



Centro de Excelencia (CoE)

Gobernanza, procesos y habilidades necesarios para construir el **Plan de Infraestructura Crítica**

Fortalecer la gobernanza y el alcance de directrices actualizadas de **ciberseguridad**



Respuesta a Incidentes



Gobierno de Seguridad alinea con la visión de impulsar la gobernanza de la seguridad a escala, proteger la empresa, acelerar la innovación y defenderse hoy contra los ataques del mañana.



Regulaciones de Gobierno

Regulaciones Globales

Utiliza como referencia este ejemplo de Estrategia de Seguridad Nacional

Vision

Core government functions - from the delivery of public services to the operation of National Cybersecurity Plan as a sovereign nation and cementing its authority as a democratic responsible cyber power.

Goal

Governments critical functions to be significantly hardened to cyber attack by 2025, with all government organizations across the whole public sector being resilient to known vulnerabilities and attack methods no later than 2030

Pilars

Pilar 1
Build
organizational
cyber resilience

Pilar 2
Defend as one
CyberShield

Objectives

Manage cyber
security risk

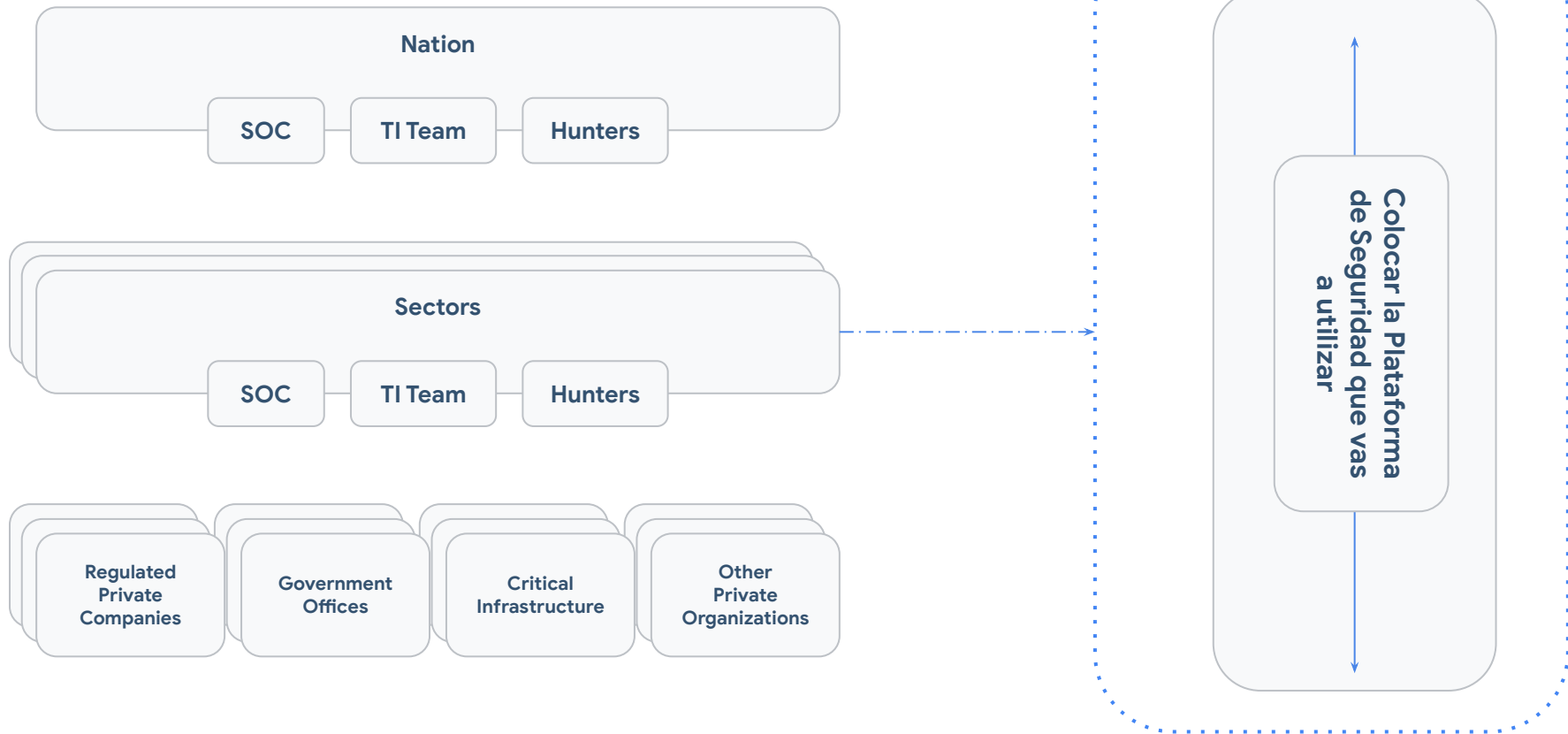
Protect against
cyber attack

Detect cyber
security events

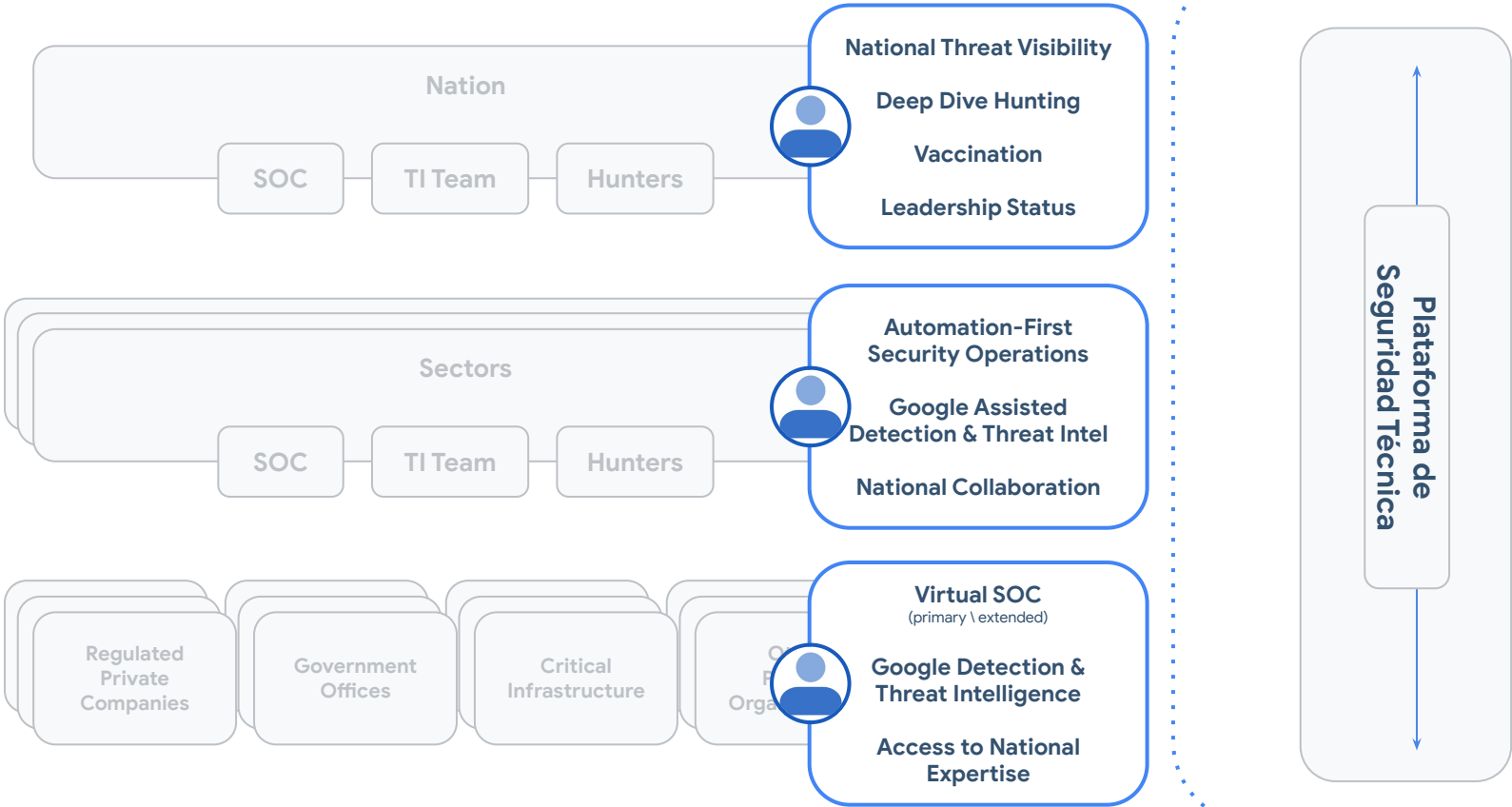
Minimize the
impact of cyber
security
incidents

Develop the
right cyber
security skills,
knowledge and
culture

1. Construye tu Plataforma Única de Seguridad Nacional de Cyber Shield



2. Selecciona Un Caso de Uso



3. Cyber Gobierno - Basado en el Caso de Uso Seleccionado construye los Componentes de tu estrategia

Plataforma

SecOps

SOC a nivel nacional
con operación
automatizada contra
principales amenazas

Seguridad Digital

Proteja los activos contra
malware, criptominería,
denegación de servicio
distribuida y más

Implementacion

Desarrollo de Capacidades

Gobernanza, procesos,
habilidades e
implementación
brindados por Google

4. Construye tu Plan a 6 Meses para Implementar tu Estrategia de CyberShield

Ejemplo de Plan a 6 Meses



CyberShield PaaS

- All-in-One
- Fully Managed
- Easy to Onboard



Sectoral SOC Implementation

- Complete Google Threat Intelligence
- Curated Detection and Response Packages
- Sectoral Hunting
- Sectoral Cyber BI



National Collaboration

- National Feeds Sharing
- National Hunting
- National Cyber BI
- Vaccination



Organization-Facing Collaboration

- Dedicated Portal
- Threats Collaboration
- Self-Service Hunting

Referencia - Plan Completo

	6 Months	9 Months	18 Months	Total
Discover phase				
Operation Model	✓	✓	✓	✓
Gather specific requirements	✓	✓	✓	✓
3rd parties tools	X	✓	✓	✓
Support Legal Documentation	✓	✓	✓	✓
Platform Setup				
SIEM+SOAR	✓	✓	✓	✓
Forwarder layer	✓	✓	✓	✓
Managed content readiness	X	✓	✓	✓
Connecting Customers				
NSOC	1	✓	✓	✓
Sector SOC	2	10	Customer Self Service	12
Organizations	4	40	Customer Self Service	44
Content				
SIEM - Source Types	6 (OOB Parsers)	Custom Parsers 5	Custom Parsers 5	10
SIEM Rules	Baseline Rules	Mandiant's Advanced Rules	Threat Hunting	N/A
SOAR Use Cases	5	15	20	40
Enablement				
Training	Basics	Advanced	Advanced	6
Documentation	basic	Advanced	Advanced	✓
Enablement	X	OJT	Self Onboarding	✓
Maintenance				
Use Cases	X	✓	✓	✓
SIEM Rules	X	✓	✓	✓

Ejemplos de Reportes en Tiempo Real
integrando toda la información de SOC's y las
Plataformas de Seguridad. Sólo para
referencia del alcance que puede tener
construir una solución completa de
CyberShield



National SOC

Situational Awareness

Threats



15
Critical

82
High

24
Medium - Low

National Health



Financial Sector



Energy Sector



Communication Sector



Health Sector



Industrial Sector



Transportation Sector



Agriculture Sector

Data Analyzed Today

4.9 TB

Active Vaccinations

Employee Data Uploads



69

Domains Observed In DarkWeb



52

Lookalike Phishing Domain







46

Phishing Campaign



46

⋮ Last Seen Actors

Actor \ Campaign	Financial Sector	Energy Sector	Agriculture Sector	Transportation Sector
 BlackBasta Group NEW	Active	0	0	0
 DragonRage Group	0	0	Cleared	Cleared
 Spear Phishing Campaign	0	Cleared	0	0
 Demon Group	0	0	Cleared	0

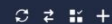
⋮ Active Threats

Threat	Trend	
 Ransomware Attack	↑ Up	
 Leaked Company Information	↓ Down	
 Exposed Employee Credentials	↓ Down	

National Vaccination Library



Released Vaccinations



Company Data In Darknet

Sensitive File Exposed (VirusTotal Detection) (v.3)



Created By NSOC

Detects exposed organization files and automates the investigation and escalation flow.



T46 Ex-filtration Campaign

T46 Ex-filtration Campaign (v.3)



Created By NSOC

Detects outbound connections with suspicious behavior (T46) and automates the investigation and escalation flow.



OM Spear Phishing

Malicious Emails (v.1)



Created By NSOC

Automated emails investigation with specific OM Spear Phishing Campaign indicators and triggers a containment flow.



Sensitive File Exposed

Sensitive File Exposed (VirusTotal Detection) (v.3)



Created By NSOC

Detects exposed organization files and automates the investigation and escalation flow.



T46 Ex-filtration Campaign

T46 Ex-filtration Campaign (v.3)



Created By NSOC

Detects outbound connections with suspicious behavior (T46) and automates the investigation and escalation flow.



OM Spear Phishing

Malicious Emails (v.1)



Created By NSOC

Automated emails investigation with specific OM Spear Phishing Campaign indicators and triggers a containment flow.



Sensitive File Exposed



T46 Ex-filtration Campaign



OM Spear Phishing

11 Cases

Clear all < 1-8 of 11 >

- ORG3** BlackBasta Ransomware IOC
26/06/2023 02:45 AM ID498
 Assigned To Sector
- ORG3** BlackBasta Ransomware IOC
26/06/2023 01:01 AM ID491
 Assigned To Sector
- ORG3** BlackBasta Ransomware IOC
26/06/2023 01:01 AM ID490
 Assigned To Sector
- ORG5** BlackBasta Ransomware IOC
26/06/2023 00:45 AM ID488
 Assigned To Sector
- GPL** BlackBasta Ransomware IOC
26/06/2023 00:40 AM ID487
 Assigned To Sector
- ORG3** BlackBasta Ransomware IOC
26/06/2023 00:39 AM ID480
 Assigned To Sector
- ORG9** BlackBasta Ransomware IOC
26/06/2023 00:22 AM ID479
 Assigned To Sector
- ORG5** BlackBasta Ransomware IOC
26/06/2023 00:21 AM ID478
 Assigned To Sector

1. BlackBasta Ransomware IOC...
19/12/2020 15:45 PM

OVERVIEW EVENTS (15) PLAYBOOKS

SECURITY ANALYST

Hello Sector F Security Analyst! Here's What We Found:

CHRONICLE DUET AI ⓘ

Last update: 5 min ago



AI Reasoning

- VirusTotal** - Strong indication on BlackBasta ransomware spread
- Mandiant** - Detected based on recent MATI feed

- Chronicle Analytics** - The activity looks like a wide occurrence
- Mandiant Hunt** - Multiple patterns that indicate ransomware distribution

What Actually Happened?

Multiple assets within the organization have communicated with domains that were found to spread the BlackBasta ransomware in private sector organizations.

The Next Steps You Should Take

- Block all connections the relevant IOCs
- Isolate infected hosts

CHRONICLE AUTO-HUNT



Chronicle IOCs Auto-Hunt

SIEM Link: <https://org.chornicle.com/search/933258772>

Reviewed 1.4 Petabytes

Hunting Summary

The hunting process extended the list of BlackBasta

Findings

The following artifacts should be immediately

MANDIANT PERSONALIZED REPORT



BlackBasta Report (for Sector F)

Full Report: <https://mandiant.com/report/BlackBasta/>

Description

The group executes ransomware and exfiltrates sensitive data, operating a cybercrime marketplace to publicly release it should a victim fail to pay a ransom

TTPs

For your type of organization we recommend to look on the following behaviors to find the full scope of the threat:

LOGS INGESTION

GOOGLE FEEDS

ADDITIONAL FEEDS

GOOGLE CURATED DETECTIONS

Financial Sector (22 Organizations)

Live

0.9 terabyte / day



GPL Banking

Live

0.4 terabyte / day



MTO Financial

Live

0.2 terabyte / day



Jobs & Careers LTD

Live

0.1 terabyte / day



CHASM International Banking

Live

0.2 terabyte / day

[View More](#)

Energy Sector (10 Organizations)

Live

1.2 terabyte / day

Industrial Sector (97 Organizations)

Live

0.7 terabyte / day

LOGS INGESTION

GOOGLE FEEDS

ADDITIONAL FEEDS

GOOGLE CURATED DETECTIONS



GCTI

Google Threat Detection

Rule sets in the Windows Threats category help identify threats in Microsoft Windows environments using Endpoint Detection and Response (EDR) logs.

Settings

Broad Rules ☒ OnPrecise Rules ☒ On


COVERAGE

MITRE Coverage

Tactics

TA0002 Execution  TA0002 Persistence  TA0005 Defense Evasion  TA0011 Command and Control 

Techniques

T12027 Obfuscated Files or Information  T1036.003 Rename System Utilities  T1059.001 PowerShell  +20

Mandiant

AI Driven Threat Detection

This pack contains rules derived from Mandiant Managed Defense's investigation and response to active incidents across the world. The rules cover Tactics and Techniques that are observed early in the attack chain, such as Initial Compromise, Execution, and Defense Evasion.

Settings

Broad Rules ☒ OnPrecise Rules ☒ On




COVERAGE

MITRE Coverage

Tactics

TA0002 Execution  TA0002 Persistence  TA0005 Defense Evasion  TA0011 Command and Control 

Techniques

T12027 Obfuscated Files or Information  T1036.003 Rename System Utilities  T1059.001 PowerShell  +26

GCTI

UEBA Threat Detection

These rule sets help identify threats in Google Cloud environments using Cloud Audit Logs. Including: Admin Action, Cloud Hacktool, Cloud SQL Ransom, IAM Abuse, Potential Ex-filtration Activity, Resource Masquerading, Service Disruption, Suspicious Behavior, Suspicious Infrastructure Change.

Settings

Broad Rules ☒ OnPrecise Rules ☒ On

COVERAGE

MITRE Coverage

Tactics

TA0002 Execution  TA0002 Persistence  TA0005 Defense Evasion  TA0011 Command and Control 

Techniques

T12027 Obfuscated Files or Information  T1036.003 Rename System Utilities  T1059.001 PowerShell  +34

Mandiant

OT Threat Detection

This pack contains rules derived from Mandiant Managed Defense's investigation and response to active incidents across the world. The rules cover Tactics and Techniques that are observed early in the attack chain.

COVERAGE

MITRE Coverage

Tactics



LOGS INGESTION

GOOGLE FEEDS

ADDITIONAL FEEDS

GOOGLE CURATED DETECTIONS

Virus Total Threat Intelligence

VirusTotal data provides a wealth of information that can be used to contextually enhance threat detections.

Enable Feed ☐ Off

Google Safe Browsing Data

Safe Browsing helps protect over five billion devices by warning users when they attempt to navigate to dangerous sites or download dangerous files. Using Safe Browsing data users are able to create high fidelity detection based on IOCs.

Enable Feed ☒ On

Google GCTI Threat Intelligence

Drive better detections with high quality, actionable, out-of-the-box threat detection content curated, built, and maintained by Google Cloud Threat Intelligence researchers.

Enable Feed ☒ On

Mandiant Threat Intelligence

Understand and proactively protect against threat actors targeting you and your peers. Get critical insights into the latest relevant threats as Mandiant blends open-source data with proprietary front-line observations.

Enable Feed ☒ On

WHOIS Data

Querying databases that store an Internet resource's registered users or assignees.

Thank you

