Retos de la Automatización del Threat Hunting

BLUE HAT CERT

Ramiro.Pulgar@bluehatcorp.com

@milovisho

+593 99 275 1705

$ telnet ceo.bluehatcorp.com 27701
ramiro@bluehatcorp> whoami

- Consultor Ciberseguridad
- Certificaciones:
  - (ISC)² CISSP
  - CSA CCSK
  - PCI SSC
    - PCI Professional (PCIP)
    - PCI Internal Security Assessor (PCI ISA)
  - PECB:
    - ISO 27001 Master
    - ISO 27005 Senior Lead Risk Manager
    - ISO 27032 Senior Lead Cybersecurity Manager
    - ISO 27035 Senior Lead Incident Manager
  - EC-Council:
    - LPT, CCISO, ECSA, CEH, CHFI, ECIH, EDRP
- Miembro:
  - OWASP – Open Web Application Security Project
  - ISACA
  - ISA – International Society of Automation
  - ACFE – Asociation of Certified Fraud Examiners
  - HTCIA – High Technology Crime Investigation Association
  - PMI - Project Management Institute

Ciberseguridad basado en Riesgos

- **Seguridad en TI**

  ISO 27033: El proceso de tomar medidas preventivas físicas y de software para proteger la infraestructura de TI del acceso no autorizado, mal uso, mal funcionamiento, modificación, destrucción o divulgación indebida, creando así una plataforma segura para que las computadoras, los usuarios y los programas realicen sus funciones críticas permitidas dentro de un entorno seguro.

- Seguridad de la Información

  ISO 27001: Preservación de la confidencialidad, integridad y disponibilidad de la información

- Riesgo

  ISO 31000: Efecto de la incertidumbre sobre los objetivos

- Ciberseguridad

  ISO 27032: Preservación de la confidencialidad, integridad y disponibilidad de la información en el ciberespacio

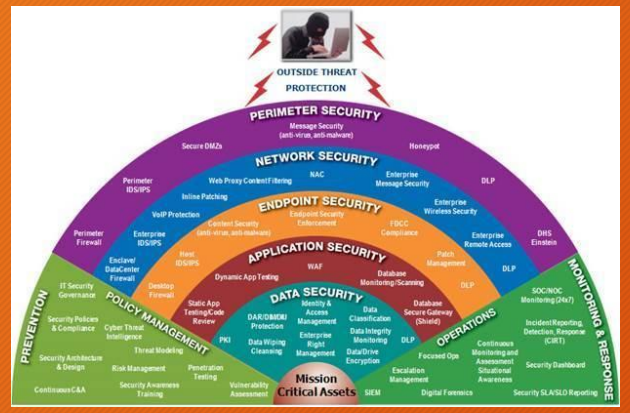
- Ciberseguridad (actual)

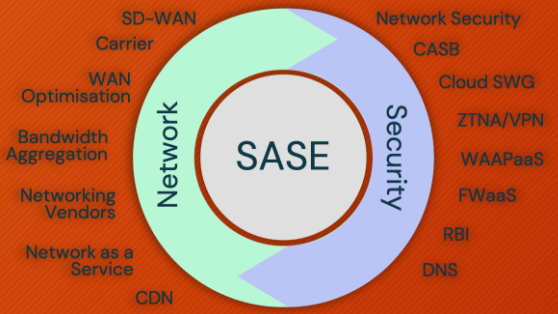
  ISO 27100: Mantener los ciber-riesgos a un nivel tolerable, a las personas, la sociedad, las organizaciones y las naciones

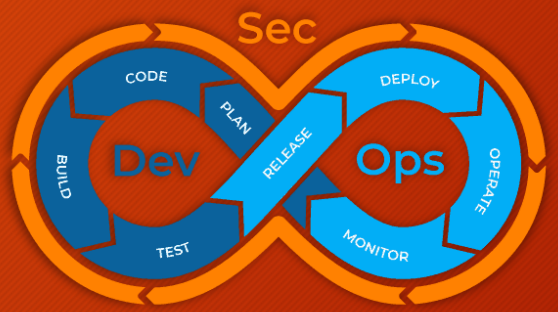
Retos de la Automatización del Threat Hunting

1. Tener claro los Activos Críticos de la Organización o Comunidad Objetivo.

Retos de Arquitectura de Seguridad



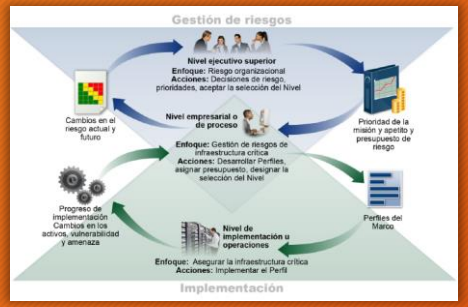




Retos de la Automatización del Threat Hunting

1. Tener claro los Activos Críticos **DE** la Organización o Comunidad Objetivo
2. Tener claro el Alcance y la Arquitectura de la infraestructura de TI

NIST Cybersecurity Framework



Identificador único de función	Función	Identificador único de categoría	Categoría
ID	Identificar	ID.AM	Gestión de activos
		ID.BE	Entorno empresarial
		ID.GV	Gobernanza
		ID.RA	Evaluación de riesgos
		ID.RM	Estrategia de gestión de riesgos
		ID.SC	Gestión del riesgo de la cadena de suministro
PR	Proteger	PR.AC	Gestión de identidad y control de acceso
		PR.AT	Conciencia y capacitación
		PR.DS	Seguridad de datos
		PR.IP	Procesos y procedimientos de protección de la información
		PR.MA	Mantenimiento
		PR.PT	Tecnología protectora
DE	Detectar	DE.AE	Anomalías y eventos
		DE.CM	Vigilancia continua de seguridad
		DE.DP	Procesos de detección
RS	Responder	RS.RP	Planificación de respuesta
		RS.CO	Comunicaciones
		RS.AN	Análisis
		RS.MI	Mitigación
		RS.IM	Mejoras
RC	Recuperar	RC.RP	Planificación de recuperación
		RC.IM	Mejoras
		RC.CO	Comunicaciones

General Risk Frameworks and Methods

Generic Frameworks for Cyber Risk Management

- NIST Cybersecurity Framework
- NIST SP 800-39
- COBIT

Risk Modeling Frameworks

- NIST SP 800-30
- CBEST
- FFIEC Cybersecurity Assessment Tool
- RiskIT

General Cyber Threat Modeling Frameworks and Methods

Threat Modeling Frameworks

- ODNI Cyber Threat Framework
- Cyber Prep 2.0 / DACS
- Attack tree modeling
- Cyber attack lifecycle modeling

Modeling to Support Design Analysis & Testing

- STRIDE & DREAD
- NIST SP 800-154
- OCTAVE
- Intel's TARA / TAL

Threat Modeling Resources Oriented to Enterprise IT

Tactics, Techniques, and Procedures-Oriented

- NIST SP 800-30 list of threat events
- ATT&CK™
- CAPEC™
- MITRE's TARA

Technology-Oriented

- Web Application threat models and methods – OWASP, PASTA
- Threat modeling for cloud computing

NIST CSF - Componentes - Perfiles

Retos de la Automatización del Threat Hunting

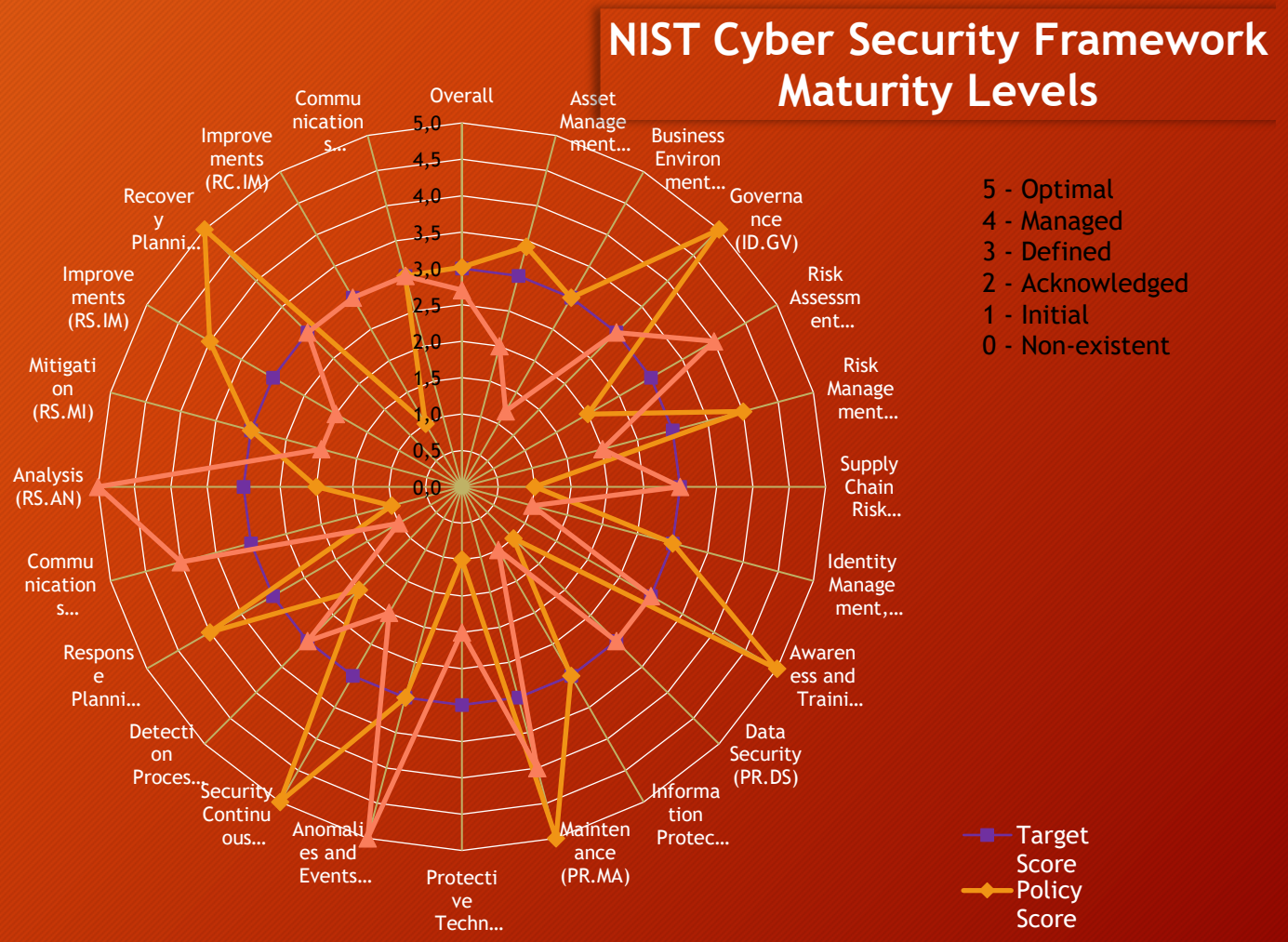
1. Tener claro los Activos Críticos **DE** la Organización o Comunidad Objetivo
2. Tener claro el Alcance y la Arquitectura de la infraestructura de TI
3.
4.
5. Tener claro los Riesgos sobre los activos críticos

NIST Cybersecurity Framework 1.1

Function	Category	Subcategory	Informative References	Policy Maturity	Practice Maturity
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried	· **CIS CSC** 1 · **COBIT 5** BAI09.01, BAI09.02 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISA 62443-3-3:2013** SR 7.8 · **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 · **NIST SP 800-53 Rev. 4** CM-8, PM-5	4.3	2.0
		ID.AM-2: Software platforms and applications within the organization are inventoried	· **CIS CSC** 2 · **COBIT 5** BAI09.01, BAI09.02, BAI09.05 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISA 62443-3-3:2013** SR 7.8 · **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2, A.12.5.1 · **NIST SP 800-53 Rev. 4** CM-8, PM-5	4.0	2.0
		ID.AM-3: Organizational communication and data flows are mapped	· **CIS CSC** 12 · **COBIT 5** DSS05.02 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISO/IEC 27001:2013** A.13.2.1, A.13.2.2 · **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8	1.2	2.0
		ID.AM-4: External information systems are catalogued	· **CIS CSC** 12 · **COBIT 5** APO02.02, APO10.04, DSS01.02 · **ISO/IEC 27001:2013** A.11.2.6 · **NIST SP 800-53 Rev. 4** AC-20, SA-9	4.0	2.0
		ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	· **CIS CSC** 13, 14 · **COBIT 5** APO03.03, APO03.04, APO12.01, BAI04.02, BAI09.02 · **ISA 62443-2-1:2009** 4.2.3.6 · **ISO/IEC 27001:2013** A.8.2.1 · **NIST SP 800-53 Rev. 4** CP-2, RA-2, SA-14, SC-6	4.0	2.0
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	· **CIS CSC** 17, 19 · **COBIT 5** APO01.02, APO07.06, APO13.01, DSS06.03 · **ISA 62443-2-1:2009** 4.3.2.3.3 · **ISO/IEC 27001:2013** A.6.1.1 · **NIST SP 800-53 Rev. 4** CP-2, PS-7, PM-11	3.0	2.0
	Category Maturity Score			3.4	2.0
		ID.BE-1: The organization's role in the supply chain is identified and communicated	· **COBIT 5** APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 · **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 · **NIST SP 800-53 Rev. 4** CP-2, SA-12	3.0	1.0

Ciberseguridad – NIST Cybersecurity Framework 1.1

	NIST CSF Categories	Target Score	Policy Score	Practice Score
	Overall	3.00	3.02	2.70
IDENTIFY (ID)	Asset Management (ID.AM)	3.00	3.42	2.00
	Business Environment (ID.BE)	3.00	3.00	1.20
	Governance (ID.GV)	3.00	5.00	3.00
	Risk Assessment (ID.RA)	3.00	2.00	4.00
	Risk Management Strategy (ID.RM)	3.00	4.00	2.00
	Supply Chain Risk Management (ID.SC)	3.00	1.00	3.00
PROTECT (PR)	Identity Management, Authentication and Access Control (PR.AC)	3.00	3.00	1.00
	Awareness and Training (PR.AT)	3.00	5.00	3.00
	Data Security (PR.DS)	3.00	1.00	3.00
	Information Protection Processes and Procedures (PR.IP)	3.00	3.00	1.00
	Maintenance (PR.MA)	3.00	5.00	4.00
	Protective Technology (PR.PT)	3.00	1.00	2.00
DETECT (DE)	Anomalies and Events (DE.AE)	3.00	3.00	5.00
	Security Continuous Monitoring (DE.CM)	3.00	5.00	2.00
	Detection Processes (DE.DP)	3.00	2.00	3.00
RESPOND (RS)	Response Planning (RS.RP)	3.00	4.00	1.00
	Communications (RS.CO)	3.00	1.00	4.00
	Analysis (RS.AN)	3.00	2.00	5.00
	Mitigation (RS.MI)	3.00	3.00	2.00
	Improvements (RS.IM)	3.00	4.00	2.00
RECOVER (RC)	Recovery Planning (RC.RP)	3.00	5.00	3.00
	Improvements (RC.IM)	3.00	1.00	3.00
	Communications (RC.CO)	3.00	3.00	3.00



Retos de la Automatización del Threat Hunting

1. Tener claro los Activos Críticos **DE** la Organización o Comunidad Objetivo
2. Tener claro el Alcance y la Arquitectura de la infraestructura de TI
3.
4.
5. Tener claro los Riesgos sobre los activos críticos
6. Proponer el mejor Tratamiento de los Riesgos

NIST CSF - Implementación

1. Priorización y definición de alcance
2. Orientación e Identificación de activos
3. Identificar la situación actual
4. Realizar un análisis de riesgos
5. Establecer objetivos
6. Determinar, analizar y priorizar las brechas detectadas
7. Implementar el plan de acción

De la Estrategia a lo Operativo

VS

ROLES Y RESPONSABILIDADES

Inicios del “Ethical Hacking”

1

Reconnaissance

Reconnaissance is nothing more than the steps taken to gather evidence and information on the targets you want to attack.

2

Scanning and Enumeration

Take the information you gathered in recon and actively apply tools and techniques to gather more in-depth information on the targets.

3

Gaining Access

In the gaining access phase, true attacksare leveled against the targets enumerated in the second phase.

4

Maintaining Access

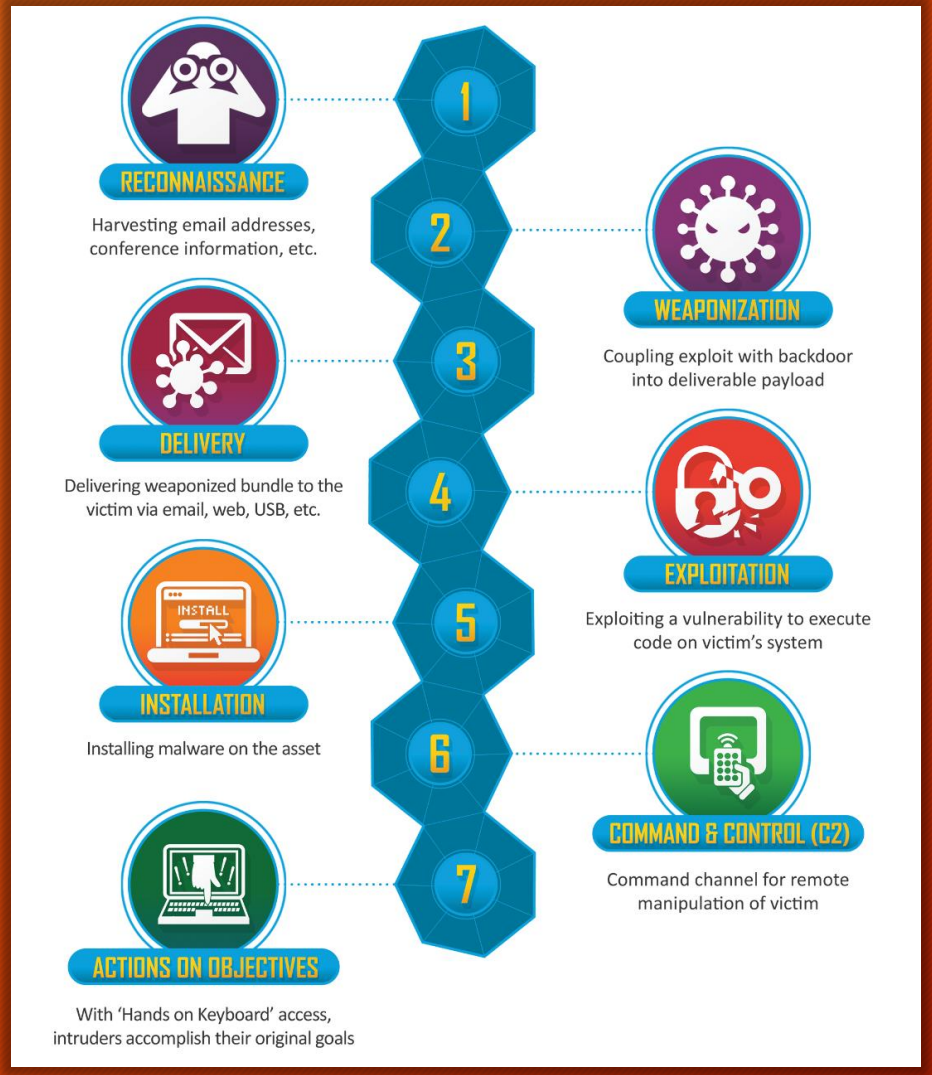
In the fourth phase, hackers attempt to ensure they have a way back into the machine or system they've already compromised.

5

Covering Tracks

In the final phase, attackers attempt to conceal their success and avoid detection by security professionals.

Cyber Kill Chain



MITRE ATT&CK

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	7 techniques	9 techniques	12 techniques	19 techniques	13 techniques	42 techniques	16 techniques	30 techniques	9 techniques	17 techniques	16 techniques	9 techniques	13 techniques
Active Scanning (3)	Acquire Infrastructure (6)	Drive-by Compromise	Command and Scripting Interpreter (8)	Account Manipulation (5)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Adversary-in-the-Middle (3)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (3)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Compromise Accounts (2)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (3)	Compromise Infrastructure (6)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (14)	Boot or Logon Autostart Execution (14)	BITS Jobs	Credentials from Password Stores (5)	Browser Bookmark Discovery	Lateral Tool Transfer	Audio Capture	Data Encoding (2)	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Data Obfuscation (3)	Exfiltration Over C2 Channel	Data Manipulation (3)
Gather Victim Org Information (4)	Establish Accounts (2)	Phishing (3)	Inter-Process Communication (3)	Browser Extensions	Create or Modify System Process (4)	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services (6)	Browser Session Hijacking	Dynamic Resolution (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Domain Policy Modification (2)	Deobfuscate/Decode Files or Information	Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Encrypted Channel (2)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Search Closed Sources (2)	Stage Capabilities (5)	Supply Chain Compromise (3)	Scheduled Task/Job (5)	Create Account (3)	Escape to Host	Deploy Container	Input Capture (4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage Object	Fallback Channels	Exfiltration Over Web Service (2)	Endpoint Denial of Service (4)
Search Open Technical Databases (5)		Trusted Relationship	Shared Modules	Create or Modify System Process (4)	Event Triggered Execution (15)	Direct Volume Access	Modify Authentication Process (5)	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository (2)	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Search Open Websites/Domains (2)		Valid Accounts (4)	Software Deployment Tools	Event Triggered Execution (15)	Exploitation for Privilege Escalation	Domain Policy Modification (2)	Multi-Factor Authentication Interception	Debugger Evasion	Use Alternate Authentication Material (4)	Data from Information Repositories (3)	Multi-Stage Channels	Transfer Data to Cloud Account	Inhibit System Recovery
Search Victim-Owned Websites			System Services (2)	External Remote Services	Hijack Execution Flow (12)	Execution Guardrails (1)	Multi-Factor Authentication Request Generation	Domain Trust Discovery		Data from Local System	Non-Application Layer Protocol		Network Denial of Service (2)
			User Execution (3)	Hijack Execution Flow (12)	Process Injection (12)	Exploitation for Defense Evasion	Network Sniffing	File and Directory Discovery		Data from Network Shared Drive	Non-Standard Port		Resource Hijacking
			Windows Management Instrumentation	Implant Internal Image	Scheduled Task/Job (5)	File and Directory Permissions Modification (2)	OS Credential Dumping (8)	Group Policy Discovery		Data from Removable Media	Protocol Tunneling		Service Stop
				Modify Authentication Process (5)	Valid Accounts (4)	Hide Artifacts (10)	Steal Application Access Token	Network Service Discovery		Data Staged (2)	Proxy (4)		System Shutdown/Reboot
				Office Application Startup (6)		Hijack Execution Flow (12)	Steal or Forge Kerberos Tickets (4)	Network Share Discovery		Email Collection (3)	Remote Access Software		
				Pre-OS Boot (5)		Impair Defenses (9)	Steal Web Session Cookie	Network Sniffing		Input Capture (4)	Traffic Signaling (1)		
				Scheduled Task/Job (5)		Indicator Removal on Host (6)	Unsecured Credentials (7)	Password Policy Discovery		Screen Capture	Web Service (3)		
				Server Software Component (5)		Indirect Command Execution		Peripheral Device Discovery		Video Capture			
				Traffic Signaling (1)		Masquerading (7)		Permission Groups Discovery (3)					
				Valid Accounts (4)		Modify Authentication Process (5)		Process Discovery					
						Modify Cloud Compute Infrastructure (4)		Query Registry					
						Modify Registry		Remote System Discovery					
						Modify System Image (2)		Software Discovery (1)					
						Network Boundary Bridging (1)		System Information Discovery					
								System Location Discovery (1)					
								System Network Configuration Discovery (1)					

Gestión de Vulnerabilidades

MITRE ATT&CK

Retos de la Automatización del Threat Hunting

1. Tener claro los Activos Críticos **DE** la Organización o Comunidad Objetivo
2. Tener claro el Alcance y la Arquitectura de la infraestructura de TI
3. Identificar las Vulnerabilidades Conocidas
4. Identificar Amenazas Conocidas
5. Tener claro los Riesgos sobre los activos críticos
6. Proponer el mejor Tratamiento de los Riesgos

Noticias de Amenazas Avanzadas

Facebook Doesn't Know What It Does With Your Data, Or Where It Goes: Leaked Document

"We do not have an adequate level of control and explainability over how our systems use data," Facebook engineers say in leaked document.

By Lorenzo Franceschi-Bicchierai April 26, 2022, 8:02am MOTHERBOARD TECH BY VICE

EL FINANCIERO

Hackeo a Hacienda: ¿qué es el 'ransomware' de Conti y cómo protegerse de ciberdelincuentes?

Por Carlos Cordero Pérez 19 de abril 2022, 8:45 AM

La advertencia de un ataque tipo *ransomware* sobre los sistemas informáticos del Ministerio de Hacienda habría activado los protocolos protección, que incluían la suspensión de los servicios en línea del sistema de la Autoridad Virtual Tributaria (ATV) y de TICA (Tecnología de Información para el Control Aduanero). Según los

Zero-day bug in uClibc library could leave IoT devices vulnerable to DNS poisoning attacks

Jessica Haworth 04 May 2022 at 14:15 UTC
Updated: 04 May 2022 at 14:23 UTC

A zero-day vulnerability in uClibc and uClibc-ng, a popular C standard library, could enable a malicious actor to launch DNS poisoning attacks on vulnerable IoT devices.

The bug, tracked as ICS-VU-638779, which has yet to be patched, could leave users exposed to attack, researchers have warned.

¿Cómo funciona Pegasus? Así infecta este software maligno los teléfonos de políticos

— Paula García Cadena SER El lunes - 10:40 h ET

Madrid • Espionajes, softwares secretos, conversaciones pinchadas... Las noticias que copan titulares estos días parecen más propias de películas que de la actualidad política.

Ukraine Says It Thwarted a Sophisticated Russian Cyberattack on Its Power Grid

April 12, 2022
Kate Conger

Officials said that if the breach had been successful, it would have deprived roughly two million people of electricity and made it difficult to restore power. Rodrigo Abd/Associated Press

Mar 17, 2021, 03:50am EDT | 5,302 views

Hackers Are Targeting U.S. Banks, And Hardware May Give Them An Open Door

Secuestro de datos en Perú y Costa Rica vaticina más problemas para la región

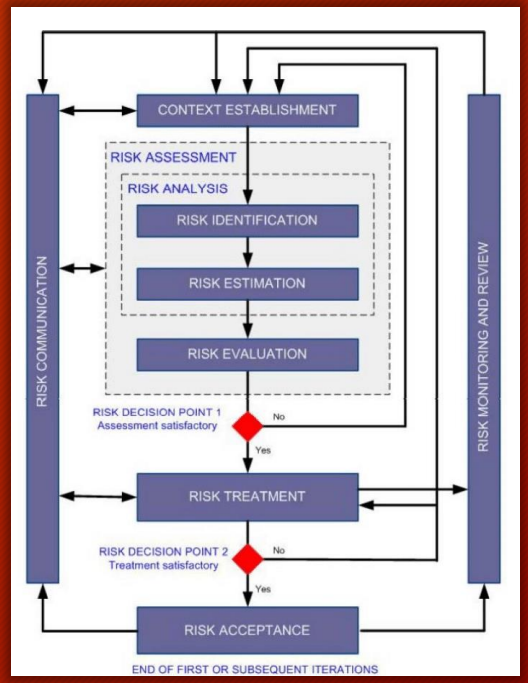
COSTA RICA | 3 MAY 2022 POR SCOTT MISTLER-FERGUSON

Un grupo de ciberdelincuentes que ha amenazado con divulgar ingentes cantidades de datos robados al gobierno de Costa Rica ahora golpeó el organismo de inteligencia de Perú, una muestra de que los gobiernos de la región siguen siendo presa fácil de los ataques de ransomware.

Identificando vulnerabilidades no conocidas

Retos de la Automatización del Threat Hunting

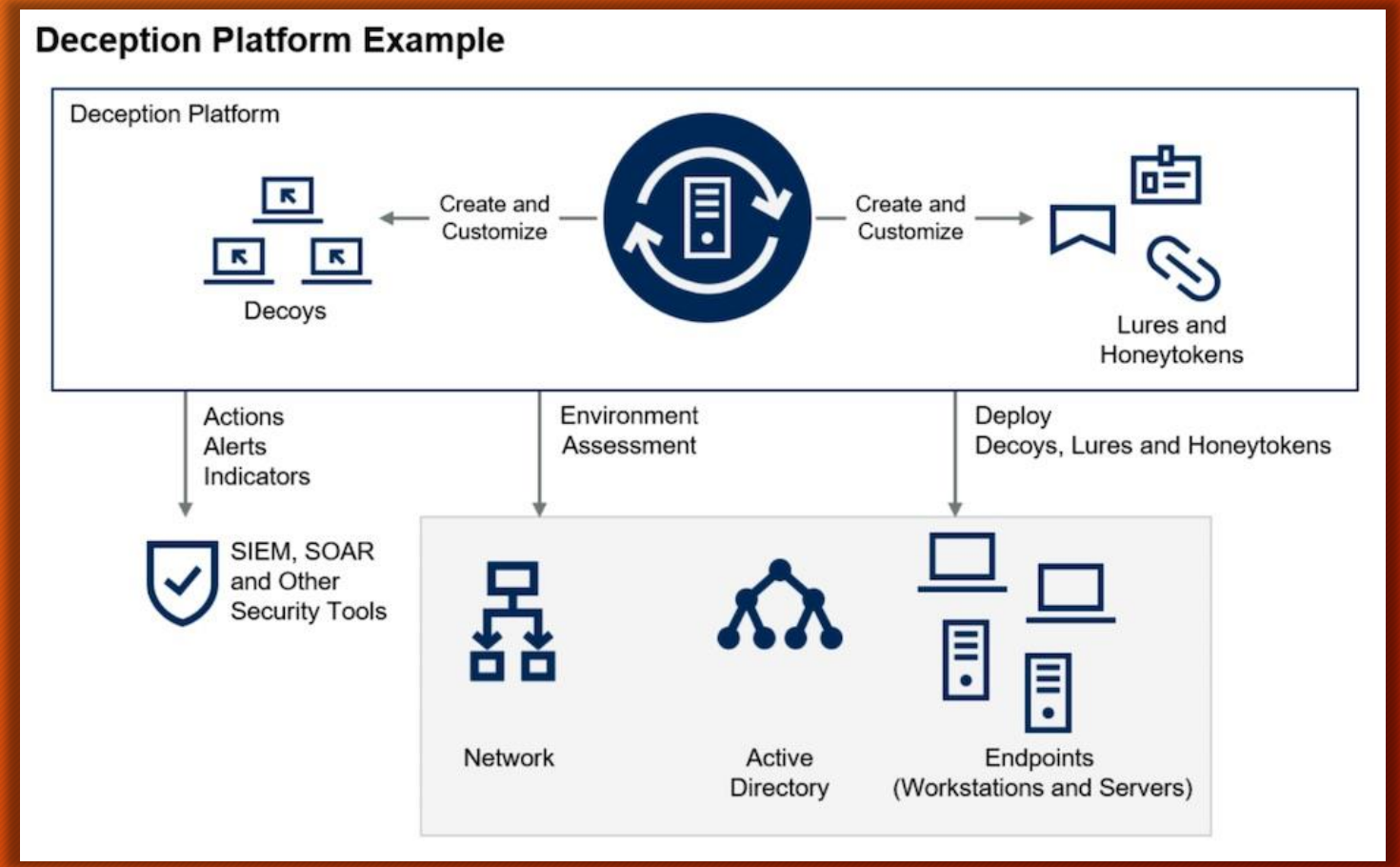
1. Tener claro los Activos Críticos **DE** la Organización o Comunidad Objetivo
2. Tener claro el Alcance y la Arquitectura de la infraestructura de TI
3. Identificar las Vulnerabilidades Conocidas y No Conocidas
4. Identificar Amenazas Conocidas
5. Tener claro los Riesgos sobre los activos críticos
6. Seleccionar el mejor Control en Tratamiento de los Riesgos



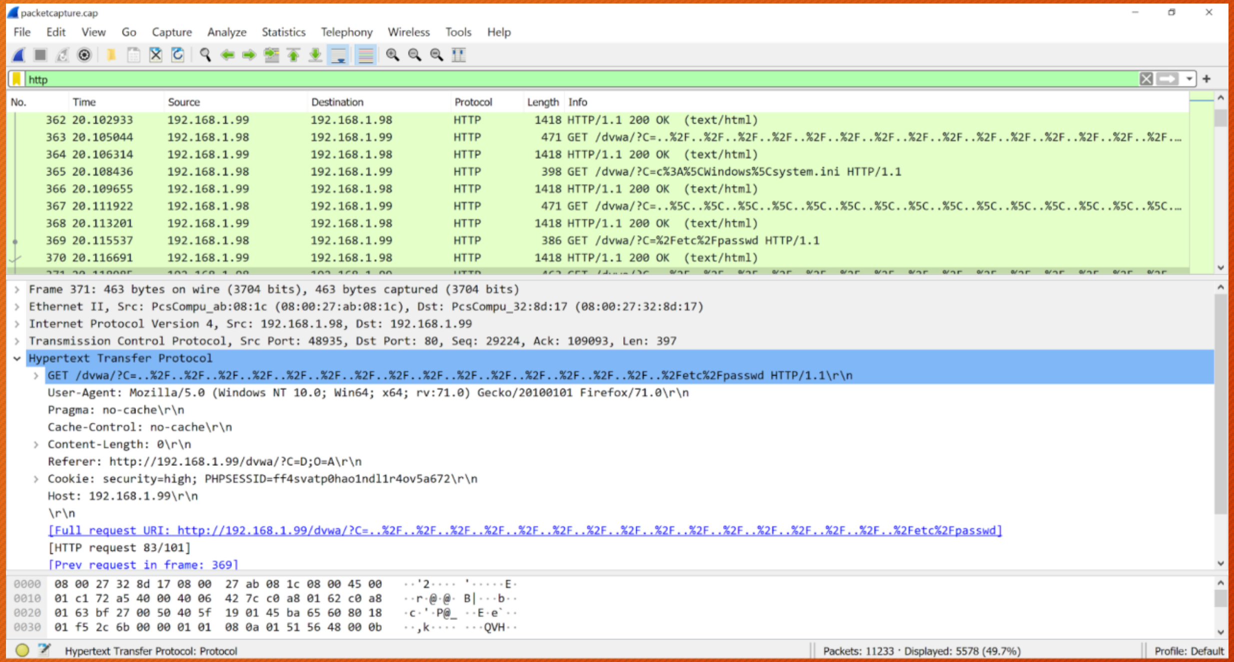
War Gaming

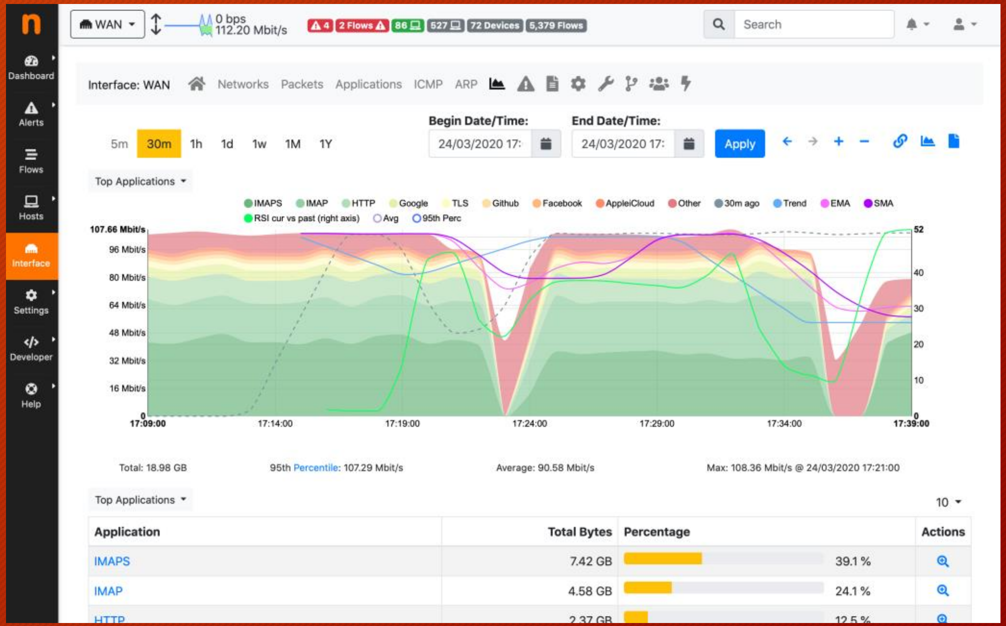

Threat Modeling to go from Reactive to Proactive
Wargaming validates controls
Operational Experience evolves threat model

Plataformas de Decepción - HonetNets



Análisis de Tráfico

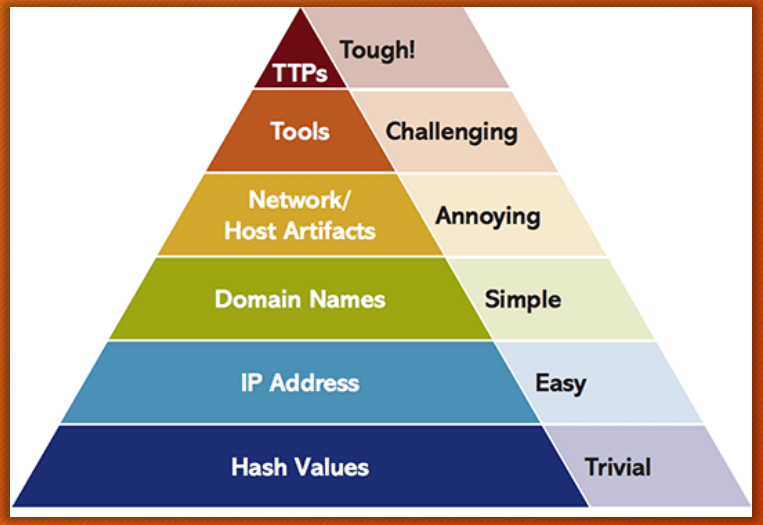


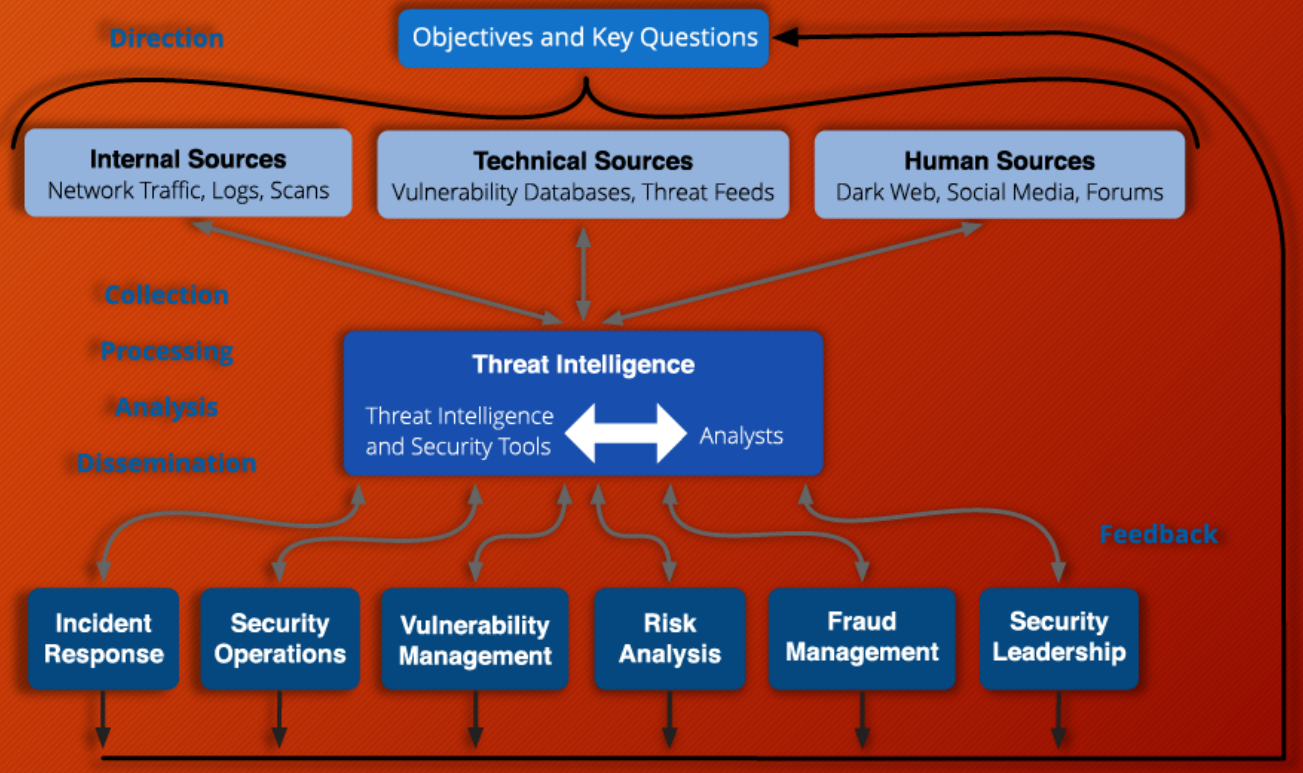


Retos de la Automatización del Threat Hunting

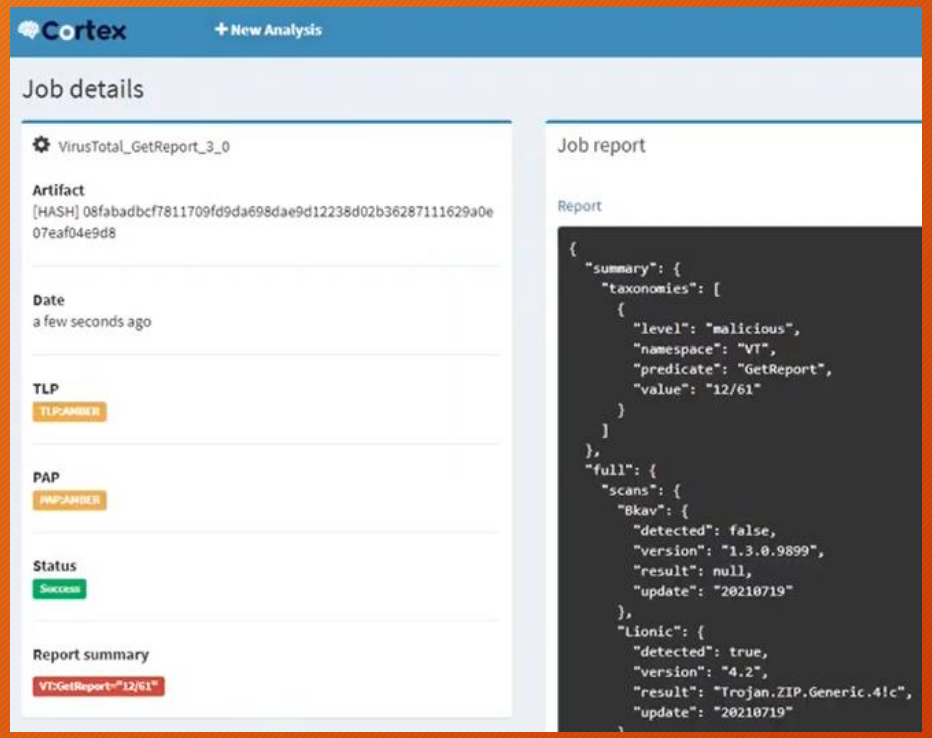
1. Tener claro los Activos Críticos **DE** la Organización o Comunidad Objetivo
2. Tener claro el Alcance y la Arquitectura de la infraestructura de TI
3. Identificar las Vulnerabilidades Conocidas y No Conocidas
4. Identificar Amenazas Conocidas y No Conocidas
   - Actividades Proactivas de Detección
5. Tener claro los Riesgos sobre los activos críticos
6. Seleccionar el mejor Control en Tratamiento de los Riesgos

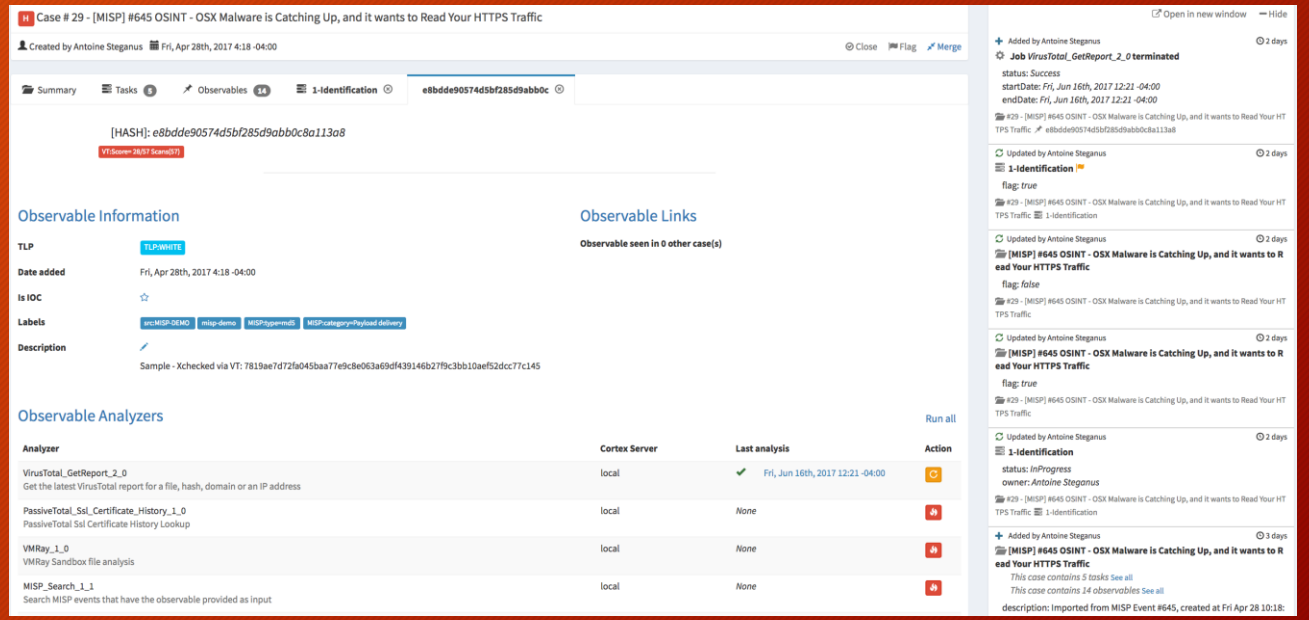
Cyber Threat Intelligence





Análisis de IoC





Compartir Información de Ciberamenazas

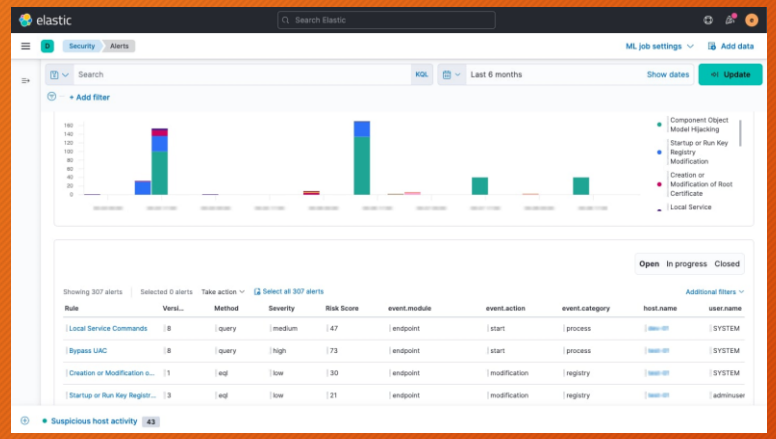
Retos de la Automatización del Threat Hunting

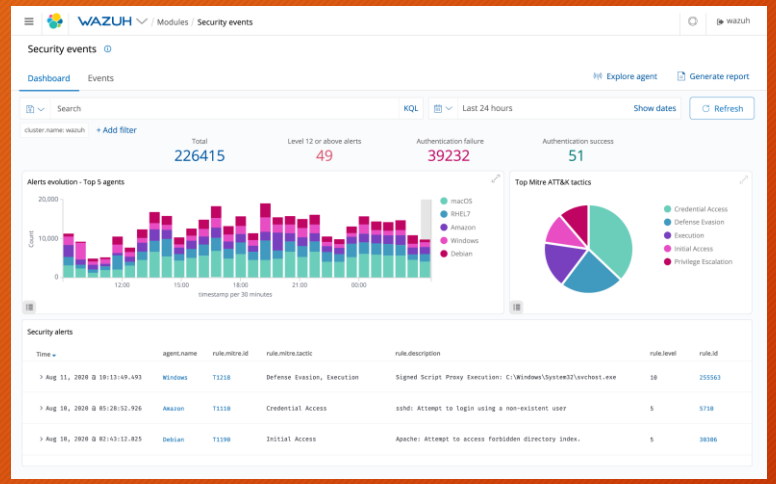
1. Tener claro los Activos Críticos **DE** la Organización o Comunidad Objetivo
2. Tener claro el Alcance y la Arquitectura de la infraestructura de TI
3. Identificar las Vulnerabilidades Conocidas y No Conocidas
4. Identificar Amenazas Conocidas y No Conocidas
   - Actividades proactivas de Detección
   - Colaboración y Compartición !!!
   - Indicadores de Compromiso
   - Indicadores de Amenaza
5. Tener claro los Riesgos sobre los activos críticos
6. Seleccionar el mejor Control en Tratamiento de los Riesgos

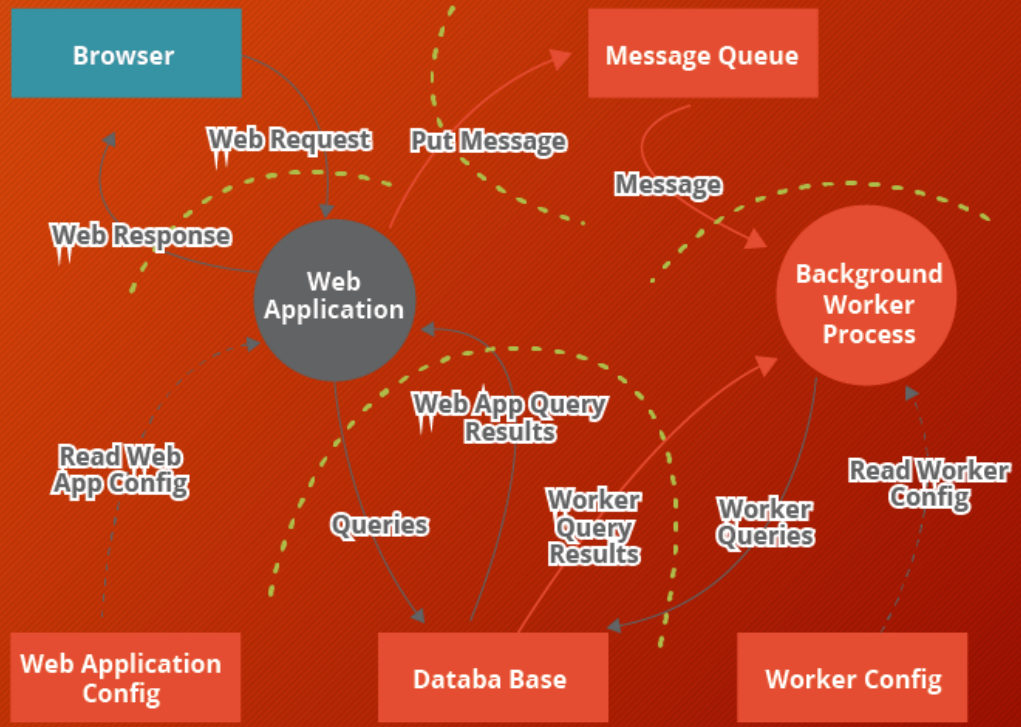
NIST CSF y CIS Controls

Identificador único de función	Función	Identificador único de categoría	Categoría
ID	Identificar	ID.AM	Gestión de activos
		ID.BE	Entorno empresarial
		ID.GV	Gobernanza
		ID.RA	Evaluación de riesgos
		ID.RM	Estrategia de gestión de riesgos
		ID.SC	Gestión del riesgo de la cadena de suministro
PR	Proteger	PR.AC	Gestión de identidad y control de acceso
		PR.AT	Conciencia y capacitación
		PR.DS	Seguridad de datos
		PR.IP	Procesos y procedimientos de protección de la información
		PR.MA	Mantenimiento
		PR.PT	Tecnología protectora
DE	Detectar	DE.AE	Anomalías y eventos
		DE.CM	Vigilancia continua de seguridad
		DE.DP	Procesos de detección
RS	Responder	RS.RP	Planificación de respuesta
		RS.CO	Comunicaciones
		RS.AN	Análisis
		RS.MI	Mitigación
		RS.IM	Mejoras
RC	Recuperar	RC.RP	Planificación de recuperación
		RC.IM	Mejoras
		RC.CO	Comunicaciones

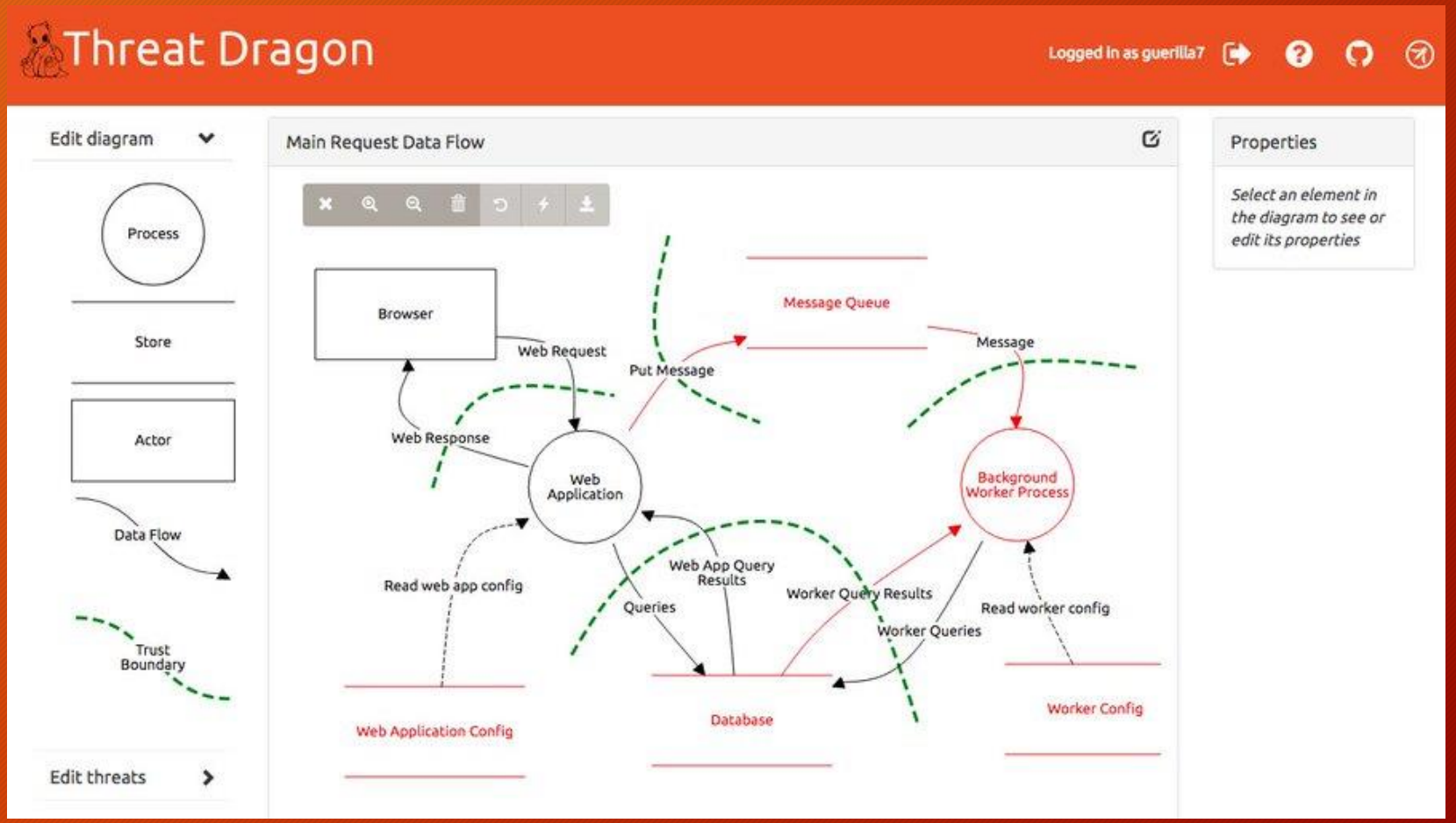
Monitoreo de Amenazas Reales



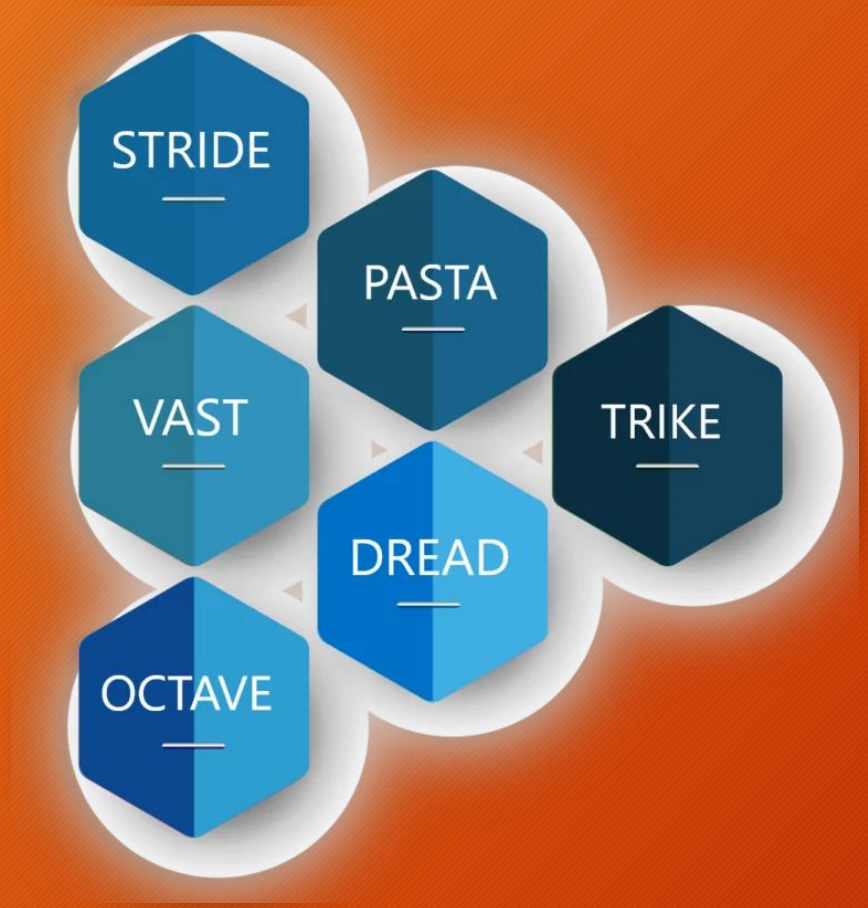




Monitoreo de Amenazas



Modelamiento de Amenazas



Stages of Process for Attack Simulation & Threat Analysis (PASTA)

Retos de la Automatización del Threat Hunting

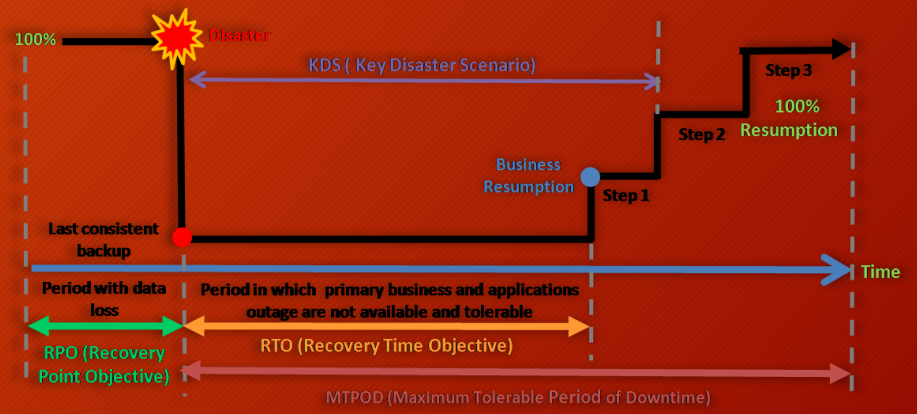
1. Tener claro los Activos Críticos **DE** la Organización o Comunidad Objetivo
2. Tener claro el Alcance y la Arquitectura de la infraestructura de TI
3. Identificar las Vulnerabilidades Conocidas y No Conocidas
4. Identificar Amenazas Conocidas y No Conocidas
5. Tener claro los Riesgos sobre los activos críticos
6. Seleccionar el mejor Control en Tratamiento de los Riesgos
7. Detectar Amenazas

Manejo de Incidentes – NIST 800-61

Identificador único de función	Función	Identificador único de categoría	Categoría
ID	Identificar	ID.AM	Gestión de activos
		ID.BE	Entorno empresarial
		ID.GV	Gobernanza
		ID.RA	Evaluación de riesgos
		ID.RM	Estrategia de gestión de riesgos
		ID.SC	Gestión del riesgo de la cadena de suministro
PR	Proteger	PR.AC	Gestión de identidad y control de acceso
		PR.AT	Conciencia y capacitación
		PR.DS	Seguridad de datos
		PR.IP	Procesos y procedimientos de protección de la información
		PR.MA	Mantenimiento
		PR.PT	Tecnología protectora
DE	Detectar	DE.AE	Anomalías y eventos
		DE.CM	Vigilancia continua de seguridad
		DE.DP	Procesos de detección
RS	Responder	RS.RP	Planificación de respuesta
		RS.CO	Comunicaciones
		RS.AN	Análisis
		RS.MI	Mitigación
		RS.IM	Mejoras
RC	Recuperar	RC.RP	Planificación de recuperación
		RC.IM	Mejoras
		RC.CO	Comunicaciones

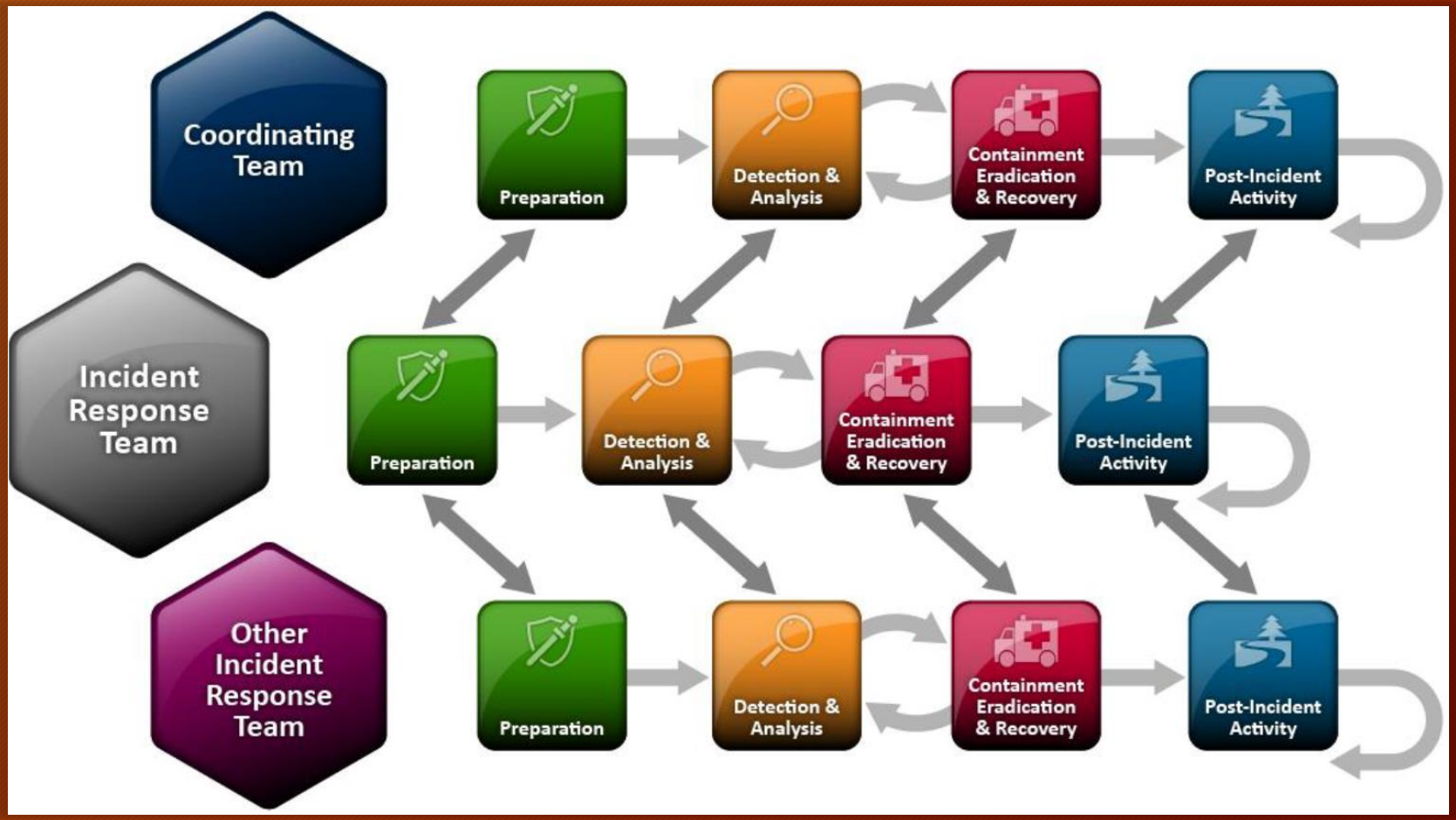
REGISTRAR INC.

SIMULACÌÓN



MEJORAR MÉTRICAS, PROCEDIMIENTOS Y RTO

Manejo de Incidentes entre CSIRTs



Reto: Co-Administración

Queries | Last 7 Days | Enter search query (Ctrl+F)

Time	Origin	Source	Source User...	Destination	Service	Ac...	Access Rule N...	Policy...	Description
Today, 7:29:27 PM	myngfw	asa-172.17.78.1...		asa-172.17.23.1...	http (TCP/80)	1	asa-accept-172....	Standard	http Traffic Dropped from 172.17.78.163 to 172.17.23.180
Today, 7:29:24 PM	myngfw	asa-172.17.78.1...		asa-172.17.23.1...	http (TCP/80)	1	asa-accept-172....	Standard	http Traffic Dropped from 172.17.78.163 to 172.17.23.180
Today, 7:29:24 PM	myngfw	asa-172.17.78.1...		asa-172.17.23.1...	http (TCP/80)	1	asa-accept-172....	Standard	http Traffic Dropped from 172.17.78.163 to 172.17.23.180
Today, 7:28:52 PM	myngfw	asa-172.17.78.1...		asa-172.17.23.1...	http (TCP/80)	1	asa-accept-172....	Standard	http Traffic Dropped from 172.17.78.163 to 172.17.23.180
Today, 7:28:24 PM	myngfw	asa-172.17.78.1...		asa-172.17.23.1...	http (TCP/80)	1	asa-accept-172....	Standard	http Traffic Dropped from 172.17.78.163 to 172.17.23.180
Today, 7:28:21 PM	myngfw	asa-172.17.78.1...		asa-172.17.23.1...	http (TCP/80)	1	asa-accept-172....	Standard	http Traffic Dropped from 172.17.78.163 to 172.17.23.180
Today, 7:28:19 PM	myngfw	169.254.169.123		myngfw (172.16....	ntp-udp (UDP/123)			Standard	ntp-udp Traffic Dropped from 169.254.169.123 to 172.16.18.152
Today, 7:28:19 PM	myngfw	169.254.169.123		myngfw (172.16....	ntp-udp (UDP/123)			Standard	ntp-udp Traffic Dropped from 169.254.169.123 to 172.16.18.152

Search For: Group | All Log Source Groups | Go | Add | Edit | Enable/Disable | Delete | Bulk Actions | Extensions | Parsing Order | Assign

Name	Desc	Status	Protocol	G...	Log Source Type	Enabled	Log Source Identifier	Tai De	Credibility	Autodiscc	Last Event Time	Creation Date	Modificati Date
Check Point source - 172...	Check P...	Success	Syslog		Check Point...	True	172.16.1...	e...	5	False	Sep 22, 2019, ...	Sep 22, ...	Sep 22, ...

```
[student<X>@ansible-1 ~]$ ssh ec2-user@snort
Last login: Fri Sep 20 15:09:40 2019 from 54.85.79.232
[ec2-user@snort ~]$ sudo grep ddos_simulation /etc/snort/rules/local.rules
alert tcp any any -> any any  (msg:"Attempted DDoS Attack"; uricontent:"/ddos_simulation"; classtype:successful-dos; sid:99000010; priority:1;
```

Reto: Co-Administración

```
[ec2-user@snort ~]$ journalctl -u snort -f
-- Logs begin at Sun 2019-09-22 14:24:07 UTC. --
Sep 22 21:03:03 ip-172-16-115-120.ec2.internal snort[22192]: [1:99000030:1] Attempted SQL Injection
Sep 22 21:03:08 ip-172-16-115-120.ec2.internal snort[22192]: [1:99000030:1] Attempted SQL Injection
Sep 22 21:03:13 ip-172-16-115-120.ec2.internal snort[22192]: [1:99000030:1] Attempted SQL Injection
```

	Event Name	Log Source	Event Count	Time
	Snort Open Source IDS Message	Snort rsyslog source - 172.16.18.39	1	14 Sep 2021, 10:21:30
	Snort Open Source IDS Message	Snort rsyslog source - 172.16.18.39	1	14 Sep 2021, 10:21:30
	Snort Open Source IDS Message	Snort rsyslog source - 172.16.18.39	1	14 Sep 2021, 10:21:30

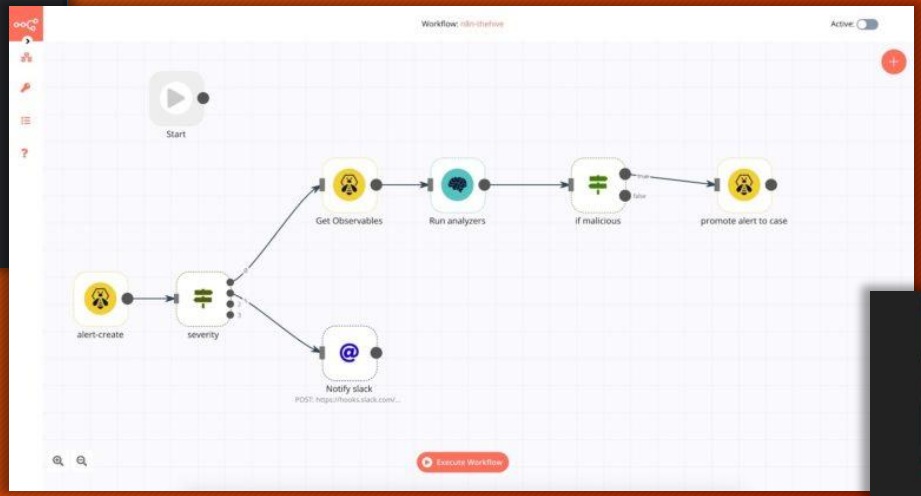
```
---
- name: Blacklist attacker
  hosts: checkpoint

  vars:
    source_ip: "{{ hostvars['attacker']['private_ip2'] }}"
    destination_ip: "{{ hostvars['snort']['private_ip2'] }}"

  tasks:
    - name: Create source IP host object
      checkpoint_host:
        name: "asa-{{ source_ip }}"
        ip_address: "{{ source_ip }}"

    - name: Create destination IP host object
      checkpoint_host:
        name: "asa-{{ destination_ip }}"
        ip_address: "{{ destination_ip }}"

    - name: Create access rule to deny access from source to destination
      checkpoint_access_rule:
        auto_install_policy: yes
        auto_publish_session: yes
        layer: Network
        position: top
        name: "asa-accept-{{ source_ip }}-to-{{ destination_ip }}"
        source: "asa-{{ source_ip }}"
        destination: "asa-{{ destination_ip }}"
        action: drop

    - name: Install policy
      cp_mgmt_install_policy:
        policy_package: standard
        install_on_all_cluster_members_or_fail: yes
      failed_when: false
```

```
[student<X>@ansible-1 ~]$ ansible-navigator run incident_blacklist.yml --mode stdout
```

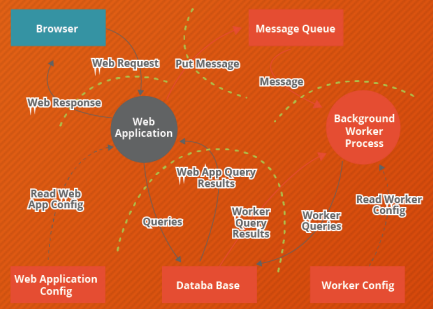
No.	Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On
1	asa-accept-172.17.199.94-to-172.17.30.140	asa-172.17.199.94	asa-172.17.30.140	Any	Any	Drop	Log	Policy Targets

Reto: Playbooks para Automatización

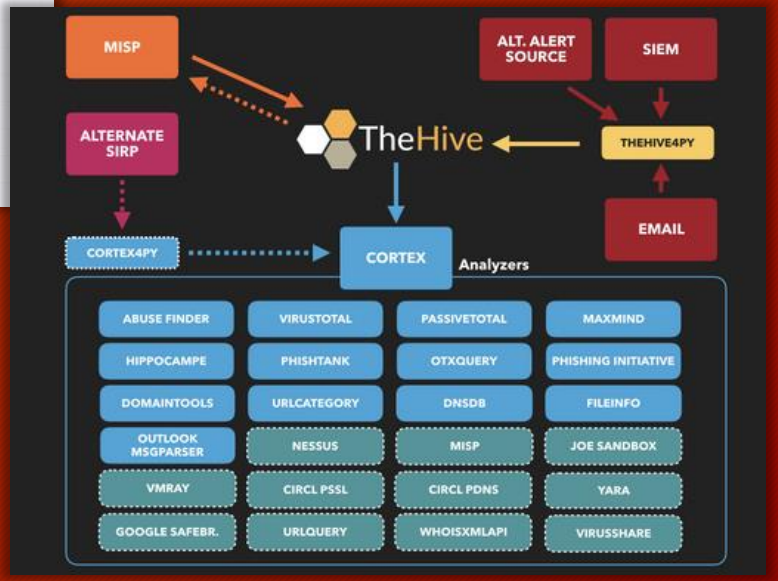
shuffler.io



n8n.io



PROCEDIMIENTOS
PLAYBOOKS



flexibleir.com

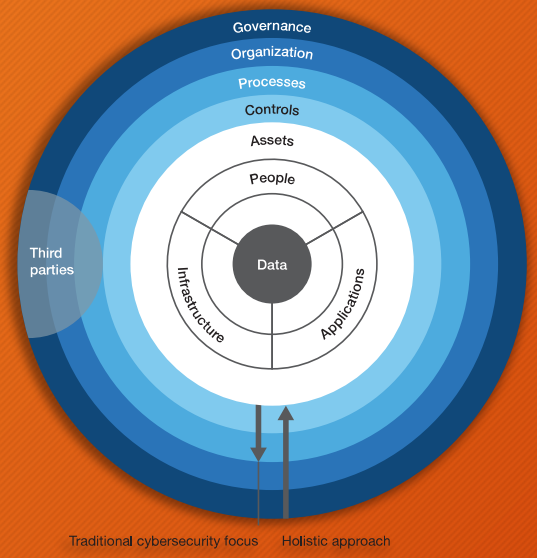
Retos de la Automatización del Threat Hunting

1. Tener claro los Activos Críticos **DE** la Organización o Comunidad Objetivo
2. Tener claro el Alcance y la Arquitectura de la infraestructura de TI
3. Identificar las Vulnerabilidades Conocidas y No Conocidas
4. Identificar Amenazas Conocidas y No Conocidas
5. Tener claro los Riesgos sobre los activos críticos
6. Seleccionar el mejor Control en Tratamiento de los Riesgos
7. Detectar Amenazas
8. Responder ante Amenazas

Gestión Riesgos Integral

The holistic approach to managing cyber risk proceeds from a top-management overview of the enterprise and its multilayered risk landscape.

Holistic cyber risk–management approach



Assets. Clearly defined critical assets

Controls. Differentiated controls to balance security with agility

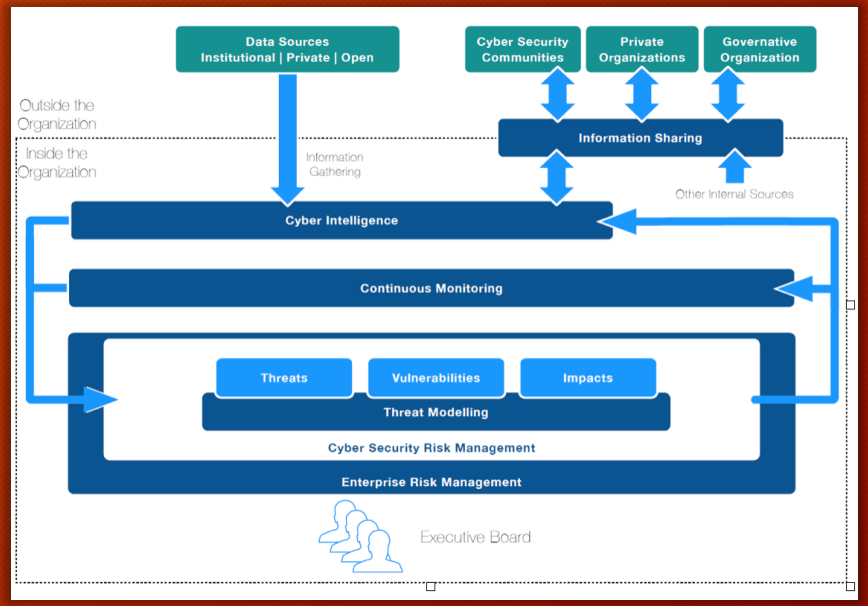
Processes. State-of-the-art cybersecurity processes focused on effective responses

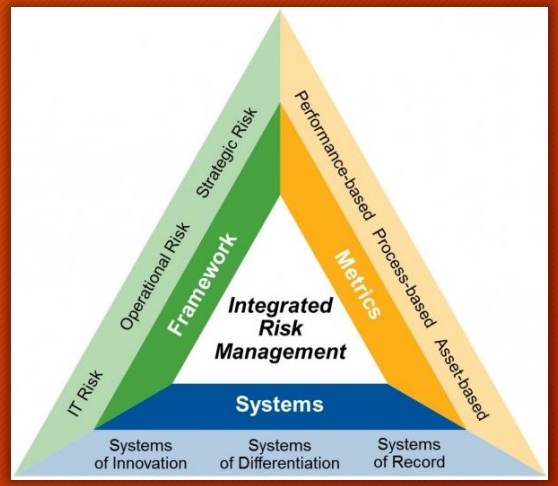
Organization. Right skills, efficient decision making, and effective enterprise-wide cooperation

Governance. Investments in operational resilience prioritized based on deep transparency into cyber risks

Third parties. Coverage of the whole value chain, including third-party services

McKinsey&Company





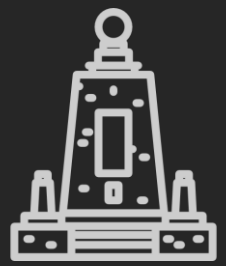
Retos de la Automatización del Threat Hunting

1. Tener claro los Activos Críticos **DE** la Organización o Comunidad Objetivo
2. Tener claro el Alcance y la Arquitectura de la infraestructura de TI
3. Identificar las Vulnerabilidades Conocidas y No Conocidas
4. Identificar Amenazas Conocidas y No Conocidas
5. Tener claro los Riesgos sobre los activos críticos
6. Seleccionar el mejor Control en Tratamiento de los Riesgos
7. Detectar Amenazas
8. Responder ante Amenazas
9. Personal preparado en Ciber Riesgos

Retos de la Automatización del Threat Hunting

1. Tener claro los Activos Críticos **DE** la Organización o Comunidad Objetivo
2. Tener claro el Alcance y la Arquitectura de la infraestructura de TI
3. Identificar las Vulnerabilidades Conocidas y No Conocidas
4. Identificar Amenazas Conocidas y No Conocidas
5. Tener claro los Riesgos sobre los activos críticos
6. Seleccionar el mejor Control en Tratamiento de los Riesgos
7. Detectar Amenazas
8. Responder ante Amenazas
9. Personal preparado en Ciber Riesgos
10. Implementar una estrategia de Ciberseguridad Basado en Riesgos ORGANIZACIONAL

ramiro.pulgar@bluehatcorp.com



GRACIAS DESDE ECUADOR