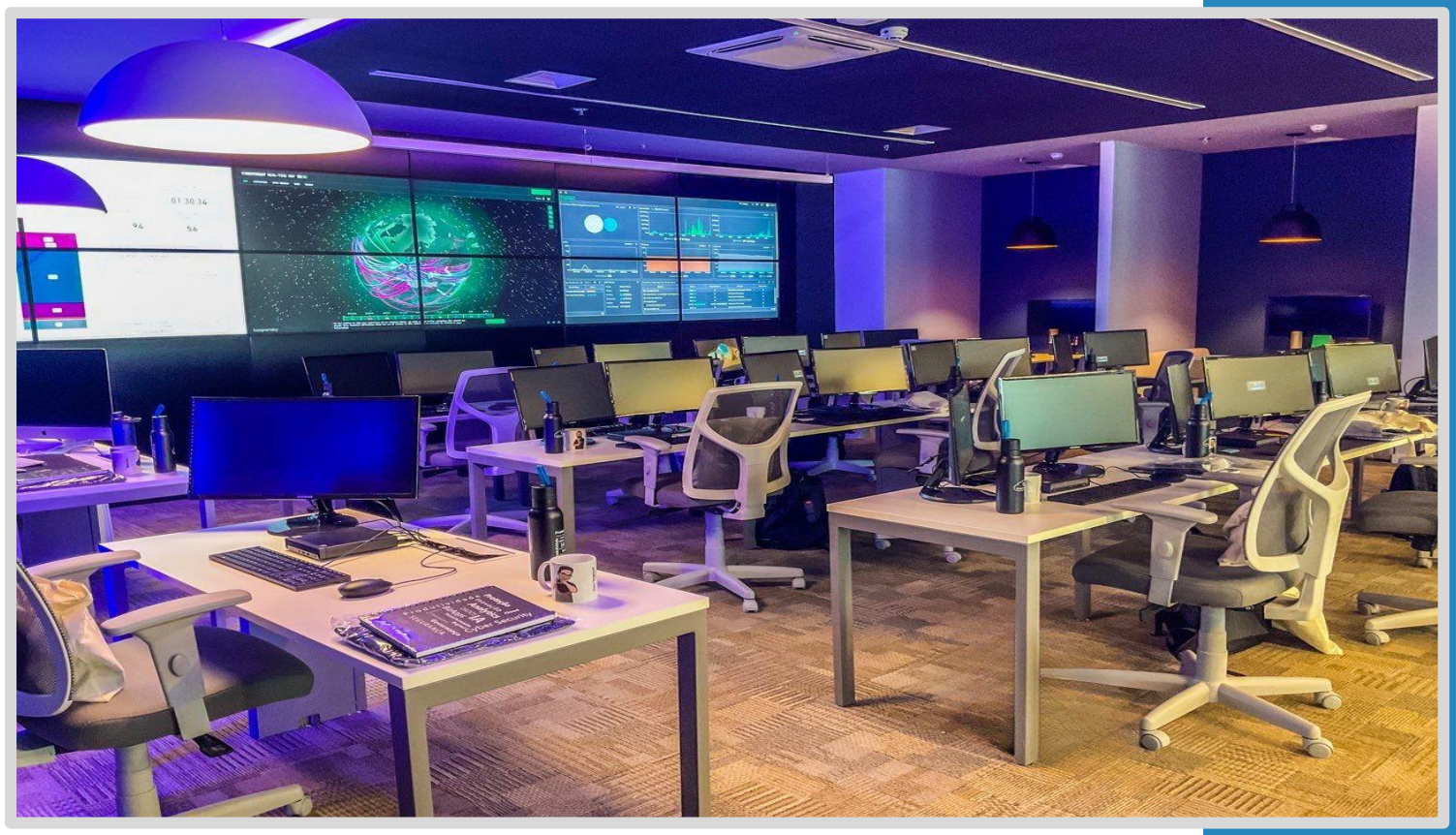


Cloud Target

Productivity | Security | Governance

Cyber Defense Center
&
Managed Security Services

#ZeroTrust #AI

+ www.cloudtarget.com.br

Cloud Target

+50
EXPERTS

+20 YEARS
EXPERIENCE IN MANAGEMENT OF COMPLEX ENVIRONMENTS

24x7
OPERATIONS CENTER
CYBER DEFENSE CENTER
MANAGED SECURITY SERVICES
HYBRID MANAGED SERVICES

3 LANGUAGES
SUPORT IN PORTUGUESE, ENGLISH, AND SPANISH

Microsoft Partner

Microsoft

- Gold Security
- Gold Cloud Platform
- Gold Cloud Productivity
- Gold Windows and Devices
- Gold Collaboration and Content
- Gold Enterprise Mobility Management
- Gold Data Analytics
- Gold Datacenter
- Gold Application Development
- Gold Small and Midmarket Cloud Solutions
- Silver Application Integration
- Silver Project and Portfolio Management

Microsoft
Partner Advanced Specialization

- Microsoft Windows Virtual Desktop
- Adoption and Change Management
- Cloud Security
- Identity and Access Management
- Information Protection and Governance
- Threat Protection

Microsoft
Fast Track Ready Partner

Awards:

MICROSOFT LATAM TEAMS HACKATHON 1

Microsoft LATAM Hackathon – Terceiro Lugar – Edição Frontline

Latam Partner of the Year 2021
Security and Compliance

A Selection of our Diverse Client Portfolio by Sector.

Cloud Target

Construction & Industry

atex BRASIL A FÓRMA DA LAJE NERVURADA
CYRELA
Gafisa
Votorantim
[redacted]
ibbl
KOMATSU
VIGOR

Legal

BP BarrosPimentel AlcantaraGil e Rodriguez ADVOGADOS
PK PINHÃO E KOIFFMAN ADVOGADOS
JUSPRO
LBCA Lee Brock Camargo ADVOGADOS
Mourão Campos
GM GUSTAVO DE OLIVEIRA MORAIS ADVOGADOS
LEFOSSE ADVOGADOS

Marketing / Telecommunications

planmark
click interativo AGÊNCIA DIGITAL
CONNECT2B
IP Corp 91 15 ANOS Telecom S.A.
outcenter
SKY

Financial Markets

stone
[B]3
Banco ORIGINAL
BANCO PAN
cielo
CSU
BRITech
AQUA CAPITAL
RB CAPITAL
crefisa
eloPar

Healthcare

A.C.Camargo Cancer Center
FRESENIUS MEDICAL CARE
Hypera pharma
REDE D'OR SÃO LUIZ
Unimed

Technology

4U IT
KPMG
multiner
TECHTRIALS
netpartners valores que trazem resultados
Neogrid

Retail

AVENIDA
BURGER KING
DIA %
VIA
natura
RCHLO RIACHUELO
Pellegrino

Professional Services

Liberty Seguros
movida
SOMPO SEGUROS
TEATRO Santander
PORTO SEGURO
taxweb Compliance Fiscal
ATENTO

Migration & Onboarding – Cases

Cloud Target

cielo — Cyber Security

Target: Sentinel Deployment

Challenge: Migration from ArchSite to Sentinel. Main Frame Integration and various other systems

Numbers: 9,000 collaborators

Extras: Connector Development

Cyber Security

Target: Sentinel Deployment

Challenge: Migration from Splunk to Sentinel.

Numbers: 5,600 collaborators

Extras: Connector Development

cielo — Cyber Security

Target: Deployment of M365 E5

Challenge: Migration from Arcsight to Sentinel as well as EDR, DLP, and Defender for Identity Deployment

Numbers: 9,000 collaborators

Extras: Connector Development

PORTO SEGURO — DevOps

Target: Application Modernization

Challenge: Cloud Adoption with Security

Numbers: US$ 147,000 Azure

Extras: Support and Mentorship

Remote Work

Target: FileServer for SharePoint migration

Challenge: Assessment Before Migration

Numbers: 200 TB of archives, 5,600 Users

Extras: Qualification Arq. / Map. From/To

ATENTO — Remote Work

Target: Adoption of Windows Virtual Desktop

Challenge: Remote Office to Call Center

Numbers: 70,000 users migrated, 13 Countries

Extras: Security workloads

CDC: Services

Cloud Target

Access Identity Management

Device Unification Management

Data Protection Management

Threat Protection Management

FW Management

Threat Intelligence

PEN Testing

Anti Virus and Anti Malware Management

Application Gateway Management

Security and Compliance Management

Applications Management

Centralized Log Management with AI (SIEM and SOAR)

Guard the entrance

Data protection anywhere

Detect and fix attacks

Cloud Target

Identify

- Asset Management
- Business Environment
- Governance
- Risk Assessment
- Risk Management Strategy

Protect

- Access Control
- Awareness and Training
- Data Security
- Info Protection Processes and Procedures
- Maintenance
- Protective Technology

Detect

- Anomalies and Events
- Security Continuous Monitoring
- Detection Processes

Respond

- Response Planning
- Communications
- Analysis
- Mitigation
- Improvements

Recover

- Recovery Planning
- Improvements
- Communications

CDC: REFERENCE MODEL

Cloud Target

Azure Sentinel

IDENTIFY | PROTECT | DETECT | RESPOND | RECOVER

Professional GRC

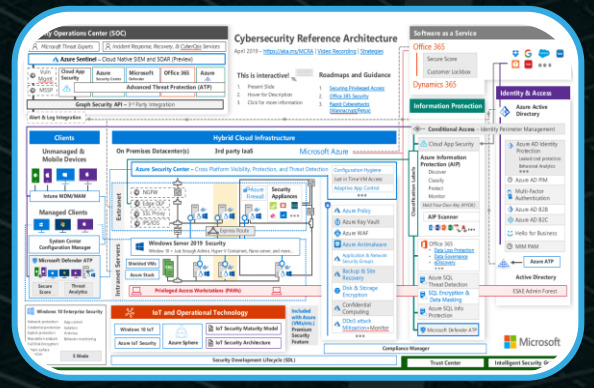
Risk and Compliance Evaluation

Professional IT / Security

Deploys Protection

SOC/CSIRT

Console
Alerts and Investigation



Alert Generation

Identity | Endpoint | Cloud | Network | Others

CDC: SECURITY INCIDENT MANAGEMENT

Cloud Target

Incident Response Process in 9 Steps

- The first priority is containment and recovery
- Contractual commitments for client notification

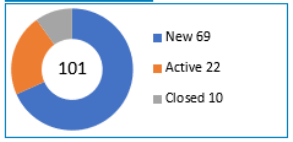
CDC: DASHBOARDS AND REPORTS

Cloud Target

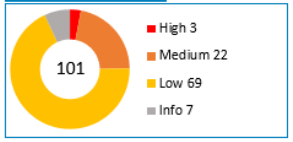
SECURITY OPERATIONS EFFICIENCY

Overview

INCIDENTS BY STATUS



INCIDENTS BY SEVERITY



CLOSED BY CLASSIFICATION

33d Time To **Acknowledge** Above the average

83d Time To **Remediate** Above the average

10 **Manually** Remediations

0 **Automated** Remediations

ⓘ Note

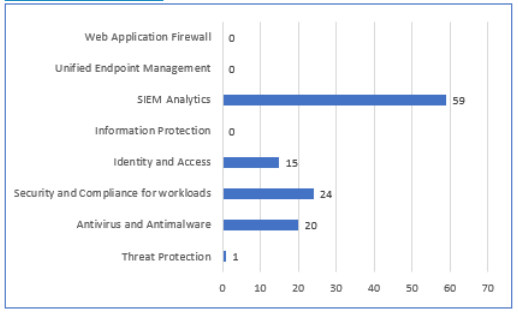
According to MetricNet's, the **average TTR** is **8.4h**, from a range of 1h to 34h

According to the RSA conference in 2020, **TTA under 12h** is a reference for a good metric

SECURITY OPERATIONS EFFICIENCY

Overview

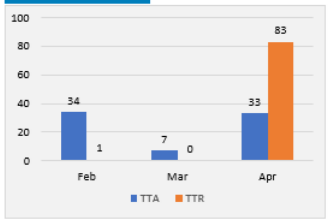
INCIDENTS BY SERVICES



ⓘ Note

SIEM Analytics are detections made by Azure Sentinel analytics rules.

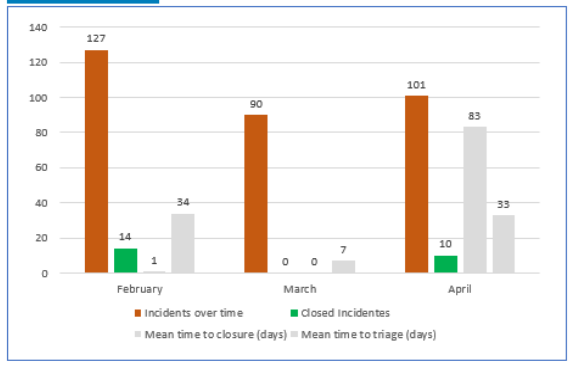
TTA & TTR Evolution



SECURITY OPERATIONS EFFICIENCY

Overview

INCIDENTS OVER TIME



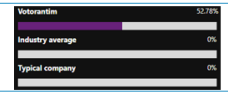
Identity and Access Management

Identity Protection

1488 **Total** Detected Identity Risks

81 **Remediated** Identity Risks

52.78 Your score is above the average for your company's industry.



0012 HIGH RISKS

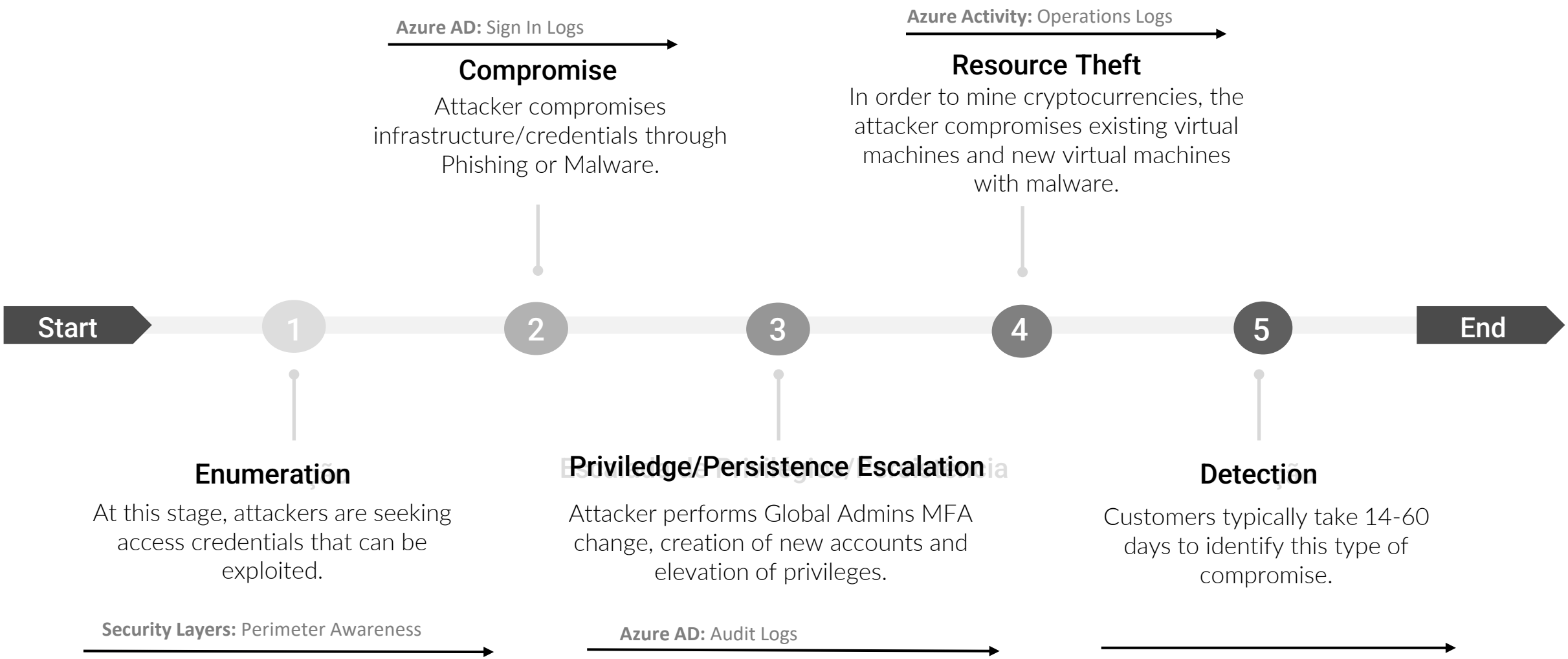
0257 MEDIUM RISKS

1219 LOW RISKS

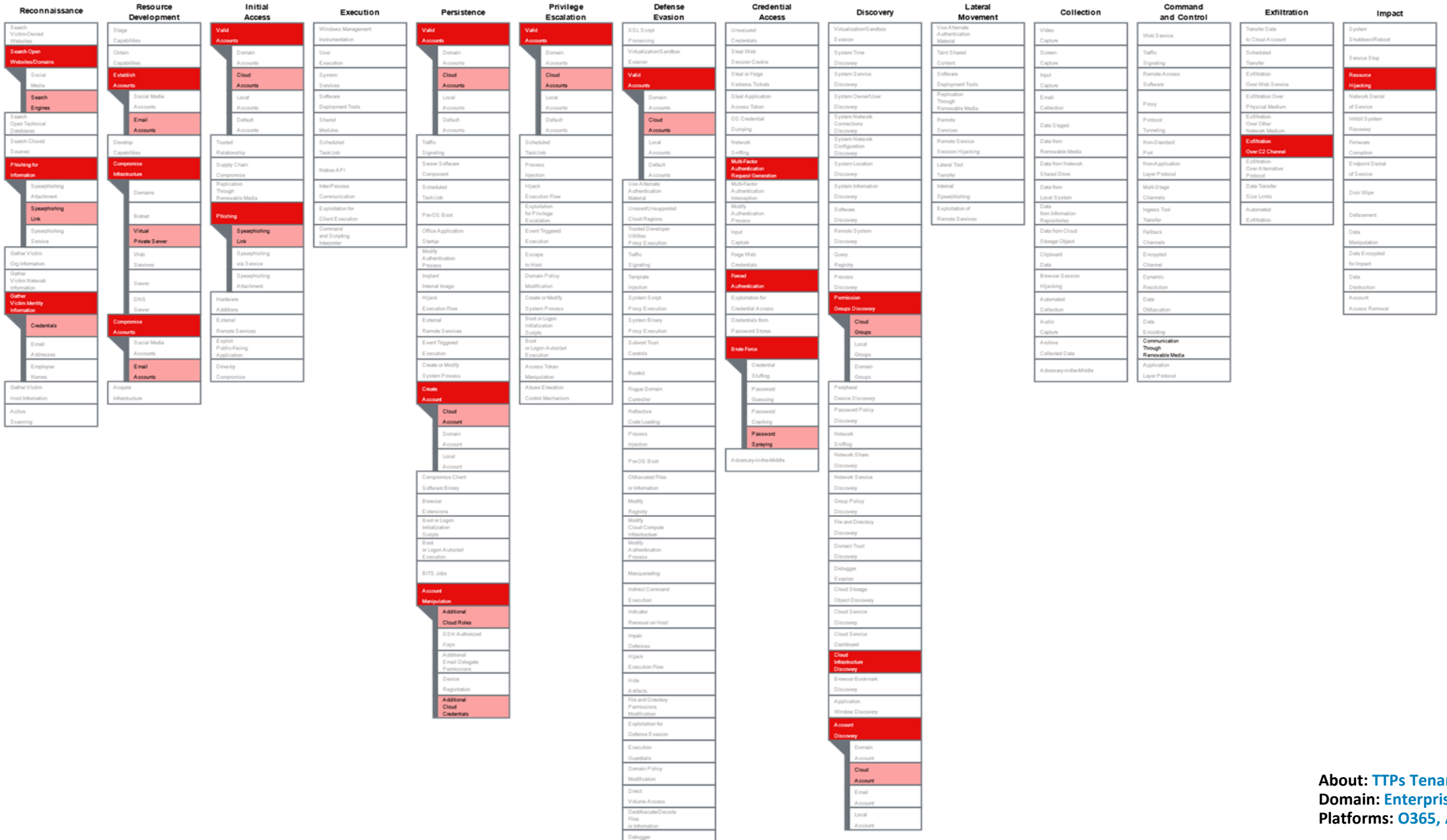
	User	Detection Type
		Unfamiliar sign-in properties
		Unfamiliar sign-in properties
com.br		Unfamiliar sign-in properties
com.br		Unfamiliar sign-in properties
com.br		Unfamiliar sign-in properties
com		Atypical travel
		Impossible travel
		Impossible travel
m		Unfamiliar sign-in properties
		Unfamiliar sign-in properties
		Unfamiliar sign-in properties
		Unfamiliar sign-in properties
		Unfamiliar sign-in properties
		Unfamiliar sign-in properties
		Unfamiliar sign-in properties

FULL REPOR

CDC: ATTACKER ACTIONS



CDC: TTPs – Mitre ATT&CK



About: TTPs Tenants Compromised
Domain: Enterprise ATT&CK v11
Platforms: O365, Azure AD, SaaS e IaaS

CDC: Cloud Target Solution – CTAntifraud

Compromise

Identity and Access Management

24x7 Azure AD monitoring, focusing on Sign -in attempts, Apps & Service Main activities with unusual signs that indicate compromise. This monitoring stops the attacker in the initial phase.

Resource Theft

Workload Compliance and Security

24x7 behavior and activity monitoring caused by Azure subscriptions and their resources (if available MDC). Through this service pack, we are able to identify anomalous Azure activities. For instance, the creation of a VM. This is the impact stage, leading to financial losses to the customer.

Start 1 2 3 4 5 End

Pentest

We perform quarterly penetration tests on Microsoft Azure platforms mapping vulnerabilities and recommending solutions.

Enummeration

Access and Identity Management

24x7 Azure AD monitoring focusing on anomalous behavior. This being creation of new users with administrative privileges or non- interactive activities of Apps & Service Principals. This monitoring indicates that the environment has already been compromised and the attacker is persisting.

Privillege/Persistence Escalation

SOC/CSIRT

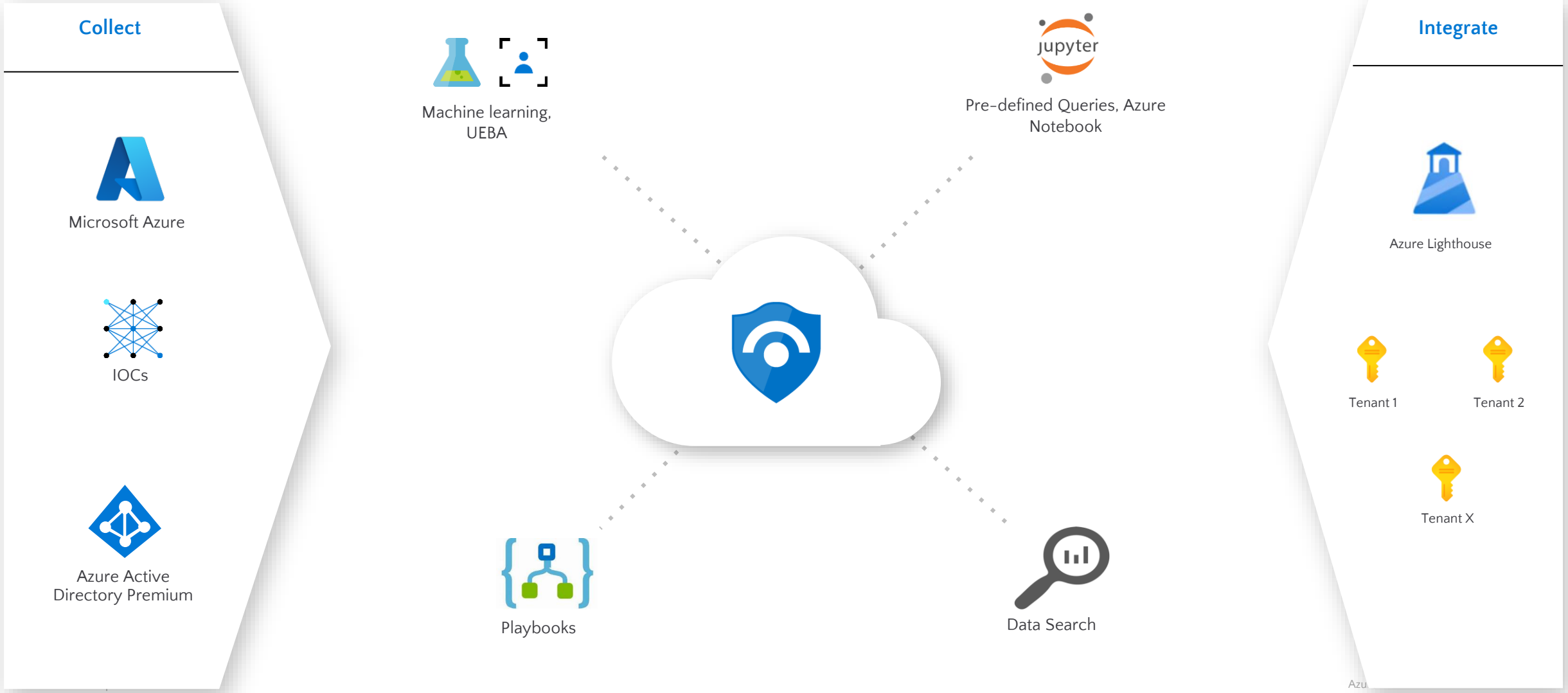
With a team focused 24x7 on detecting and responding to security incidents using Microsoft Sentinel as a SIEM tool, we are able to detect the initial stage of an attack in less than 30 minutes (test VM).

Alert: User Creation, Elevation of Privileges, Virtual Machine Creation.

Automation: Credencial blocking, notification of specific individuals.

Detection and Response

CDC: Cloud Target Solution – CTAntifraud



CDC: Cloud Target Solution – CTAntifraud

SCOPE

PHASE 1 – INITIAL SETUP (2 weeks)
- Survey of the Customer's environment and its managed Tenants
- Initial customization on customer premises
- Automated deployment across all Tenants

PHASE 2 – ONBOARDING (1 Week per 200 Clients)
- Automated deployment across all Tenants
- Adjustments of ingested LOGs to reduce consumption

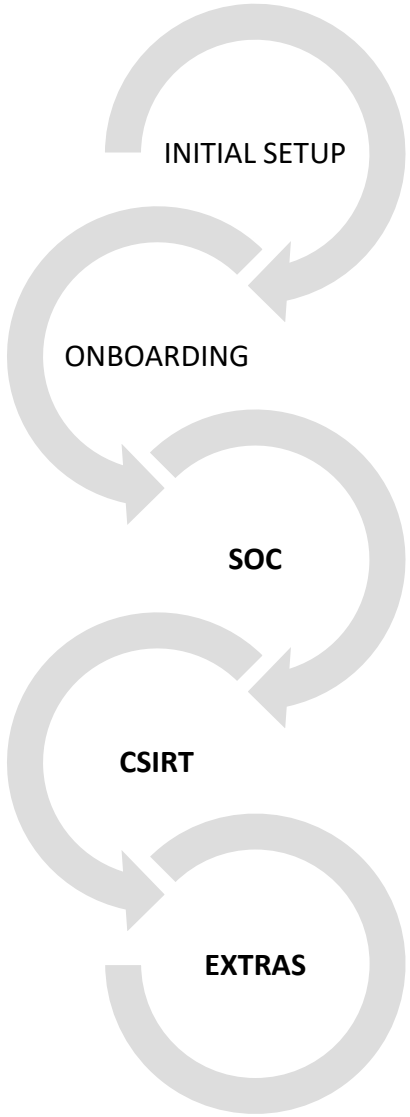
PHASE 3 – CYBER DEFENSE CENTER (PROFESSIONAL BUNDLE)
- SOC (Monitoring)

PHASE 4 – CYBER DEFENSE CENTER (PREMIUM BUNDLE)
- CSIRT (Incident Response with Specialists)

PHASE 5 – CYBER DEFENSE CENTER (UNIQUE BUNDLE)
- Exemple of Additional Services:
  - PEN Test
  - Compliance Management

DELIVERIES
- SOC Efficiency Report - Monthly
- Creation and/or Update of Use Cases (detection rules) - Monthly
- LOG Consumption Report - Monthly
- Pen Test Report (if contracted additionally) - Quarterly
- Compliance Report (if contracted additionally) - Monthly

OBLIGATIONS
- Customer shall at least pay the cost of AD Premium for users with Administrative privileges, costing $6USD per user
- Sentinel will be configured for each End Customer and the cost of data onboarding will be paid by the End Customer




Cloud Target
THANKYOU!