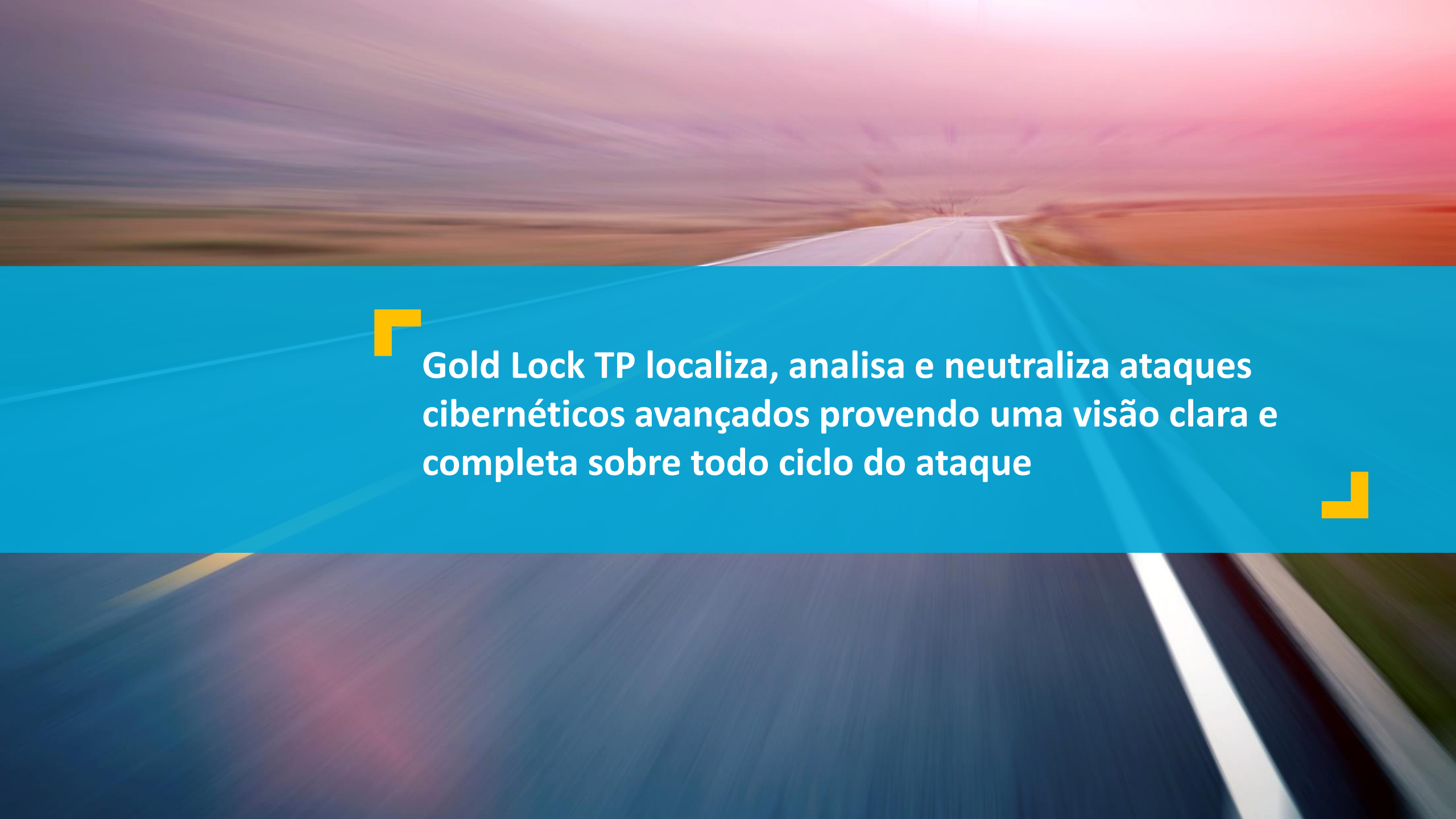


Gold Lock TP localiza, analisa e neutraliza ataques cibernéticos avançados provendo uma visão clara e completa sobre todo ciclo do ataque

Entendendo a cadeia de cyber ataques

Gold Lock DA monitora a Deep Web e a Dark Web em busca de atividades direcionadas a cada cliente e alertas ao primeiro sinal de ameaça

Gold Lock TP monitora todos os vetores de ataque - Rede, Endpoints, Arquivos, Comando e controle, Movimento lateral - e automatiza as investigações

Source: Lockheed Martin, 2011


Gold Lock TP
é uma plataforma unificada,
totalmente integrada por design,
que emprega Inteligência Artificial de nível militar
DATA
para automatizar a maior parte das Investigações Cibernéticas,
simplificando a vida dos analistas humanos
E encurtando o tempo entre detecção e resposta

O mercado de detecção e resposta hoje

Super categoria

Gold Lock TP
Detecção e Resposta

Sub categoria

Detecção e prevenção de violações

Visibilidade e Investigação

Resposta do incidente

Ferramentas

Adv. Detection

- Sandbox
- Containment
- Deception
- SIEM
- User Behavior

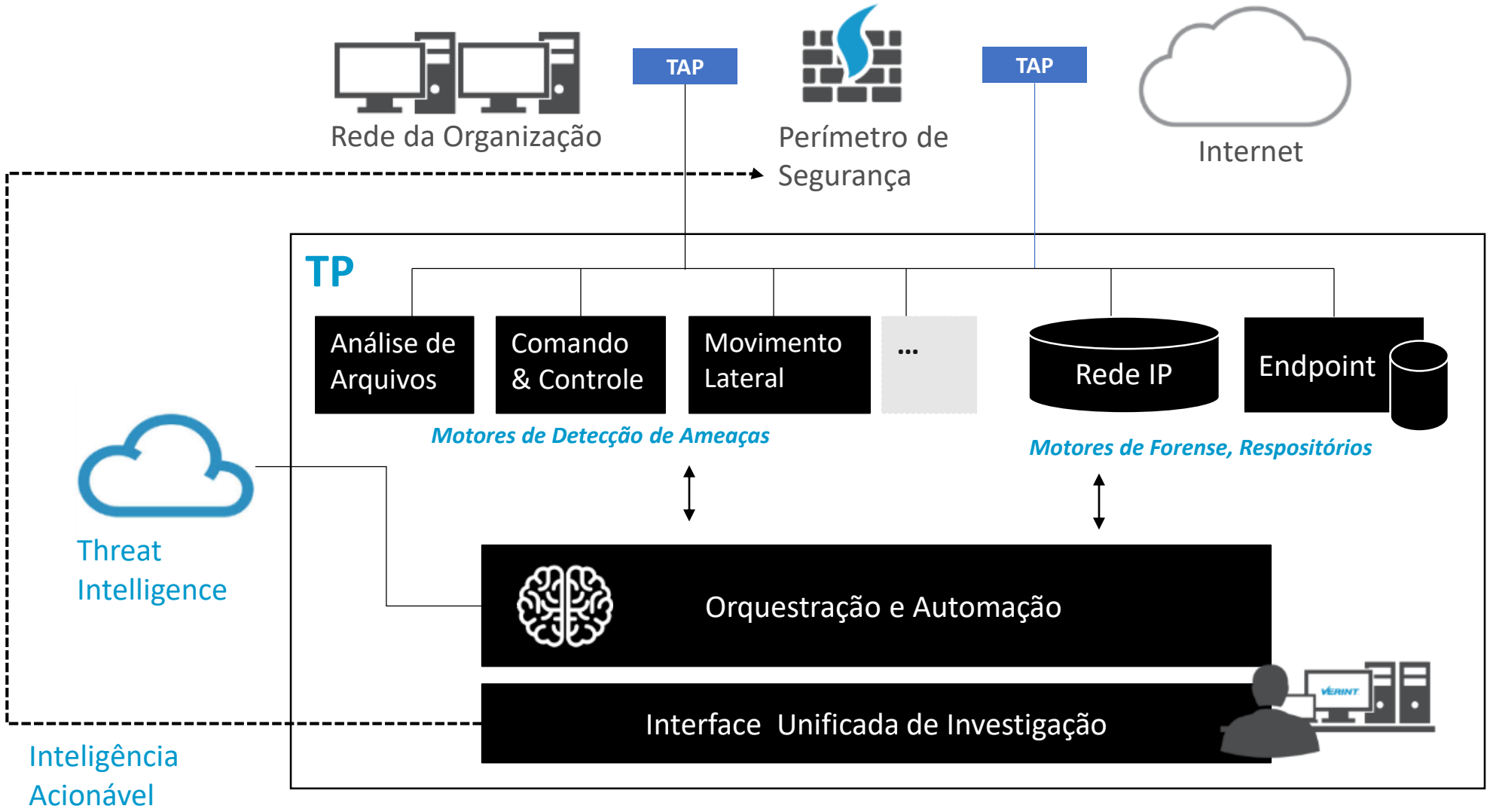
Security Analytics

- NW traffic analysis
- NW forensics

Automation & Orchestration

- Endpoint Detection Response
- Incident Response
- Orchestration

Sistema de Proteção Contra Ameaças Cibernéticas (TP)



Os sensores do TP

- Gold Lock TP vem com um conjunto de sensores de detecção, totalmente integrados por design:
- Sensor Forense de Rede
- Sensor forense de Endpoint + Agente forense de Endpoint
- Sensor de Análise de Arquivos
- Sensor de comando e controle com máquina de Inteligência Artificial
- Sensor de Movimento Lateral
- OT e Sensor de Infraestrutura Crítica (opcional)

- Diferenciais:
- transforma milhares de alertas em apenas alguns incidentes, entregando tudo mastigado para o analista
- reduz tempo com investigações
- totalmente integrado para SOC (centro de operações de segurança) e tudo vem em um módulo só
- Detecção antecipada de malwares, eficiência do SOC, economia de custos, processamento de dados em tempo real, tecnologia de analise de comportamento de ameaças, investigação forense em rede, endpoints e arquivos
- Conjunto extenso de motores de detecção, com filtros embutidos, análise adaptativa e comportamental com mecanismo de auto aprendizagem, cross validação entre os motores (segunda opinião)
- Investigação forense: rede, endpoints, arquivos, fontes externas
- Arquitetura aberta – facilmente se adiciona novas tecnologias

Arquitetura de Hardware

- Arquitetura Escalável
- Hardware Padrão de Mercado
- Especificação Otimizada para Cyber
- Storage Acessível

Switch de Agregação (Até 10Gb/s)

Atrás

15U

Frente

- Decodificador
- Coletor Forense
- Sensores de Detecção - Rede
- Sensor de Detecção - Arquivos
- Análises, Alertas, Incidentes
- Investigação Unificada
- Storage para Forense (100's TB)

Gold Lock TP Pode Ajudar Você a Proteger seus Clientes

VISBILIDADE AMPLA

DETECÇÃO MULTI-DIMENSIONAL

INTELIGÊNCIA COM ORQUESTRAÇÃO

INVESTIGAÇÃO UNIFICADA

PLATAFORMA ABERTA

REDUÇÃO DO RUÍDO

CONSTRUÇÃO DA ESTÓRIA DO ATAQUE

INTELIGÊNCIA ACIONÁVEL DE FORMA IMEDIATA

ÁGIL E ADAPTÁVEL

Plataforma de Inteligência Acionável

CAPTURA DE DADOS

- Operacional
- Transacional
- Telecomunicações
- Mídias Sociais
- Payload & Arquivos
- End Point
- Rede

PROCESSAMENTO DE DADOS

- Limpeza de Dados
- Fusão de Dados
- Enriquecimento
- Não-Estruturados e Estruturados
- Motores de Detecção

MOTORES DE ANÁLISE

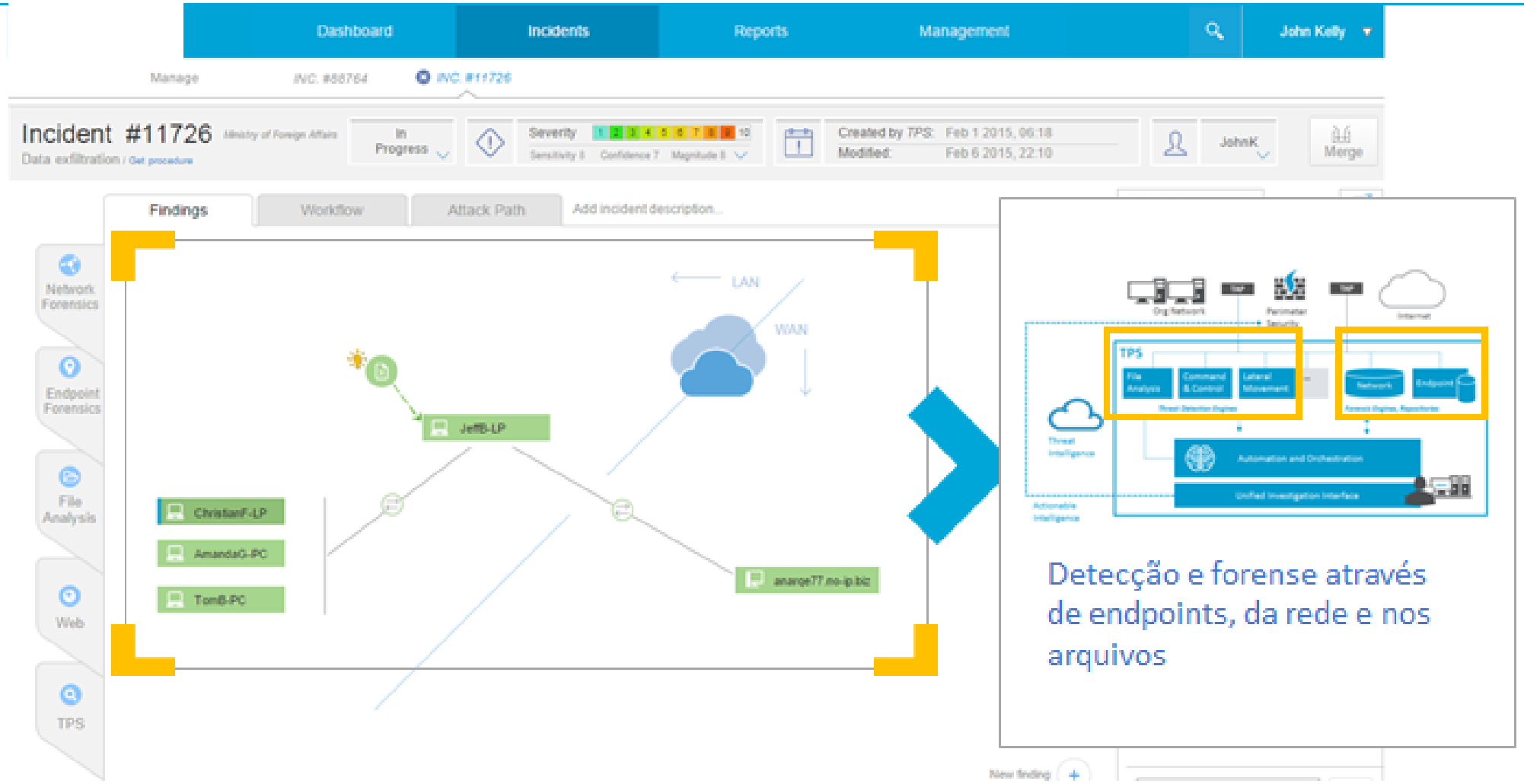
- Classificação
- Correlação
- Detecção por Anomalia
- Analisador de Identid.
- Forense
- Analizadores como plugins

EMPENHO E AÇÃO

- Dashboard
- Bancada de Análise
- Tendências
- Gestão de Casos
- Gestão de Fluxos
- Alimentar para Prevenir
- Alertas Preditivos

SERVIÇOS COMUNS & GESTÃO

AMPLA VISBILIDADE



DETECÇÃO MULTI-DIMENSIONAL – MITIGANDO TODO O KILL CHAIN

Coleta de Inteligência

Montar Armas e Infiltrar

Comunicação com a Base

Movimento Lateral

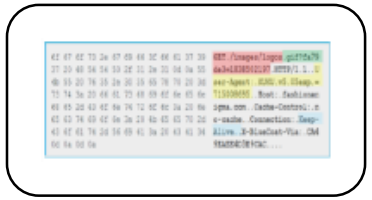
Atacar e Cobrir os Rastros

Threat Intelligence

- Lab de Pesquisa
- Cloud de Inteligência
- Fontes de Reputação

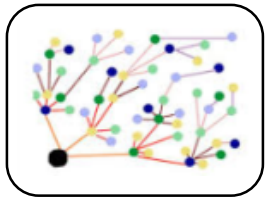
Malicious File Detection

- Static File Analysis
- Dynamic Memory Analysis
- Resiliente a Anti-Sandboxing



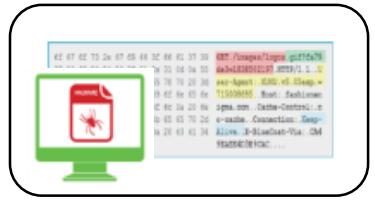
Detecção de C&C Baseado na Rede

- Máquinas de Aprendizagem
- Reputação
- Detecção de Evasão
- Detecção por Anomalia



Análise Multi-Dimensional

- Motores especializados nos estágios do ML
- Correlação de visões da Rede + Endpoint



Monitoramento da Rede & Endpoint

- Sinaliza Atividade de Rede Não Usual
- Forense de Endpoint e Rede Dinâmica

Gold-Lock Brasil

Av. Pacaembu 1976
Pacaembu - SP
Cep: 01234-000

Tel.: (11) 3511-3855
Web: www.goldlock.com.br