



# He recibido un e-mail APD

Mayo, 2019

Fireeye

Antonio Cañada, [antonio.canada@fireeye.com](mailto:antonio.canada@fireeye.com)

# **OUR MISSION**

To relentlessly protect our customers with innovative technology and expertise learned on the front lines of cyber attacks.

# On the Front Lines. Every Day.

**700+**

THREAT RESEARCHERS,  
PLATFORM ENGINEERS,  
MALWARE ANALYSTS,  
INTELLIGENCE ANALYSTS, AND  
INVESTIGATORS

**35+**

NATION-STATE  
SPONSORED APTs  
TRACKED

**4**

CYBER THREAT  
OPERATIONS  
CENTERS  
WORLDWIDE

**24,000**

INTELLIGENCE  
REPORTS PUBLISHED  
IN 2018

**THOUSANDS**

OF INCIDENT RESPONSE HOURS  
EACH YEAR

**600K – 1M**

MALWARE SAMPLES  
COLLECTED DAILY FROM  
70+ SOURCES

**FireEye Catches What Others Miss**



FireEye knows more about **cyber threats** than anyone.



# La transformación digital

- El alcance de la transformación digital se expande
- Activos digitales
  - Datos
  - Procesos
- Exposición en redes

The screenshot shows the header of the website 'Expansión economía digital' with navigation links for 'COMPANIAS', 'PROTAGONISTAS', and 'INNOVACIÓN'. Below the header, a main headline reads 'Así abrazan las empresas españolas la digitalización'. A red box highlights the URL: <http://www.expansion.com/economia-digital/companias/2017/06/20/592c636c2260>.

## LA BANCA, A LA CABEZA DE LA TRANSFORMACIÓN

Las entidades financieras españolas están realizando un esfuerzo significativo para

## AL SERVICIO DEL TURISTA DIGITAL

Las empresas turísticas españolas deben afrontar la transformación digital

## LA DISTRIBUCIÓN ANTE EL RETO DEL ECOMERCE

El sector de la distribución de bienes de consumo cambiará más en la próxima

## ENERGÍA, ORIENTACIÓN AL CLIENTE

El cambio de los hábitos de los consumidores en la era digital ha obligado a las

## LA INDUSTRIA ESPAÑOLA DA EL SALTO DIGITAL Y ENTRA EN LA ERA 4.0

La industria española tiene ante sí la oportunidad de dar un salto de gigante

## LA NECESARIA INNOVACIÓN EN INFRAESTRUCTURAS

La innovación es una de los pilares que sostienen la competitividad del sector de

# La gestión empresarial

- Objetivos de la compañía
  - Desarrollo de productos
  - Procesos productivos
  - Gestión de la organización
  - Procesos de venta y foco en el cliente
  - Generación de valor

- ◆ El riesgo
  - ▶ Productos no adecuados
  - ▶ Procesos de producción que fallan
  - ▶ Organización inestable
  - ▶ No encontrar a los clientes
  - ▶ No hay valor

## ¿porqué?

La ciberamenaza materializa el riesgo de pérdida

# El rol de la dirección

- Liderazgo -> Polarización, motivación, fe
- Seguridad-> Confianza
- Incertidumbre <-> Dudas, desconfianza
- Toma de decisiones => Información de contexto
- Sin indicadores -> no hay toma de decisiones
- Conocimiento -> Acierto -> Confianza -> Base del liderazgo



# La ciberamenaza

## ■ La actividad de

### – Estados Nación

### – Criminales

### – Terroristas

### – Activistas

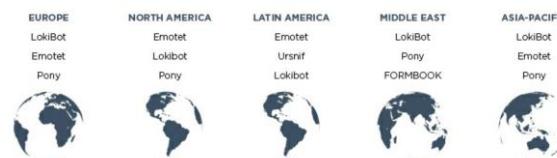
APT GROUP	DEFENSE AREA	DATA THEFT OR CONTEXT
APT1	Aerospace Naval Systems Telecommunications	APT1 stole information on the Huey II helicopter, satellite programs and UAV, radar, radio, sensor and satellite simulation technology.
APT2	Aerospace Maritime Government	APT2 intrusions are generally consistent with larger PRC military modernization goals. APT2 recently targeted a European satellite constellation used by the country's military.
APT3	Avionics Propulsion Missiles Government	Technical data related to a military reconnaissance aircraft and associated sensor packages, communications, avionics and missile systems. This group's theft of rotary-wing aircraft, missile and U.S. aerial reconnaissance data could be related to critical needs in the PRC's aviation industry and the PLA's warfighting doctrine.
APT4	Aerospace Command & Control	Intrusions against DIB companies specializing in military aerospace and command and control systems are consistent with larger PRC military modernization goals.
APT5	SATCOM Data Encryption UAV Sensors	Data theft included SATCOM hardware on both terrestrial and space-based platforms, encryption and decryption software the algorithms, technical documentation and maintenance processes. We also observed APT5 stealing data from companies specializing in UAV sensor suites, including imaging systems, surveillance sensors, uncrewed aerial vehicles, and other components used in military and civilian aircraft.
APT6	Aerospace Command & Control	In one instance, APT6 stole information related to rotary-winged missile systems. The pattern of targeted enterprises suggests actors seek information on satellite communication technology, command and control systems and components for military and civilian aircraft.
APT7	Aerospace Command & Control Telecommunications	Targeted companies manufactured aircraft and produced components for the aerospace industry. In one instance, APT7 and at least four other APT groups targeted the same telecommunications firm in the same time period.
APT9	Imaging Systems Rotary Wing Aircraft	Impacted companies produced multispectral imaging systems for both military and commercial use and rotary-wing aircraft.
APT10	Aerospace Communications Imaging Systems Command & Control UAVs	APT10 targeted propulsion systems for aircraft, aircraft-mounted sensors, military aircraft or UAV's, military-grade imaging and command and control technology, power-generation technology, including electrical systems for aircraft.

### Top Credential Theft-Capable Malware Targeting by Region, Observed Across All Industries

The following table and image highlight the top detected malware with credential theft capabilities per region in September 2018 and irrespective of industry vertical. Cyber criminals distributing these malware variants commonly leverage compromised credentials to conduct fraudulent banking activities.

Europe	North America	Latin America	Middle East	Asia Pacific
LokiBot	Emotet	Emotet	LokiBot	LokiBot
Emotet	LokiBot	Ursnif	Pony	Emotet
Pony	Pony	LokiBot	FORMBOOK	Pony

Table 2: Top detected malware with credential theft capabilities per region in September 2018



**Cyber Espionage Operation Targets U.S. Cancer Research Facility**

May 06, 2019 19-00007950, Version: [1]

UNITED STATES CYBER ESPIONAGE PHARMACEUTICALS HEALTHCARE

**Executive Summary**

- FireEye devices detected and blocked a series of medically themed emails that were designed to compromise a U.S. cancer research facility.
- Technical analysis revealed that each attempt to compromise the system, through a malicious link or attachment, would result in installation of EWLNUGET malware.
- The threat actors directly interacted with an analyst workstation and FireEye Threat Intelligence observed the actors perform reconnaissance, downloading, uploading, and deleting files.
- As previously reported, we believe that China's national priority on pharmaceutical innovation and rising cancer rates are catalysts behind targeting the healthcare sector.

**Threat Detail**

From April 8-9, 2019, suspected Chinese cyber espionage actors attempted on four separate occasions to compromise computer systems at a U.S. cancer research facility through targeted emails that contained links to CVE-2017-11882 exploit documents or malicious attachments. FireEye technical analysts determined that all



Solutions Services Partners Support Resources Company

### Threat Intelligence Reports by Industry

To stop cyber threats to every industry and every industry, FireEye conducts extensive threat intelligence research. We strive to understand the nature of your business, needs and vulnerabilities. We even explore the motivations of attackers and threats specific to your industry. Our findings can help build valuable and relevant cyber security solutions for your organization. Put our threat intelligence to work for you.



**Aerospace and Defense**  
Read the latest outlook for aerospace and defense sectors as threat groups seek to gain military and economic advantages.



**Construction and Engineering**  
Learn why the construction and engineering sectors are prime targets for state-sponsored threat actors engaged in cyber espionage.



**Education**  
Understand the cyber threats targeting the education industry, including subsectors impacted by advanced threat groups.



**Energy**  
Learn what situations contribute to threat activities toward organizations in the energy industry.



**Entertainment and Media**  
Discover why the entertainment and media industries are valuable targets for APT groups and hacktivists seeking influence.



**Financial Services and Insurance**  
Get a glimpse of cyber-threats the financial services and insurance sectors are facing, including top malware and crimeware detected.



**Healthcare and Health Insurance**  
Learn about current and impending cyber threats to the healthcare and health insurance industry.



**High Tech and Information Technology**  
Get a threat outlook for high tech and IT sectors as their relevance to economic intelligence and security.



**International Organizations and Nonprofits**  
Gain insights into the nature and rationales of cyber threats international organizations and.

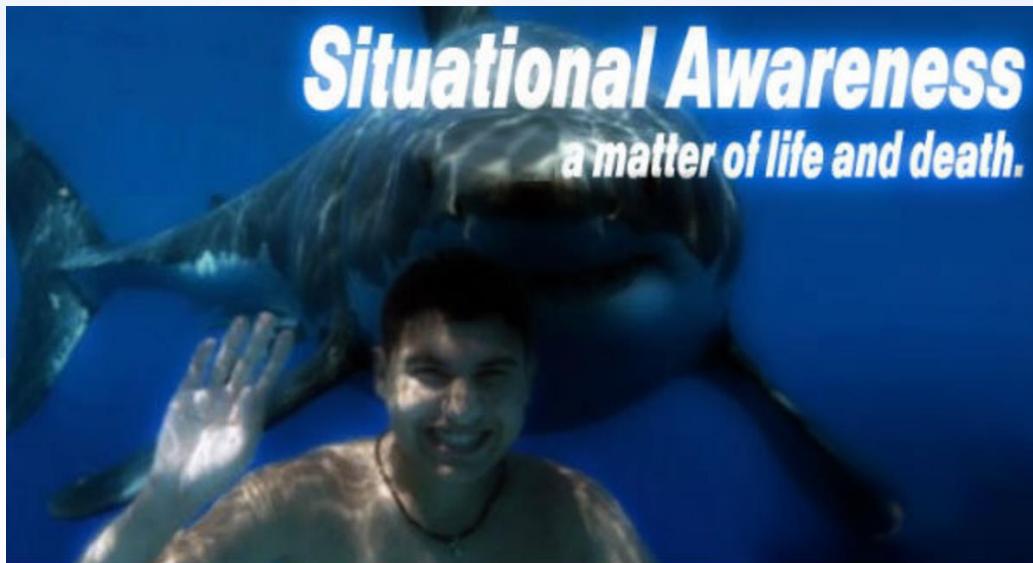
# Ciberincidentes

CRITERIOS DE DETERMINACIÓN DEL NIVEL DE PELIGROSIDAD DE LOS CIBERINCIDENTES <sup>11</sup>			
NIVEL	AMENAZA(S) SUBYACENTE(S) MÁS HABITUAL(ES)	VECTOR DE ATAQUE	CARACTERÍSTICAS POTENCIALES DEL CIBERINCIDENTE
CRÍTICO	Ciberespionaje	- APTs, campañas de malware, interrupción de servicios, compromiso de sistemas de control industrial, incidentes especiales, etc.	- Capacidad para exfiltrar información muy valiosa, en cantidad considerable y en poco tiempo. - Capacidad para tomar el control de los sistemas sensibles, en cantidad y en poco tiempo.
MUY ALTO	Interrupción de los Servicios IT / Exfiltración de datos / Compromiso de los servicios	- Códigos dañinos confirmados de Alto Impacto (RAT, troyanos enviando datos, rootkit, etc.) - Ataques externos con éxito.	- Capacidad para exfiltrar información valiosa, en cantidad apreciable. - Capacidad para tomar el control de los sistemas sensibles, en cantidad considerable.
ALTO	Toma de control de los sistemas / Robo y publicación o venta de información sustraída / Ciberdelito / Suplantación	- Códigos dañinos de Medio Impacto (virus, gusanos, troyanos). - Ataques externos – compromiso de servicios no esenciales (DoS / DDoS). - Tráfico DNS con dominios relacionados con APTs o campañas de malware. - Accesos no autorizados / Suplantación / Sabotaje. - Cross-Site Scripting / Inyección SQL. - Spear phishing / pharming	- Capacidad para exfiltrar información valiosa. - Capacidad para tomar el control de ciertos sistemas.
MEDIO	Logro o incremento significativo de capacidades ofensivas / Desfiguración de páginas web / Manipulación de información	- Descargas de archivos sospechosos. - Contactos con dominios o direcciones IP sospechosas. - Escáneres de activos y vulnerabilidades. - Códigos dañinos de Bajo Impacto (adware, spyware, etc.) - Sniffing / Ingeniería social.	- Capacidad para exfiltrar un volumen apreciable de información. - Capacidad para tomar el control de algún sistema.
BAJO	Ataques a la imagen / menoscabo / Errores y fallos	- Políticas. - Spam sin adjuntos. - Software desactualizado. - Acoso / coacción / comentarios ofensivos. - Error humano / Fallo HW-SW.	- Escasa capacidad para exfiltrar un volumen apreciable de información. - Nula o escasa capacidad para tomar el control de sistemas.



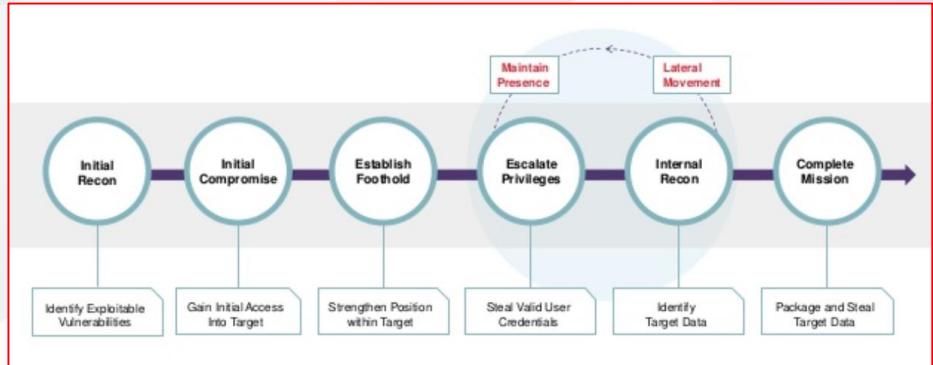
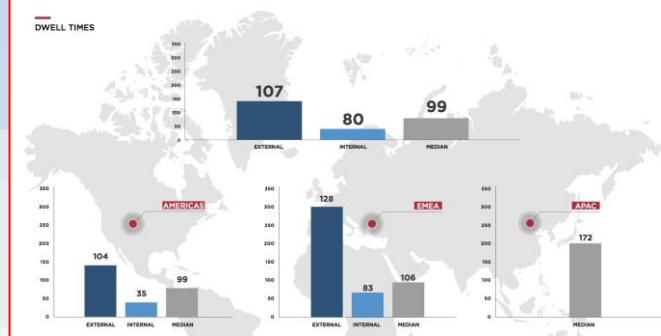
# Consciencia de situación

- Manteniendo el foco de negocio
  - Mirar alrededor
  - Estado de alerta
  - Capacidad de reacción
    - Bloquear amenazas
    - Minimizar pérdidas
  - Resiliencia: seguir en contingencia y recuperarse



# Afrontar la brecha

- Entrenamiento
- Detección
- Análisis de contexto
- Asignación de gravedad: relación con la pérdida potencial (análisis de riesgos)
  - Leve
  - Media
  - Alta
- Planes de respuesta alternativos
- Proceso de toma de decisiones
- Activación del plan de respuesta
  - Organización
  - Comunicación: interna /externa
  - Ejecución
- Aprendizaje y mejora
- Entrenamiento



# Suplantación

## Evolución de las técnicas del atacante



- Newly Registered Domains



- Looks-Like & Sounds



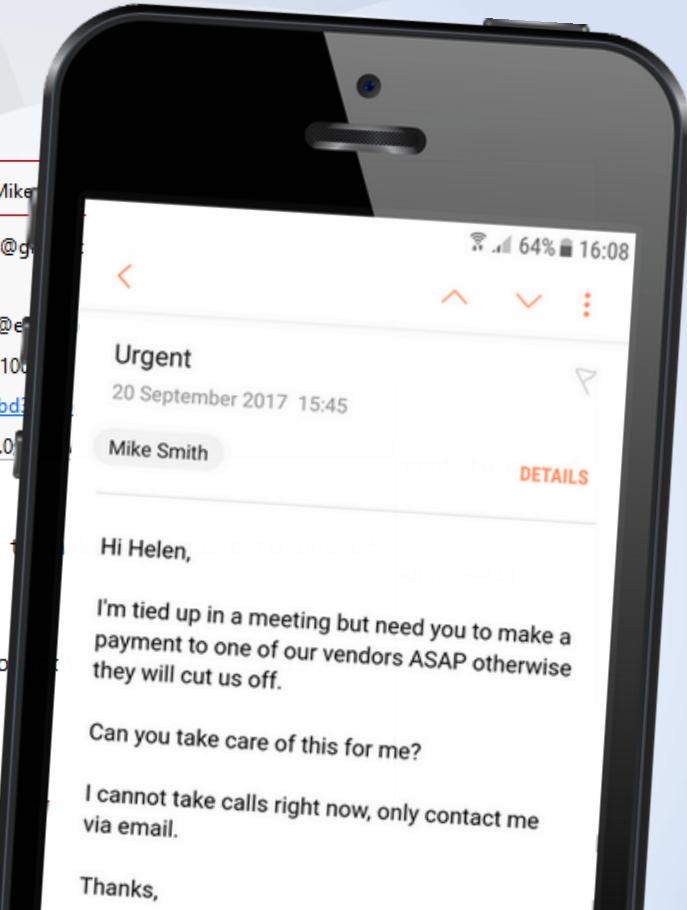
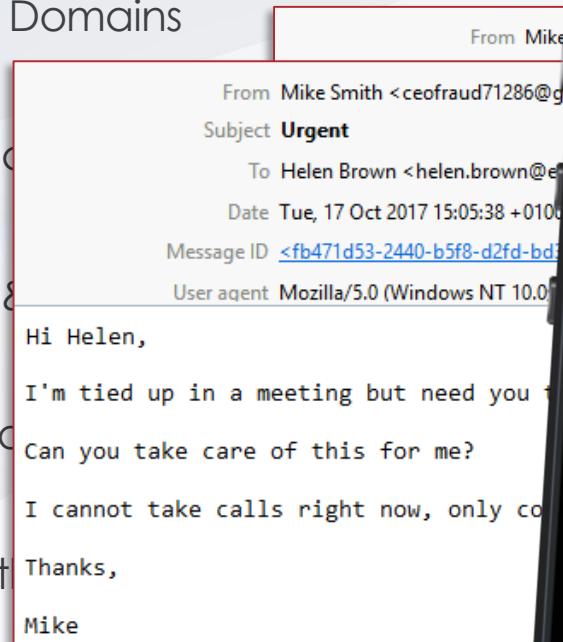
- Reply-to-Address



- Friendly Display Name

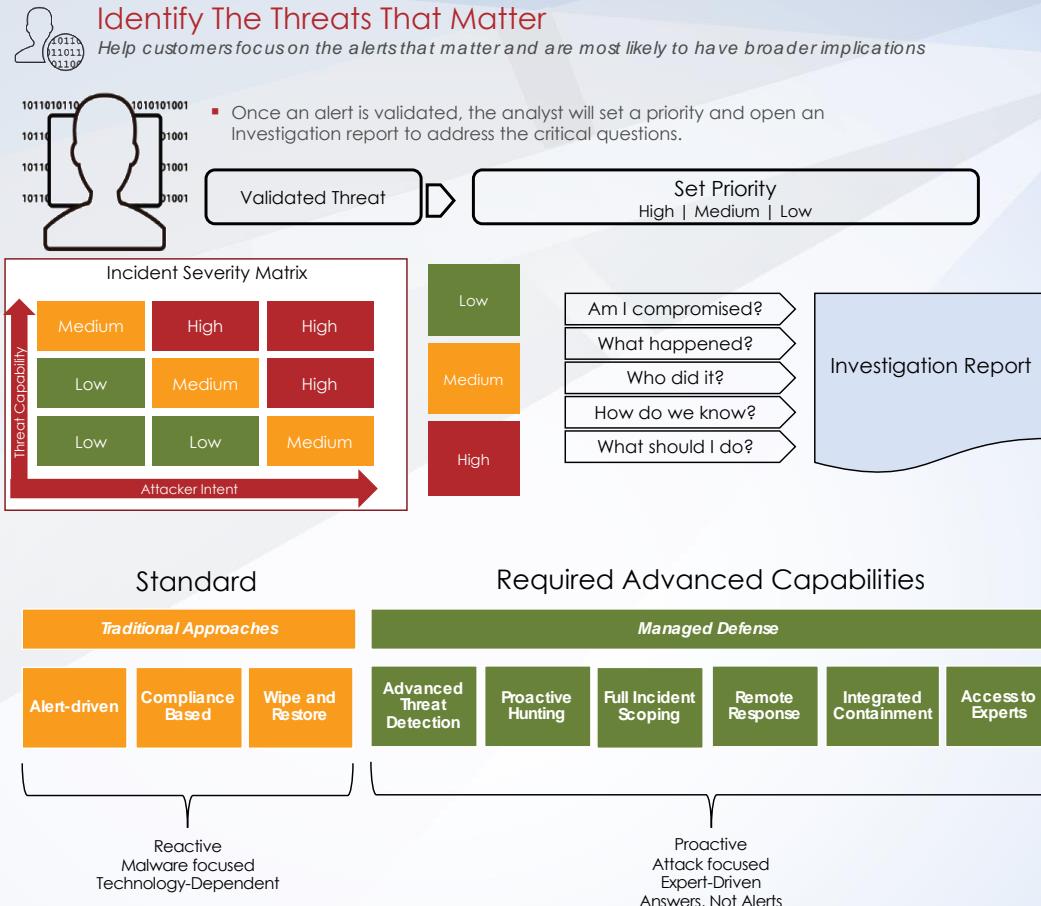


- CEO Fraud Algorithm



# Detección

- Eficacia: detectar los hechos relevantes
  - Positivos
  - Todos: minimizar falsos negativos
- Eficiencia: hacer el mejor uso de los recursos
  - Minimizar falsos positivos
- Capacidad de ejecución



# Ciberseguridad corporativa

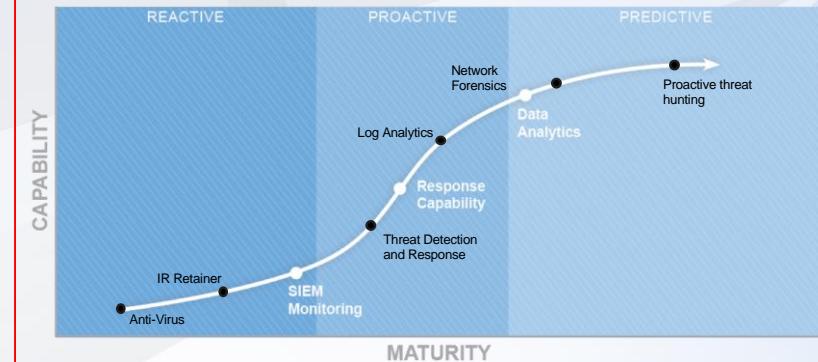
## ■ Alcance

- Corporación / Negocios
- IT / OT
- Interno / Proveedores

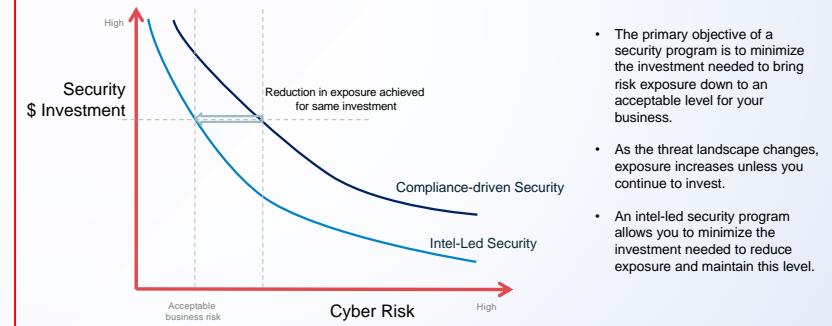
## ■ Modelo: Capacidades

- Propias
- Híbridas
- Externalizadas

Planning Your Security Programme Progression

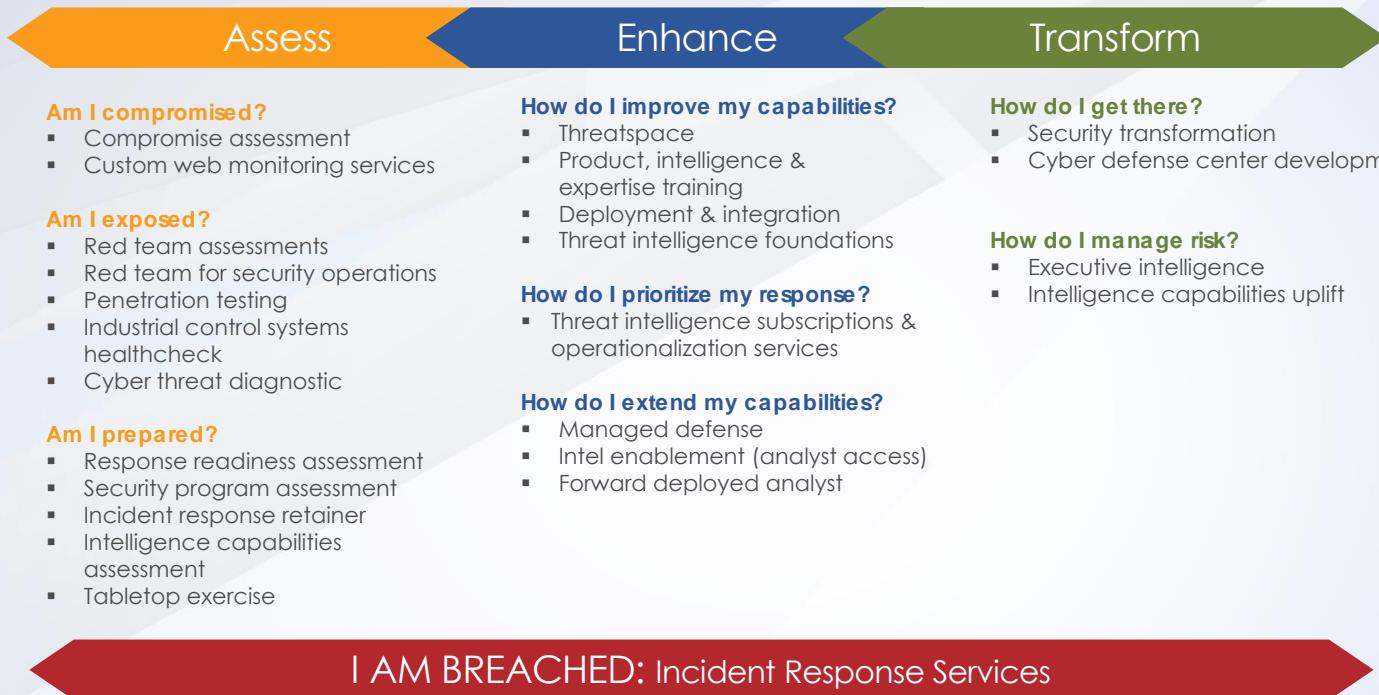


Appropriate Security: Aligning Security Investment to your Risk



# Enfoque de trabajo

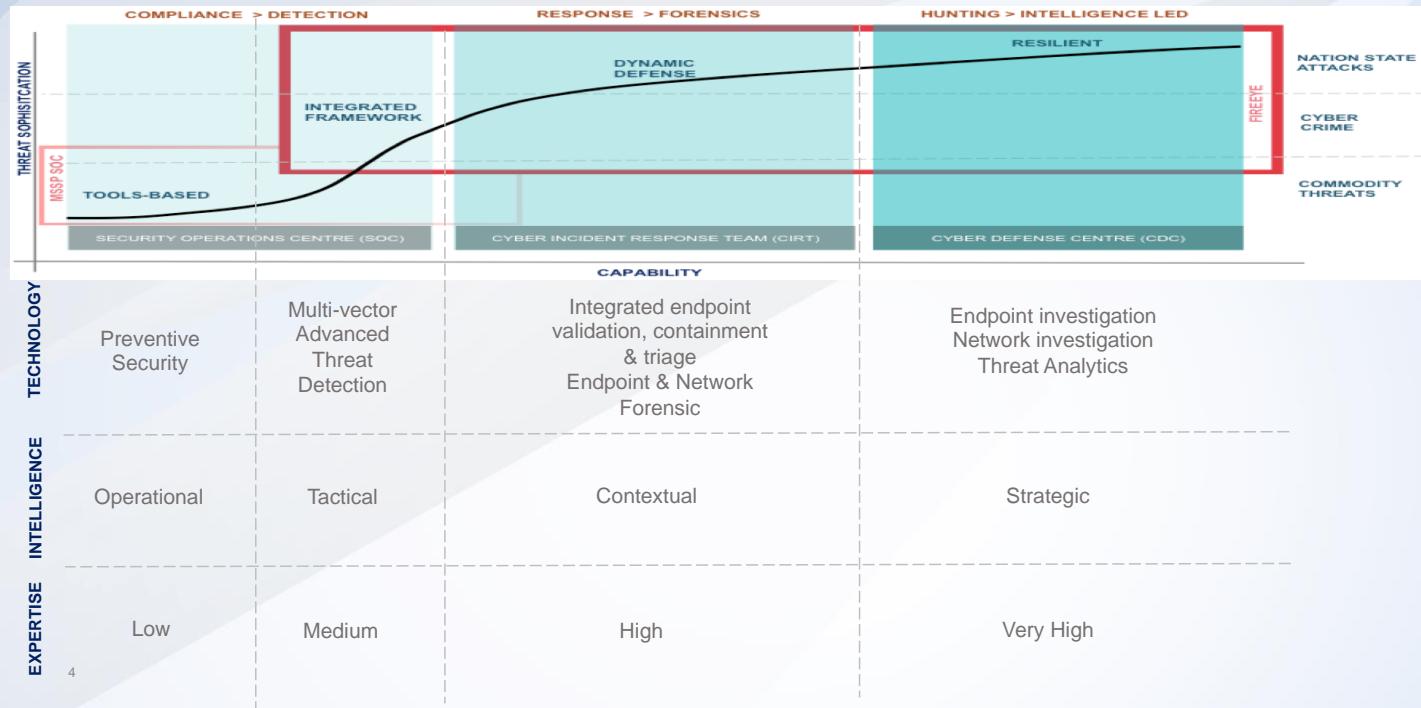
## Combined Intelligence & Services Portfolio



# Madurez

## Risk Mitigation against Advanced Attacks

FireEye's goal is to support you defend from the consequences of advanced cyber attacks by improving security maturity.



# Incident Response Retainer

- Preparar la respuesta sin la tensión de un incidente
- Respaldo de una organización con competencias contra las amenazas reales
- Línea de base de capacidades independiente del estado de madurez

	IRR DESCRIPTION	SLA
Tier 1	<b>Description</b> <ul style="list-style-type: none"><li>Basic terms and conditions for incident response services</li><li>Access to 24/7 hotline and email for incident response services request</li><li>Access to Mandiant incident response support with Mandiant technology stack</li></ul>	No Cost - Best Effort SLA
Tier 2	<b>Description</b> <ul style="list-style-type: none"><li>Basic terms and conditions for incident response services</li><li>Access to 24/7 hotline and email for incident response services request</li><li>Incident Preparedness Service</li><li>Access to Mandiant technology stack</li><li>Block of pre-paid support hours</li><li>Mandiant incident response support at a discounted rate</li><li>Additional support hours at a discounted rate</li></ul>	Prepaid Hours with Guaranteed SLA
Tier 3	<b>Description</b> <ul style="list-style-type: none"><li>Basic terms and conditions for incident response services</li><li>Access to 24/7 hotline and email for incident response services request</li><li>Incident Preparedness Service</li><li>Access to Mandiant technology stack</li><li>Prepaid Mandiant consulting services</li><li>Mandiant incident response support at discounted rate</li></ul>	Prepaid Services with Guaranteed SLA

1 Delivery to commence within the covered period  
2 Upon declaration acceptance

Tipo de incidente	Supuesto	Recursos	Presupuesto
No hay incidente	Incidente que se resuelve con operación de sistemas	Cualificación de Fireeye-Mandiant: no se actúa y no se consumen recursos	
Mínimo	Incidente en una sede, que se resuelve con dedicación de 25 horas	No se requiere despliegue de tecnología gracias a la información disponible suficiente. Se factura el mínimo de 40 horas.	
Grave en un país (local, esfuerzo bajo)	Incidente en una sede grande con esfuerzo bajo (5 semanas de 1 consultor)	Se despliega tecnología PX y HX para una sede, con viajes y 200 horas de consultor	
Grave en 3 países (multisede, afectación del negocio en el país, esfuerzo medio)	Incidente detectado en 3 países con 6 sedes involucradas, y un consultor dedicado dos meses	Se despliega tecnología PX y HX en las sedes de los países involucrados, con un consultor y viajes	
Muy grave en todos los países (muchas sedes, afectación alta del negocio, esfuerzo alto)	Incidente que afecta a todos los países, 25 sedes y dos consultores dedicados 6 meses	Se despliega equipamiento en todos los puestos de trabajo y servidores, y en todas las redes. Dos consultores trabajando 6 meses	

Pérdida estimada >

# Priorizar

- El perfil de la amenaza cambia
  - Pasado reciente:
    - Malware: nuevas capacidades de detección
    - Tráfico de red: opaco por el cifrado
  - Actualidad
    - Correo: alta capacidad de conseguir resultados con esfuerzo reducido
    - Texto en vez de software: pasar desapercibido
    - Suplantación de identidad

## ◆ Medidas higiénicas

- ▶ Concienciación y educación
- ▶ Entrenamiento en respuesta a incidentes
- ▶ Protección del e-mail
- ▶ Segundo factor de autenticación
- ▶ Capacidad en el endpoint
- ▶ Recursos especializados
  - Propios
  - Ajenos

# Inteligencia y equipo

## ■ S21-Nextel y la función de gestión de la ciberseguridad

- Conocimiento de negocio y riesgos del cliente
- Conocimiento de la amenaza
- Actitud
  - Alerta
  - Análisis y planes de acción
  - Procesos de toma de decisiones
- Ejecución
  - Conocimiento => conciencia de situación
  - Tecnología = herramientas



# GRACIAS