Soluciones Tecnólogicas

- Server, Network & End Point Protection.
- Web, Email, Data & Mobile Security.

Servicios Administrados de Seguridad

- Unified Security Management & Threat Intelligence.
- Ethical Hacking and Vulnerability Assestments.
- Security Operation Center Monitoring.
- Incident Response.

Servicios de Consultoría

- Sistemas de Gestión: Seguridad de TI.
- Continuidad de Negocio, Riesgos, Cumplimiento.
- SGSI - BCP - Risks - GRC

TECNOLOGÍAS GLOBALES PARA LA SEGURIDAD DE LA INFORMACIÓN

www.globalteksecurity.com

Sector Financiero – Proyectos de alta complejidad

globaltek SECURITY

fna AHORRO Construyendo Sociedad

Banco Agrario de Colombia

BCV

POSITIVA COMPAÑIA DE SEGUROS

BANCOLDEX

Superintendencia Financiera de Colombia

Clientes Sector Público (I)

globaltek SECURITY

MINDEFENSA

MinAmbiente
Ministerio de Ambiente y Desarrollo Sostenible

MinMinas
Ministerio de Minas y Energía

Cancillería
Ministerio de Relaciones Exteriores

MinJusticia
Ministerio de Justicia y del Derecho

FUNCIÓN PÚBLICA
Departamento Administrativo de la Función Pública

MinVivienda
Ministerio de Vivienda

MinInterior
Ministerio del Interior

Clientes Sector Público (II)

globaltek SECURITY

POSITIVA COMPAÑIA DE SEGUROS

Banco Agrario de Colombia

UAE - FONDO NACIONAL DE ESTUPEFACIENTES
Ministerio de la Protección Social

Colpensiones

UNIVERSIDAD NACIONAL DE COLOMBIA

INSTITUTO COLOMBIANO DE ANTROPOLOGÍA E HISTORIA

Superintendencia Financiera de Colombia

Clientes Sector Público (III)

globaltek SECURITY

clubmilitar

Innovación, cultura de servicio y altos estándares de calidad.

Centro Nacional de Memoria Histórica

ALCALDÍA MAYOR DE BOGOTÁ D.C. | BOGOTÁ MEJOR PARA TODOS

SECRETARÍA DE DESARROLLO ECONÓMICO

Desarrollo Económico, Industria y Turismo

ALCALDÍA MAYOR DE BOGOTÁ D.C. | BOGOTÁ MEJOR PARA TODOS

HOSPITAL CENTRO ORIENTE

II NIVEL de atención E.S.E

Mapa del Sitio Encuestas Empleo Glosar

ALCALDÍA MAYOR DE BOGOTÁ D.C. | BOGOTÁ MEJOR PARA TODOS

Fondo de Prestaciones Económicas, Cesantías y Pensiones FONCEP

SECTOR HACIENDA

HOSPITAL SAN BLAS II NIVEL E.S.E.

Trabajamos para mejorar su calidad de vida

Alcaldía de Medellín

Medellín todos por la vida

Soluciones de protección contra robo o fuga de información confidencial

globaltek SECURITY

FORCEPOINT POWERED BY Raytheon

MINDEFENSA

Ajover

Banco Agrario de Colombia

Colpensiones

POSITIVA COMPAÑIA DE SEGUROS

Famisanar EPS 20 AÑOS PORQUE EN LA SALUD DE COLOMBIA SE PUEDE CONFIAR

fna AHORRO Construyendo Sociedad

BCV

GLORIA

PETROAMAZONAS EP

Implementación de Sistemas de Gestión de Seguridad de la información SGSI

globaltek SECURITY

MINDEFENSA

Cancillería
Ministerio de Relaciones Exteriores

FUNCIÓN PÚBLICA
Departamento Administrativo de la Función Pública

Centro de Memoria

USPEC Unidad de Servicios Penitenciarios y Carcelarios

TODOS POR UN NUEVO PAÍS
PAZ EQUIDAD EDUCACIÓN

MINJUSTICIA

INTERACTIVO

MINEDUCACIÓN

icfes mejor saber

TODOS POR UN NUEVO PAÍS
PAZ EQUIDAD EDUCACIÓN

CRC
Comisión de Regulación de Comunicaciones
REPÚBLICA DE COLOMBIA

fna AHORRO
Construyendo Sociedad

Aseguradora Solidaria de Colombia
¡ Siempre junto a ti !

Proyectos de alto nivel Incluyendo Alien Vault con acuerdos de calidad de servicio (SLAs)

globaltek SECURITY

MINDEFENSA

ARMADA NACIONAL
REPÚBLICA DE COLOMBIA

Cancillería
Ministerio de Relaciones Exteriores

USPEC Unidad de Servicios Penitenciarios y Carcelarios

TODOS POR UN NUEVO PAÍS
PAZ EQUIDAD EDUCACIÓN

MINJUSTICIA

POSITIVA
COMPAÑIA DE SEGUROS

fna AHORRO
Construyendo Sociedad

Colpensiones

Banco Agrario de Colombia

globaltek SECURITY

FORCEPOINT
POWERED BY Raytheon

Whitepaper

Investigative Analytics: An End to the Era of Uncertainty

No one is immune to cybercrime. The days of absolute protection are over. The crush of tech consumerism by users, matched with mobility/Bring Your Own Device and the demise of the traditional perimeter, has ushered in a New Reality.

INVESTIGATIVE ANALYTICS BRINGS AN END TO AN ERA OF UNCERTAINTY

- Hoy en dia, los riesgos son inevitables. Se trata de tener conciencia de ellos y gestionarlos de manera proactiva, con el proposito de reducir los tiempos de respuesta a los incidentes de seguridad.
- Por qué las respuestas efectivas a los incidentes (aquellas que no solo arreglan el problema sino que ademas toman las medidas para que no vuelvan a suceder) toman tanto tiempo?

AVERAGE NUMBER OF DAYS REQUIRED TO RESOLVE A COMPROMISE, ACCORDING TO ATTACK CATEGORY

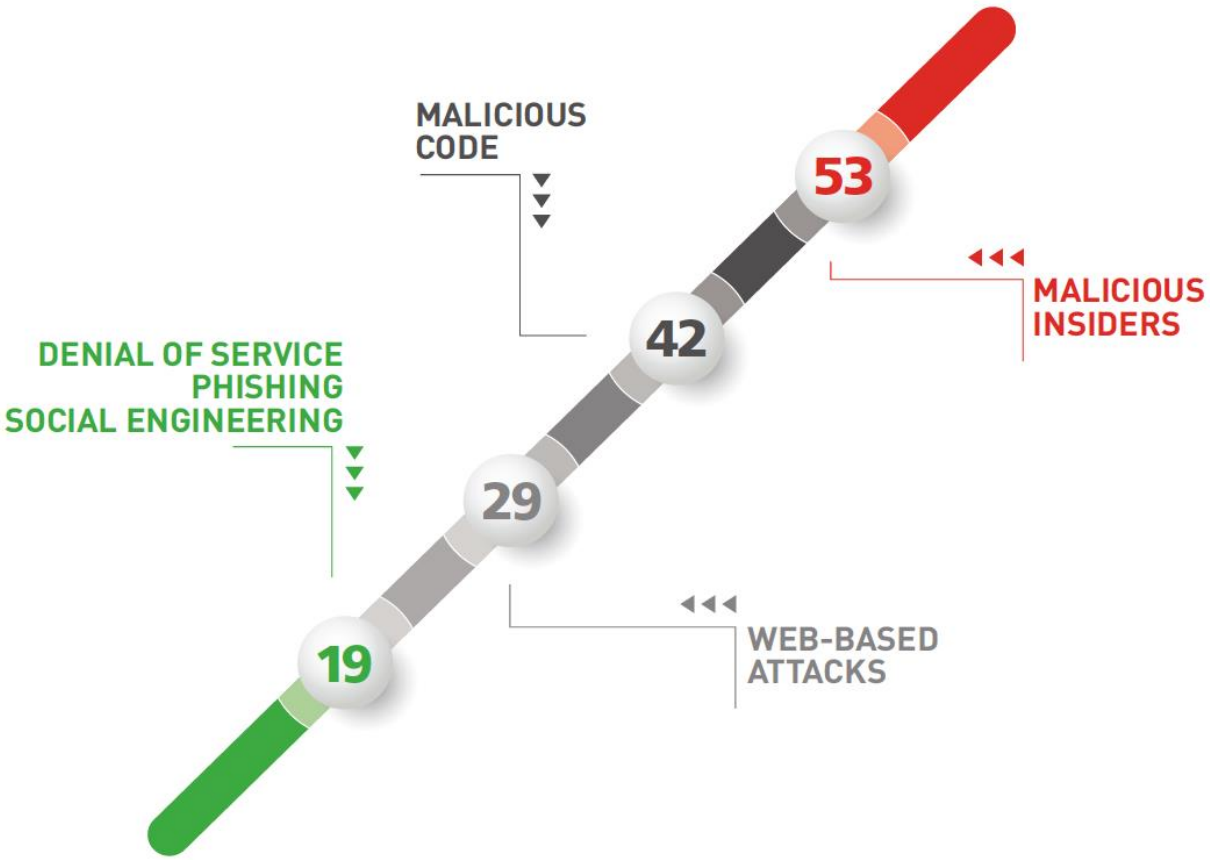

Figure 1. Source: Ponemon Institute

INVESTIGATIVE ANALYTICS BRINGS AN END TO AN ERA OF UNCERTAINTY

- Debido al costo de los incidentes y a otros factores, hay urgencia de mejorar las estrategias y las soluciones de ciberseguridad.
- Las innovaciones tecnologicas en analitica investigativa permiten conocer no sólo qué sucedió dentro de la red, sino cuándo, dónde, y cómo sucedió.

TOP SOURCES OF LOSSES DUE TO COMPROMISES

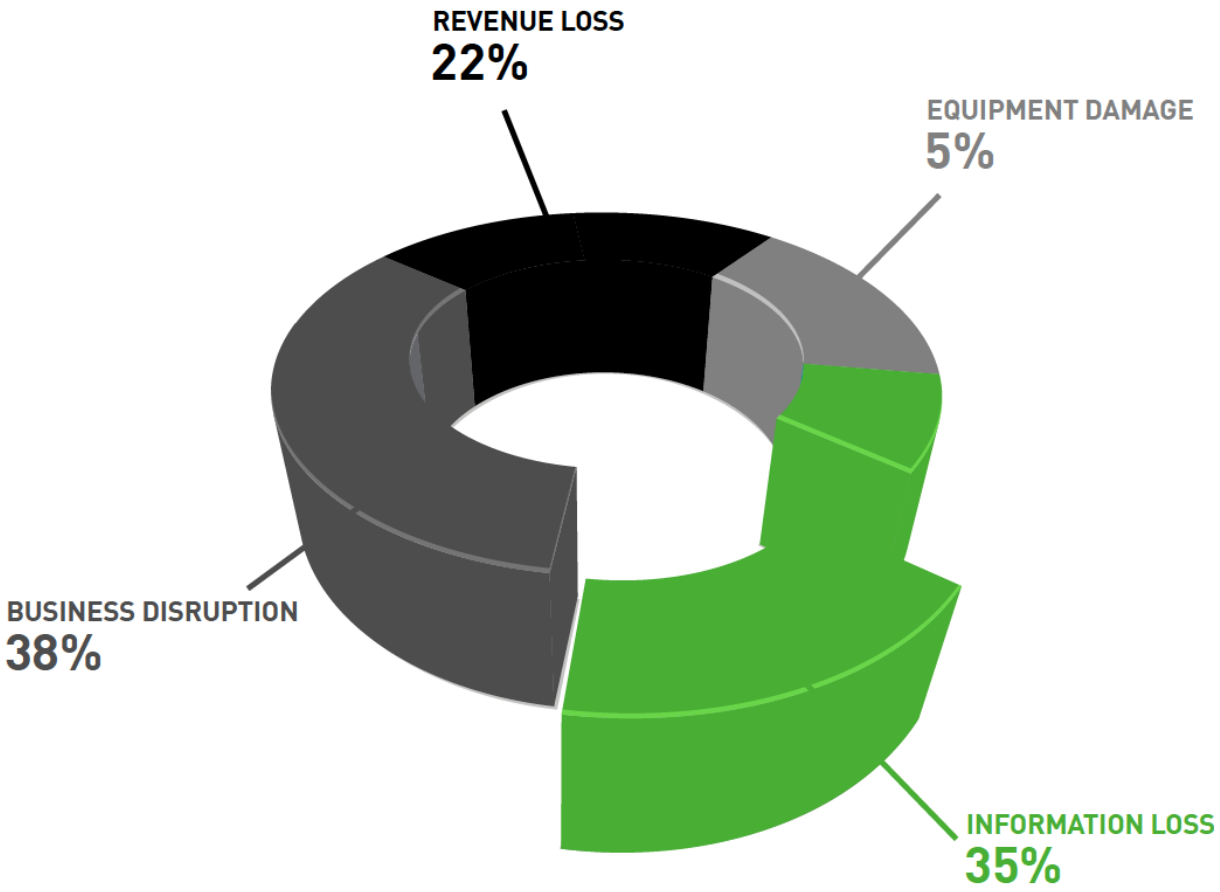

Figure 3. Source: Ponemon Institute

INVESTIGATIVE ANALYTICS BRINGS AN END TO AN ERA OF UNCERTAINTY

- Pocas organizaciones usan capacidades analiticas sobre su data o su Big Data para hacer inteligencia avanzada de amenazas como parte de sus esfuerzos de seguridad y menos del 10% afirman que esten utilizando herramientas de análisis de datos no estructurados.
- Usando "Base lines", se pueden determinar comportamientos inusuales de los sistemas y/o de los usuarios que puedan llevar a los equipos de seguridad a un analisis mas detallado de los datos.
- La demanda por "Security Analitics" esta aumentando a mayor ritmo incluso que la analitica de negocios.

INVESTIGATIVE ANALYTICS BRINGS AN END TO AN ERA OF UNCERTAINTY

- 1er Desafio: Conciencia diaria de la situacion
- Cerca de 2/3 partes de los Information Security Officers (ISOs) citan la inhabilidad para recolectar suficientes datos operacionales y de seguridad –para hacer asociaciones- como el principal impedimento para descubrir brechas de seguridad, responder y tomar desiciones efectivas en el dia a dia.

SYSTEMS CURRENTLY IN PLACE AMONG ORGANIZATIONS TO COLLECT, ANALYZE AND CORRELATE LARGE QUANTITIES OF SECURITY AND EVENT DATA

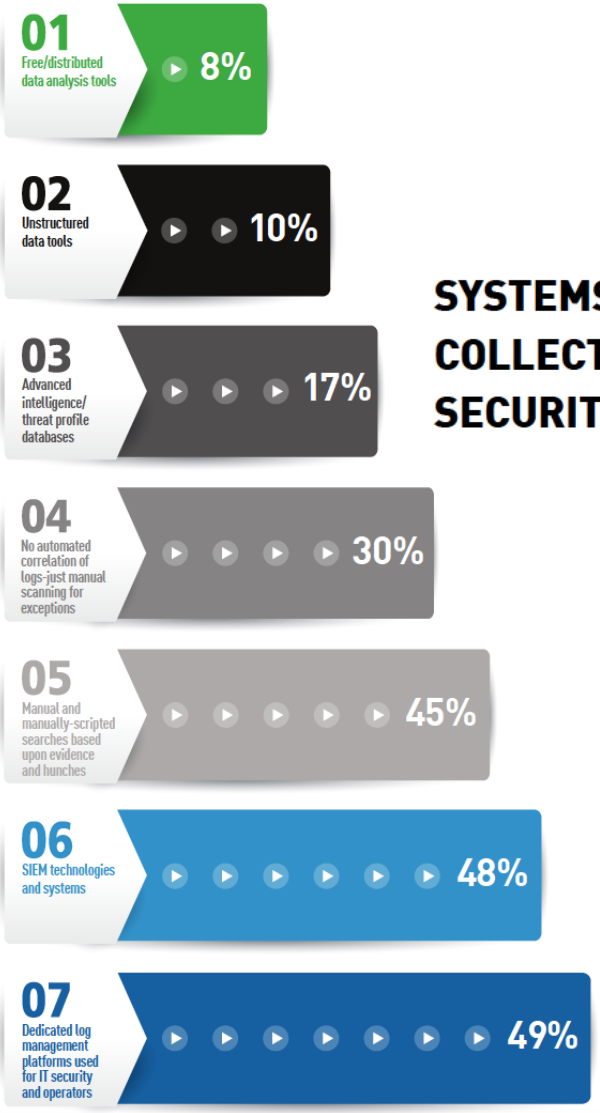

Figure 4. Source: SANS Institute

SYSTEMS CURRENTLY IN PLACE AMONG ORGANIZATIONS TO COLLECT, ANALYZE AND CORRELATE LARGE QUANTITIES OF SECURITY AND EVENT DATA

INVESTIGATIVE ANALYTICS BRINGS AN END TO AN ERA OF UNCERTAINTY

- 2do Desafio: Respuesta Rapida a Incidentes de seguridad
- Se debe reducir el tiempo requerido para las 4 fases de respuesta a incidentes: prevencion, deteccion, respuesta y recuperacion.
- Elementos involucrados: tecnologicos & Factores humanos.
- Equipo de trabajo insuficiente o mal capacitado.

INVESTIGATIVE ANALYTICS BRINGS AN END TO AN ERA OF UNCERTAINTY

- 3er Desafio: Foco en las mejoras futuras
- Sin conciencia de la situacion del dia a dia, sin una respuesta rapida y una vision a largo plazo, los Information Security Officers se ven atrapados en una tormenta perfecta de problemas que solo benefician a los atacantes.
- Ellos intentaran crear una foto completa de su incidente, pero con las herramientas actuales, procesos y agendas personales, se les nublara su visibilidad, dejando incertidumbre y confusion para actuar prontamente.

WHAT ORGANIZATIONS LACK IN THREAT INTELLIGENCE CORRELATION CAPABILITIES

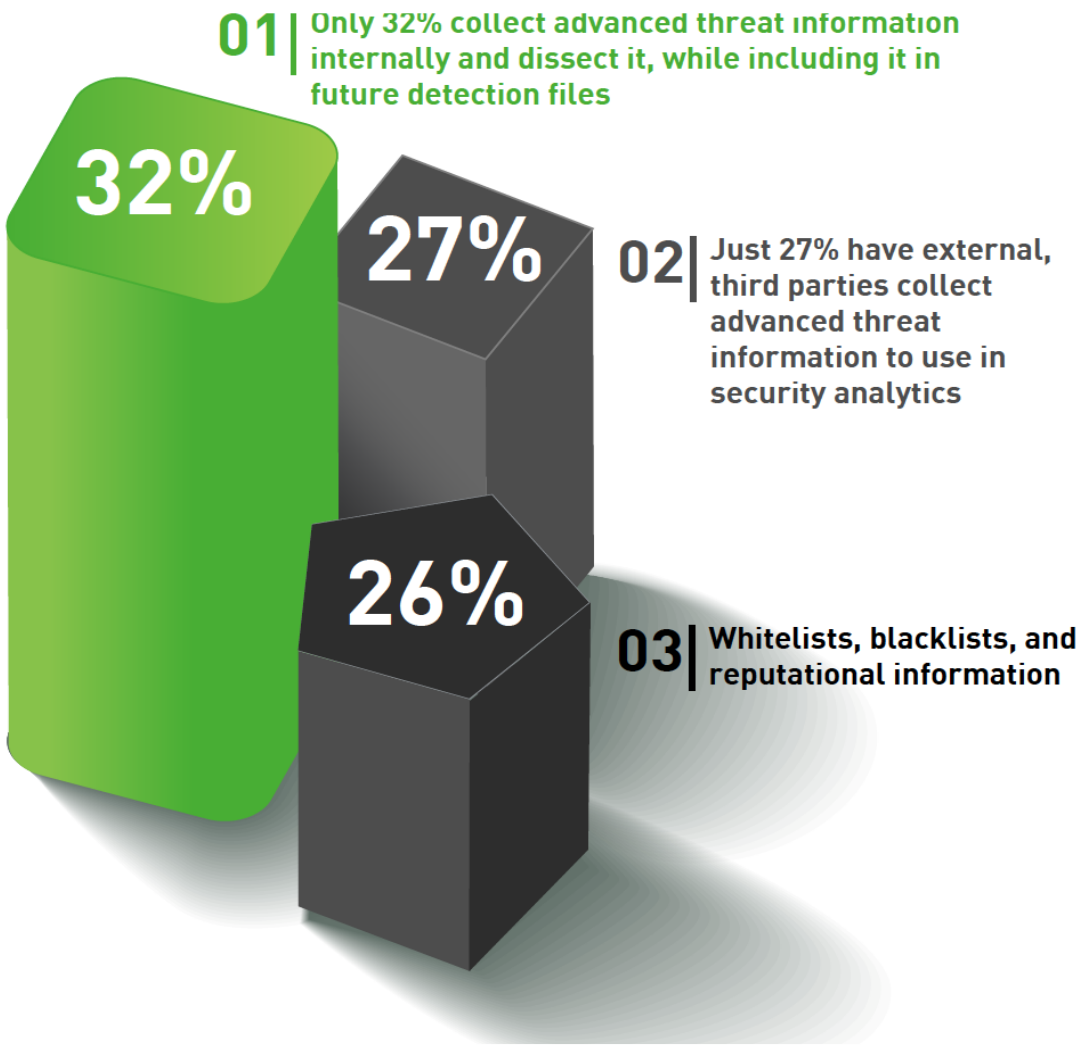

Figure 5. Source: SANS Institute

INVESTIGATIVE ANALYTICS BRINGS AN END TO AN ERA OF UNCERTAINTY

- Hay una razon para que el mercado de soluciones de analitica de seguridad este creciendo a una rata tan impresionante: Los productos estan conduciendo a los ISOs para que nunca mas vuelvan a decir: “No sé lo que sucedió”.

INVESTIGATIVE ANALYTICS BRINGS AN END TO AN ERA OF UNCERTAINTY

- Con la analitica, se establece una visión inigualable sobre todos los aspectos fundamentales, incluyendo factores forenses- ¿quién hizo qué, cuándo, dónde lo hicieron, y cómo? – logrando conciencia situacional total.
- Con el monitoreo automatico y la Identificación de anomalías, ya no habra mas la interminable e inutil actividad manual de busqueda de datos.
- Se les dará a los ISOs un nuevo sentido de autoridad y credibilidad que les genera reconocimiento como lideres estrategicos. Dado que ¾ partes de los Ejecutivos (C) no sienten que los ISOs sean considerados miembros del equipo de lideres de la organización.

INVESTIGATIVE ANALYTICS BRINGS AN END TO AN ERA OF UNCERTAINTY

- La plataforma Forcepoint™ SureView¨ Analytics es una herramienta de busqueda investigativa y de analitica que reduce dramaticamente el tiempo requerido para ocuparse de las 4 fases de la respuesta a incidentes.
- Permite a los ISOs rapida y facilmente acceder, centralizar, y examinar grandes cantidades de datos de multiples fuentes como appliances, firewalls, dispositivos de red, servidores y aplicaciones y prontamente transformar los hallazgos en inteligencia “accionable”.

INVESTIGATIVE ANALYTICS BRINGS AN END TO AN ERA OF UNCERTAINTY

SureView Analytics le permite a las organizaciones:

- Informacion diaria y notas breves de inteligencia de seguridad que permiten conciencia de la situacion incluyendo detalles sobre comportamiento sospechoso y visibilidad de aspectos preocupantes para los ISOs como ataques a otras organizaciones, infecciones de red, correlacion de eventos, visualizacion y analisis de informacion.
- Como resultado, el tiempo de respuesta a incidentes se reduce dramaticamente.
- Investigaciones profundas asociados con vulnerabilidades/ataques, de tal manera que los equipos de seguridad puedan explorar los detalles de lo que sucedió, donde, cuando y cómo.

INVESTIGATIVE ANALYTICS BRINGS AN END TO AN ERA OF UNCERTAINTY

Conclusiones

- ISOs y sus equipos enfrentan cada dia mayores retos y una avalancha de nuevos ataques.
- Ahora, pueden lograr estas capacidades fundamentales: Conciencia de la seguridad de sus sistemas y una respuesta rapida a incidentes.
- Se puede salvar a las organizaciones de perdidas de datos, cortes en la productividad, caidas de las operaciones, daños reputacionales y/o riesgos regulatorios.