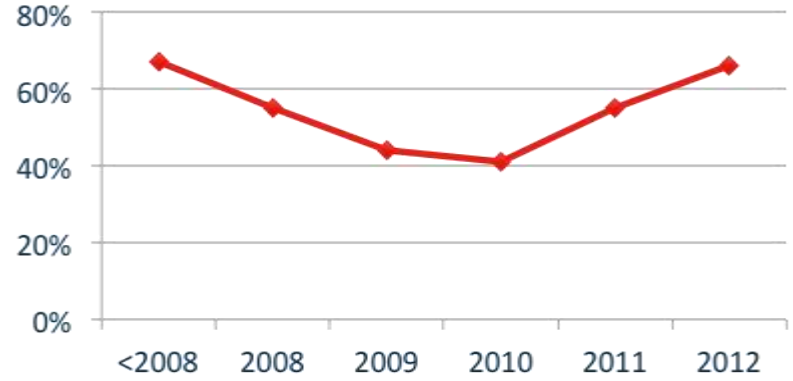
DAMBALLA

Automated Breach Defense

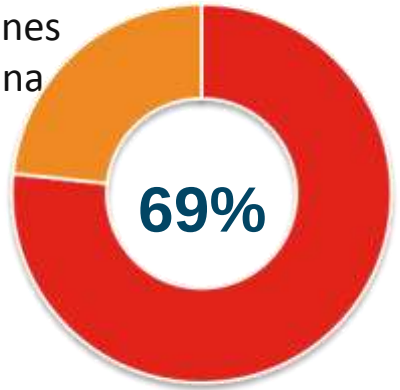
¿Por qué? Protección contra amenazas avanzadas y la contención de las mismas?

Porcentaje de las violaciones que quedan sin descubrir durante meses o más



"Hay un acuerdo generalizado de que los ataques avanzaron y están rebasando, la seguridad tradicional basada en firmas ... La amenaza es real. Muchas organizaciones están en entredicho con su seguridad, pero simplemente no lo saben ".
– Gartner, Inc., 2012

69% de las violaciones fueron vistos por una parte externa
Y solo el 9% fueron vistos,
por los clientes.
22% de malware, no se ha identificado



"Prevention is crucial, and we can't lose sight of that goal. But we must accept the fact that no barrier is impenetrable, and ***detection/response represents an extremely critical line of defense. Let's stop treating itlike a backup plan if things go wrong and start making it a core part of the plan****."*

– Verizon Data Breach Study 2013

DAMBALLA

Que tan grande es el problema y como se estima?

63%

De las empresas dicen que es sólo una cuestión de tiempo hasta que para estar implementando soluciones APT

JP Morgan Securities audit

32 days

El tiempo promedio para resolver un ataque cibernético conocido

$1.04M

El costo total promedio para la organización durante 32 días, dependiendo el impacto y el tamaño de esta.

DAMBALLA

Que tan grande es en terminos de recursos?

2/3's

De cada CISO, o responsables de TI, dicen que estan cortos de personal y por lo tanto, son vulnerables a las violaciones

JP Morgan Securities audit

86%

De los CISO dice sentir, falta de confianza en la capacidad de gestionar el riesgo debido a la falta de capacitacion y conocimiento del personal.

81%

De los líderes en seguridad dicen que los desafíos de falta de personal capacitado en Seguridad, seguirán siendo los mismos en los próximos 5 años.

DAMBALLA

Quien sabe lo que es un APT?

Hace cuanto tiempo has pensado en que, tus soluciones actuales de seguridad, no los son tanto? Y por que?

Quien puede decirnos por que no es facil identificar el Malware avanzado?

DAMBALLA

La Seguridad de Pila, ya es Vieja

Riesgo de Infeccion

Riesgo del negocio

ATTACK → **Prevention** → INFECTION → **Detection** → DAMAGE → **Response** Forensics

- Firewall
- IDS/IPS
- Web Security
- Email Security
- Sandboxing
- Host AV/IPS/FW

Los recursos, los esfuerzos de investigación y controles manuales, son ineficientes contra los ataques intensivos.
"¿Es esto, una alerta o un falso positivo?"

- IDS/IPS
- Web Security
- Logs/PCAPs

- Network DVR
- Forensics Client
- NBAD

ALERT & LOGS

SIEM
Single Pane of Glass

SOC

El Nuevo Modelo de Seguridad

INFECTION RISK

BUSINESS RISK

ATTACK → **Prevention** → INFECTION → **Detection** → DAMAGE → **Response** Forensics

- NGFW
- Endpoint Containment
- Sandboxing
- Email Gateway

LEGACY
Host AV/IPS/FW

Damballa llena el vacío de seguridad entre la prevención del fallo y su respuesta a incidentes

- Network DVR
- Forensics Client
- NBAD

ALERT & LOGS

SIEM
Single Pane of Glass

SOC

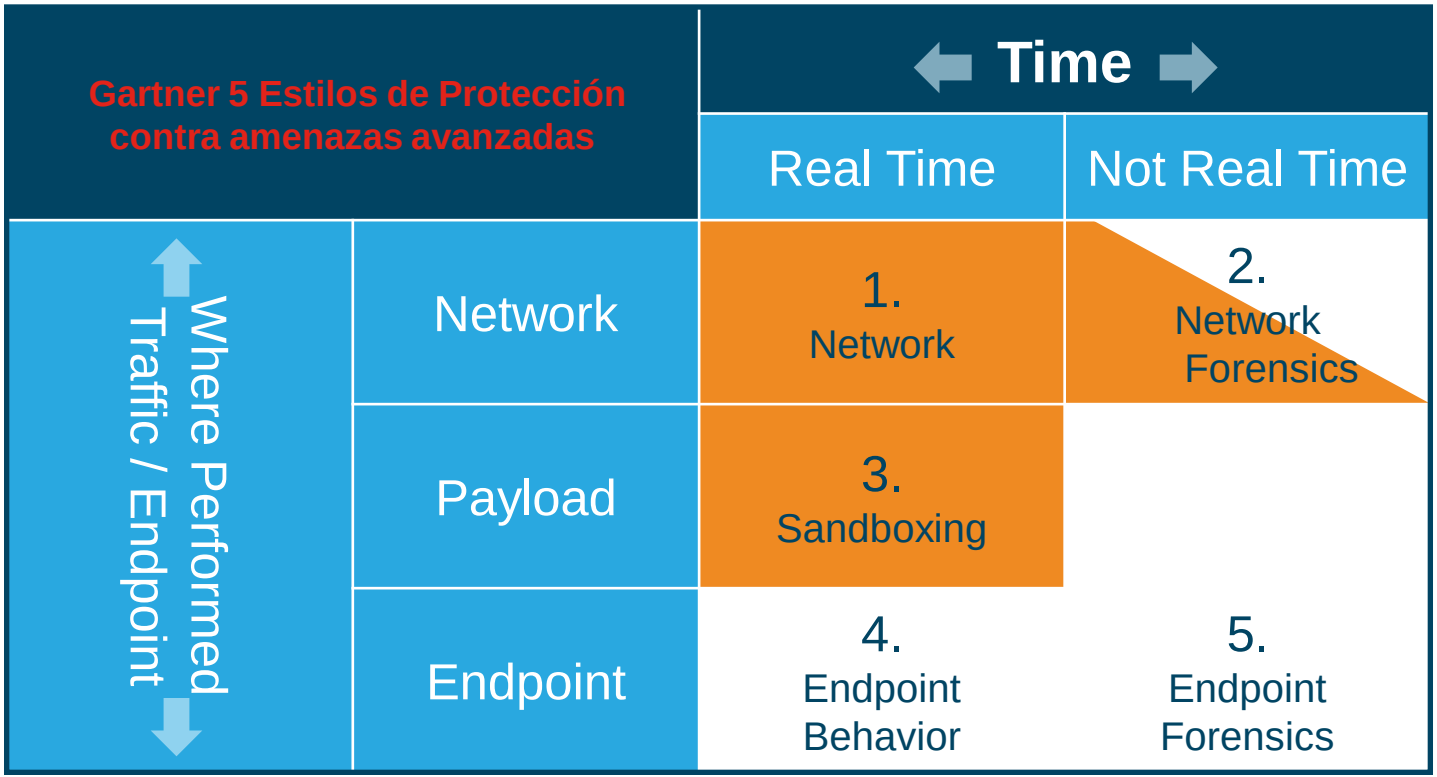
Damballa: Automated Breach Defense

- Identifica automáticamente las amenazas activas
  Con certeza
- Independientemente de la visibilidad o conocimientos previos de la muestra de malware, Infección vector O de la fuente
- Centrarse realmente en infecciones activas
  priorizar respuesta de alertas y control
  Proactivamente bloquear las infecciones no ha llegado a un vector de ataque

Enabling A
Breach Resistant Organization

DAMBALLA

Gartner 5 Estilos de Protección contra amenazas avanzadas.



"Las amenazas de hoy requieren un modelo de defensa en capas y actualizado que utilice tecnologías "de apoyo hacia adelante" en tres niveles:

la red, la carga útil (ejecutables, archivos y objetos Web) y de punto final (End Points) ... Las organizaciones deben implementar la tecnología "que vaya hacia adelante" de al menos dos de las tres capas estructurales (de red, de aplicaciones y end points).

- Gartner, Five Styles of Advanced Threat Defense, August 2013

DAMBALLA

Damballa permite a las organizaciones:
Rápidamente identificar amenazas activas
Con el 100% de Asertividad
Sin los esfuerzos de falta de recursos o retrasos
Independiente de tener una muestra de malware
Independientemente del tipo de malware, vector de infección, ataque o de la fuente

Como una organización basada en estandares de calidad. (Gobierno, Enterprise, Academicas)
Damballa ayudara a:
Rápidamente y eficientemente detener las pérdidas reales
Encuentrar las amenazas no detectadas previamente
Retira las amenazas que pueden causar pérdidas a la organización.
Aumentar la eficiencia y la eficacia del personal mediante la eliminación de atencion a alertas no confirmadas y Reducir drásticamente el riesgo global

Damballa Fail Safe, Si tomara accion de remediacion.

DAMBALLA

Contención avanzada de Amenazas: Descubrimiento Contextual y riesgos Analitico

Damballa crea, un analisis Automatizado y sofisticado, el análisis de redes en tiempo real, la aplicación de técnicas de deteccion y de evaluación de riesgos . Para "Detectar y responder“ como apoyo a las mejores prácticas.

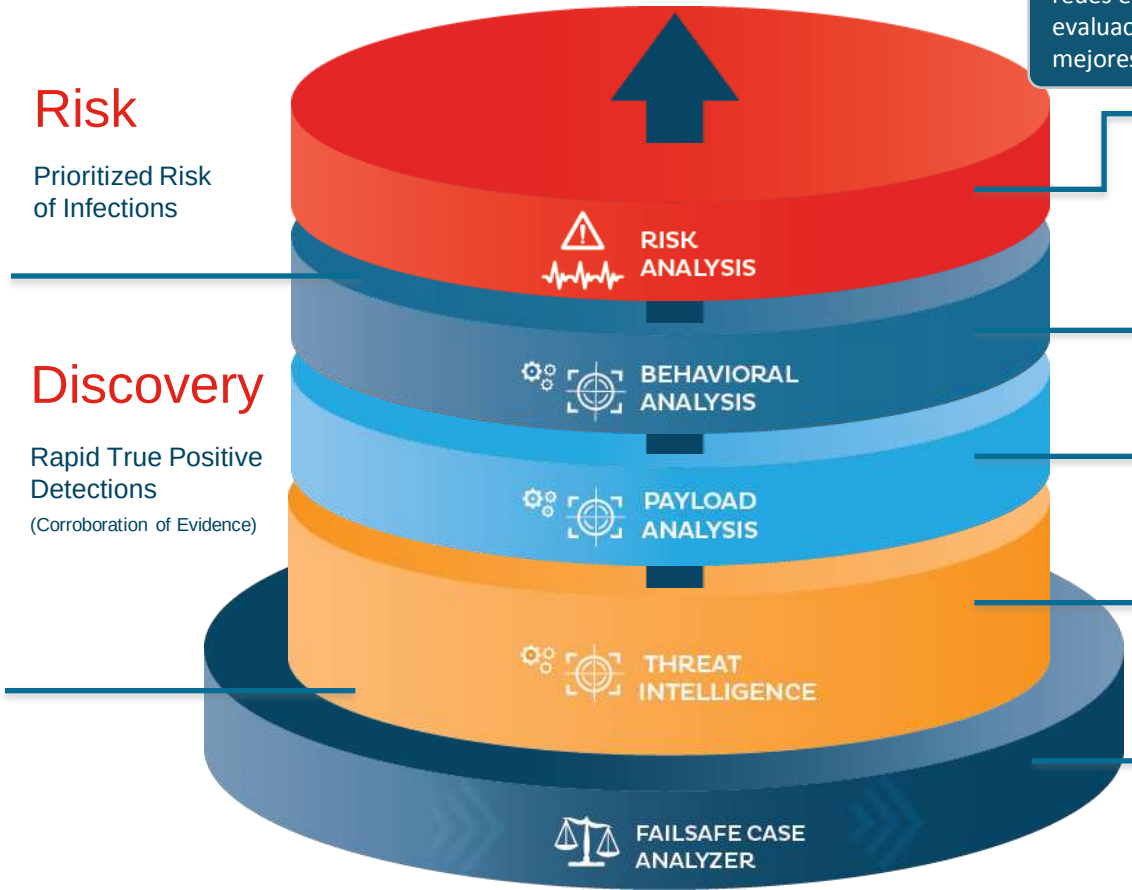
Risk

Prioritized Risk of Infections

Discovery

Rapid True Positive Detections

(Corroboration of Evidence)



- ✓ Data Transferred
- ✓ PCAPs
- ✓ Communication Success
- ✓ Malicious File Availability
- ✓ Sequence of Events
- ✓ Importance of Endpoint
- ✓ Malware Family Intent
- ✓ Severity
- ✓ AV Coverage

Damage Potential

- **Observed Activity?**
- **Which Device?**
- **Threat Intent?**

- ✓ Domain Fluxing
- ✓ Automation
- ✓ Execution
- ✓ Peer-To-Peer

- **Automated Malicious Activity**
- **Observed Evasion Tactics**

- ✓ File
- ✓ Request

- **Zero Day Files**
- **Suspicious HTTP Content**

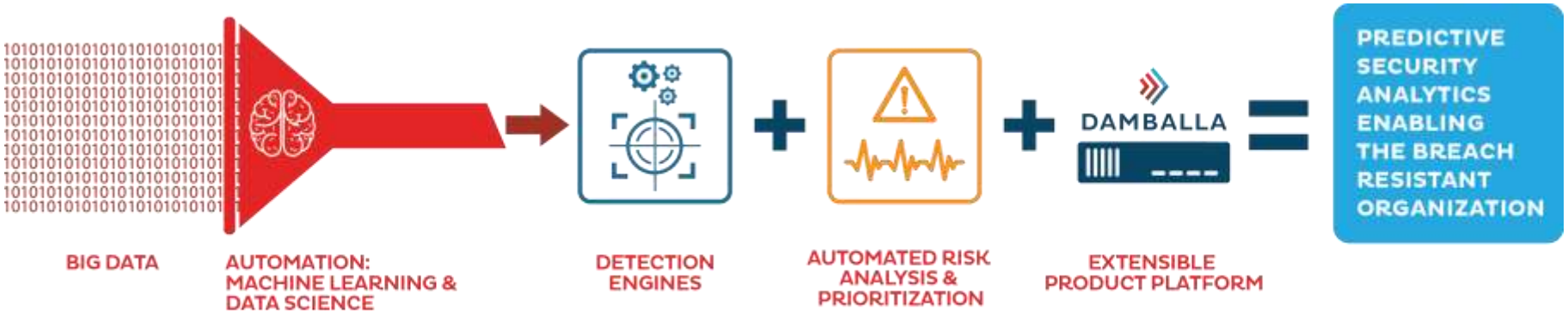
- ✓ Connection
- ✓ Query

- **Indicators of Compromise**
- **Threat Actors / Intent**

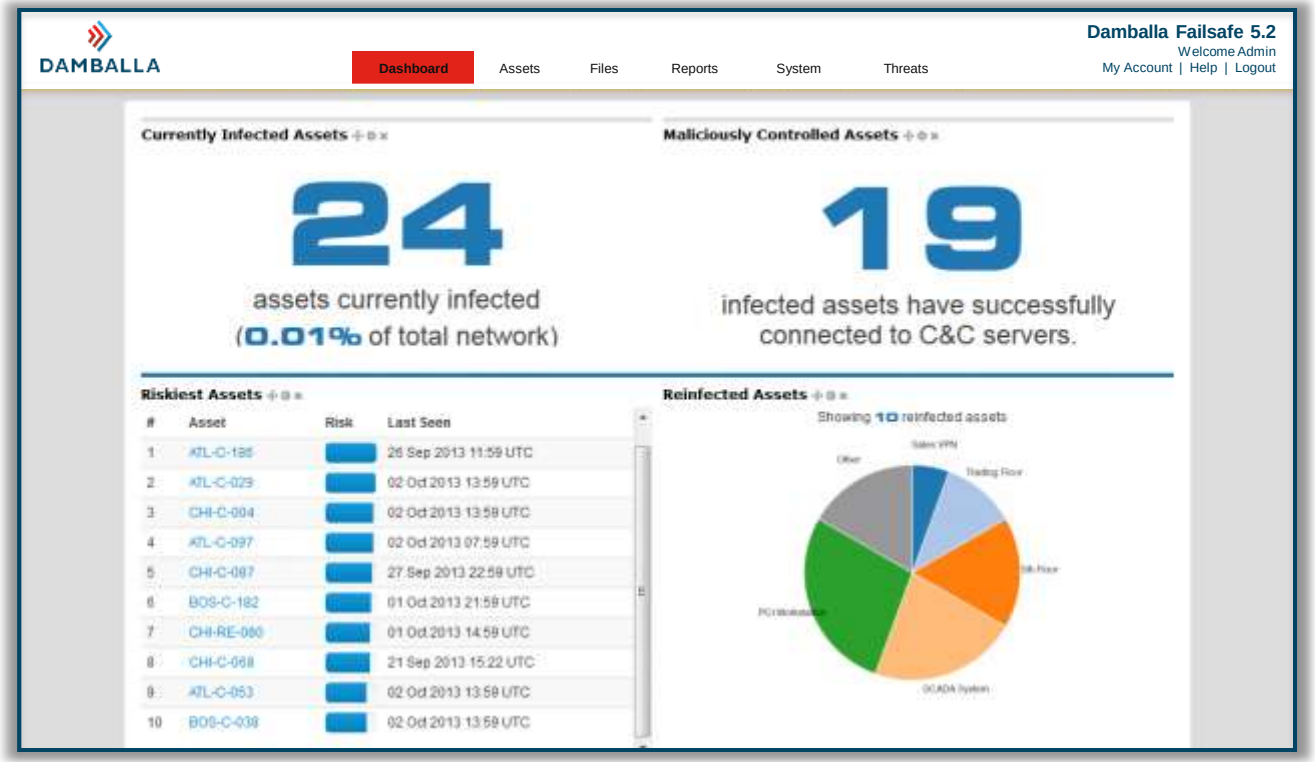
Damballa Failsafe Case Analyzer Platform

DAMBALLA

Our Formula – Delivering Predictive Security Analytics



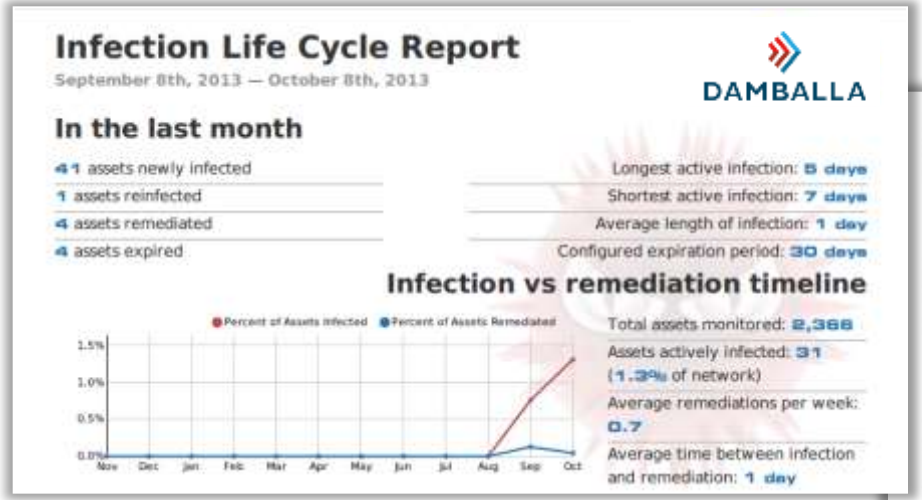
Visibility for Security and Risk Professionals

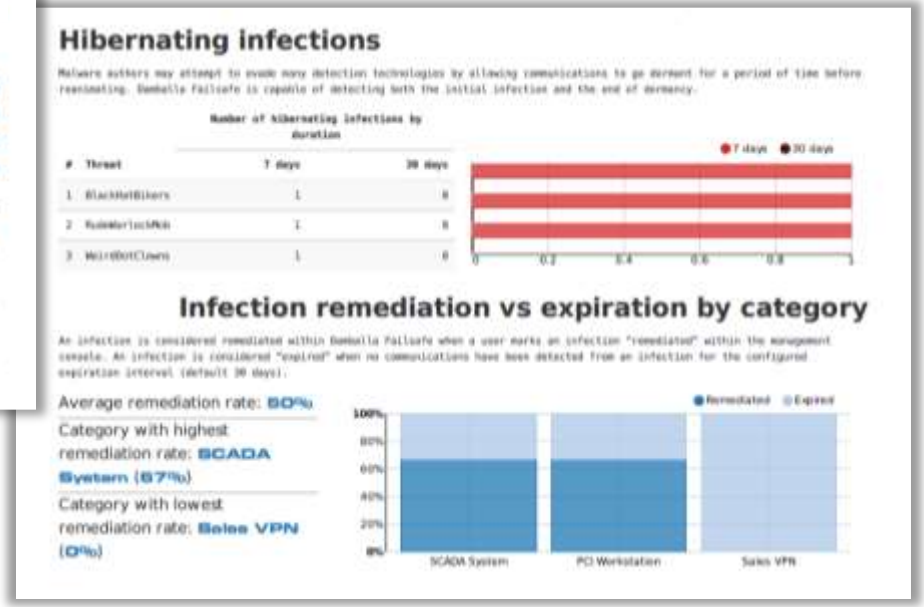


Infographics styled dashboards, presenting critical information upon login.

DAMBALLA

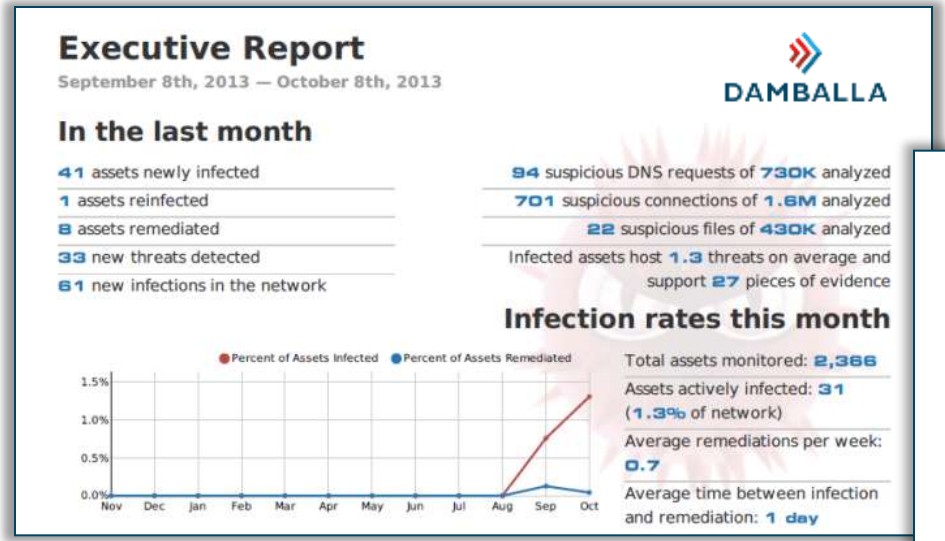
Incident Reports for Security Managers





DAMBALLA

Assurance for Executives



Executive Report

September 8th, 2013 — October 8th, 2013

DAMBALLA

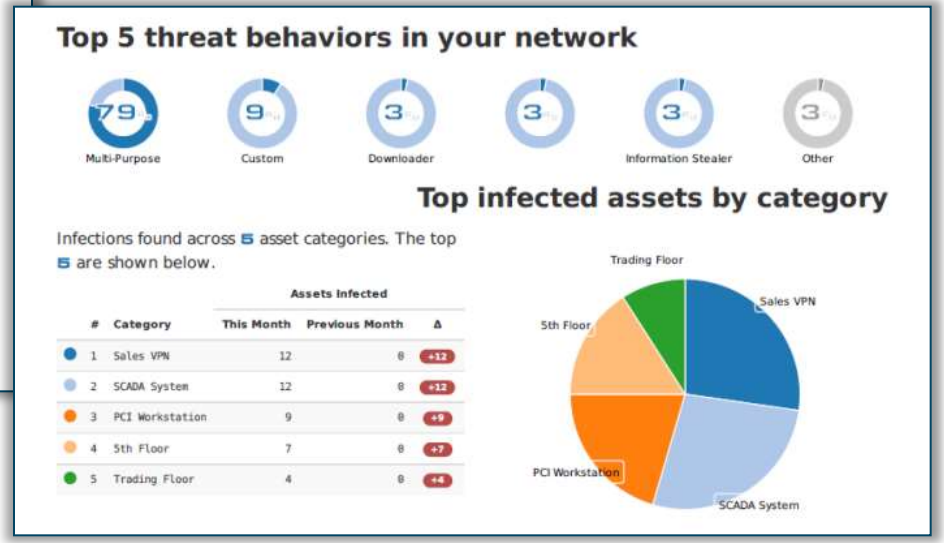
In the last month

41 assets newly infected
1 assets reinfected
8 assets remediated
33 new threats detected
61 new infections in the network

94 suspicious DNS requests of **730K** analyzed
701 suspicious connections of **1.6M** analyzed
22 suspicious files of **430K** analyzed
Infected assets host **1.3** threats on average and support **27** pieces of evidence

Infection rates this month

Total assets monitored: **2,366**
Assets actively infected: **31** (**1.3%** of network)
Average remediations per week: **0.7**
Average time between infection and remediation: **1 day**



Top 5 threat behaviors in your network

Top infected assets by category

Infections found across **5** asset categories. The top **5** are shown below.

#	Category	Assets Infected: This Month	Assets Infected: Previous Month	Δ
1	Sales VPN	12	0	+12
2	SCADA System	12	0	+12
3	PCI Workstation	9	0	+9
4	5th Floor	7	0	+7
5	Trading Floor	4	0	+4

DAMBALLA

La ultima generacion tecnologica para la prevencion, deteccion, analisis y remediacion de amenazas avanzadas.

Joel Guerrero
Latin America
Regional Sales Director
Joel.guerrero@damballa.com

DAMBALLA