agesic
DESARROLLANDO EL URUGUAY DIGITAL

PRESIDENCIA
REPÚBLICA ORIENTAL DEL URUGUAY

¿Cómo pueden ayudar los servicios del SOC?

José Callero

jcallero

jornadas tecnológicas

¿Qué es el SOC Nacional?

jornadas tecnológicas

¿Cuánto tiempo dispongo para estar al día con lo que pasa?

¿Hago seguimiento de las vulnerabilidades publicadas?

¿Cuánto tiempo dedico a analizar logs de forma proactiva?

¿Si un equipo no presenta ningún sintoma y está infectado, me entero?

¿Tengo claro todo lo que pasa en mi infraestructura?

¿Cuántos recursos idoneos en seguridad poseo?

jornadas tecnológicas

Cuentas comprometidas

INFORMACIÓN

- Login OK / NO OK
- IP origen / destino
- Asunto
- Nombre de los archivos adjuntos
- Cadencia de eventos por dominio / casilla

ENRIQUECIMIENTO

- Indicadores de Compromiso (IoC)
- Geolocalización
- Amenazas actuales
- Análisis de comportamiento

RESULTADOS

- Detección de cuentas comprometidas
- Detección de equipos infectados
- Prevención de infecciones

Cuentas comprometidas

¿Cómo detectamos?

- Análisis de accesos fuera de Uy
- Cadencia de eventos
- Análisis de asuntos / adjuntos

¿Cómo se comportan los afectados?

- Descargan piezas de software
- Se conectan a botnets
- Envían mail

¿Cómo lo podemos prevenir?

- Notificaciones tempranas
- Bloqueos de IP/URL

jornadas tecnológicas

Equipos comprometidos

- Proxys
- Consultas de DNS
- IPs origen / destino

VirusTotal

PhishTank

CERT

ENRIQUECIMIENTO

IBM X-Force

Recorded Future

SHODAN Computer Search Engine

- IoC Propios
- Análisis de amenazas / campañas
- Threat intelligence

RESULTADOS

- Más de 4k eventos detectados
- Mitigación de Campañas de malware
- Identificación de Equipos infectados
- Identificación de victimas de phishing

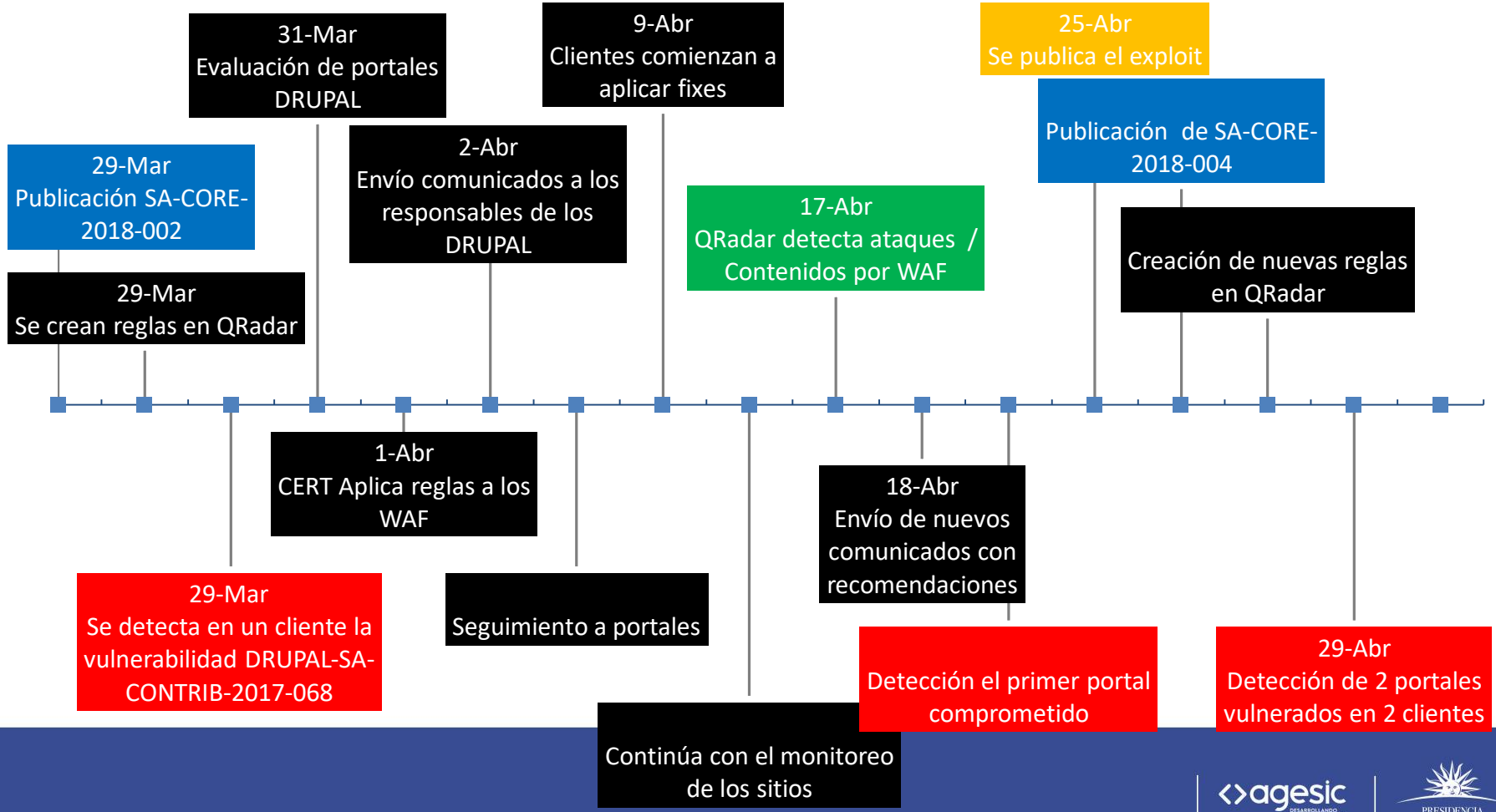
Incidente Drupal (marzo-abril de 2018)

Contexto

- Semana de turismo
- Red de WAF
- Vulnerabilidad crítica
- Cientos de portales

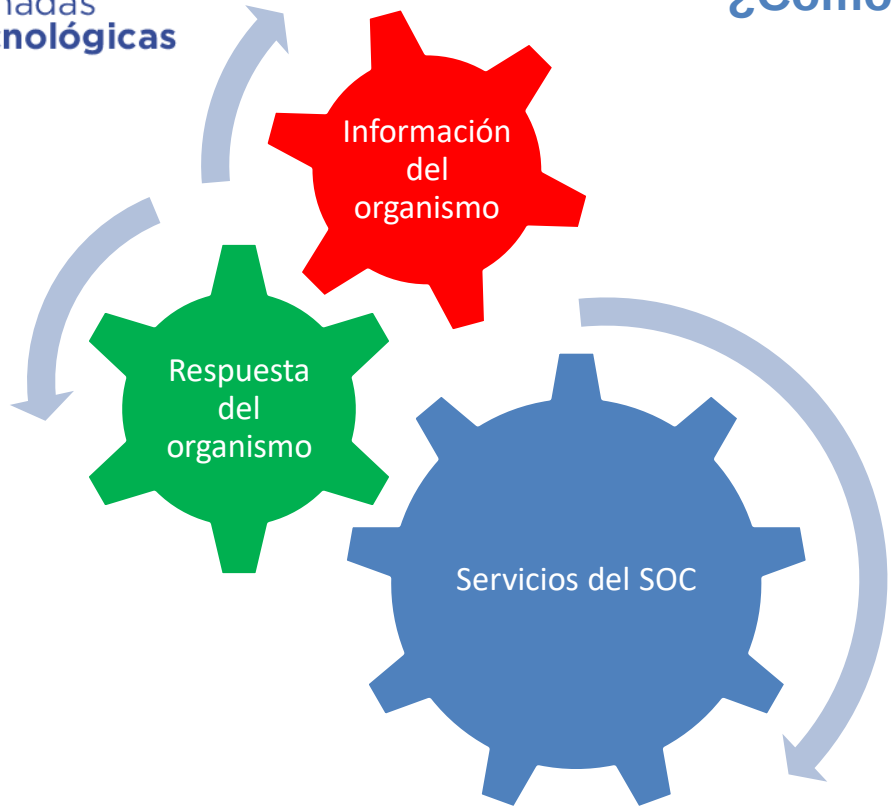
Factores Clave

- Feeds de información
- Logs de sitios / WAF
- SIEM
- Servicio 24x7


31-Mar
Evaluación de portales DRUPAL
9-Abr
Clientes comienzan a aplicar fixes
25-Abr
Se publica el exploit
29-Mar
Publicación SA-CORE-2018-002
2-Abr
Envío comunicados a los responsables de los DRUPAL
Publicación de SA-CORE-2018-004
17-Abr
QRadar detecta ataques / Contenidos por WAF
29-Mar
Se crean reglas en QRadar
Creación de nuevas reglas en QRadar
1-Abr
CERT Aplica reglas a los WAF
18-Abr
Envío de nuevos comunicados con recomendaciones
29-Mar
Se detecta en un cliente la vulnerabilidad DRUPAL-SA-CONTRIB-2017-068
Seguimiento a portales
Detección el primer portal comprometido
29-Abr
Detección de 2 portales vulnerados en 2 clientes
Continúa con el monitoreo de los sitios

jornadas tecnológicas

¿Cómo me pueden ayudar los servicios del SOC?



- Gestión de vulnerabilidades
- Monitoreo reactivo
- Monitoreo proactivo
- Análisis de comportamiento
- Información de la Dark Web
- Threat Intelligence

agesic
DESARROLLANDO EL URUGUAY DIGITAL

PRESIDENCIA
REPÚBLICA ORIENTAL DEL URUGUAY

¡Muchas gracias!

jose.callero@cert.uy

jcallero