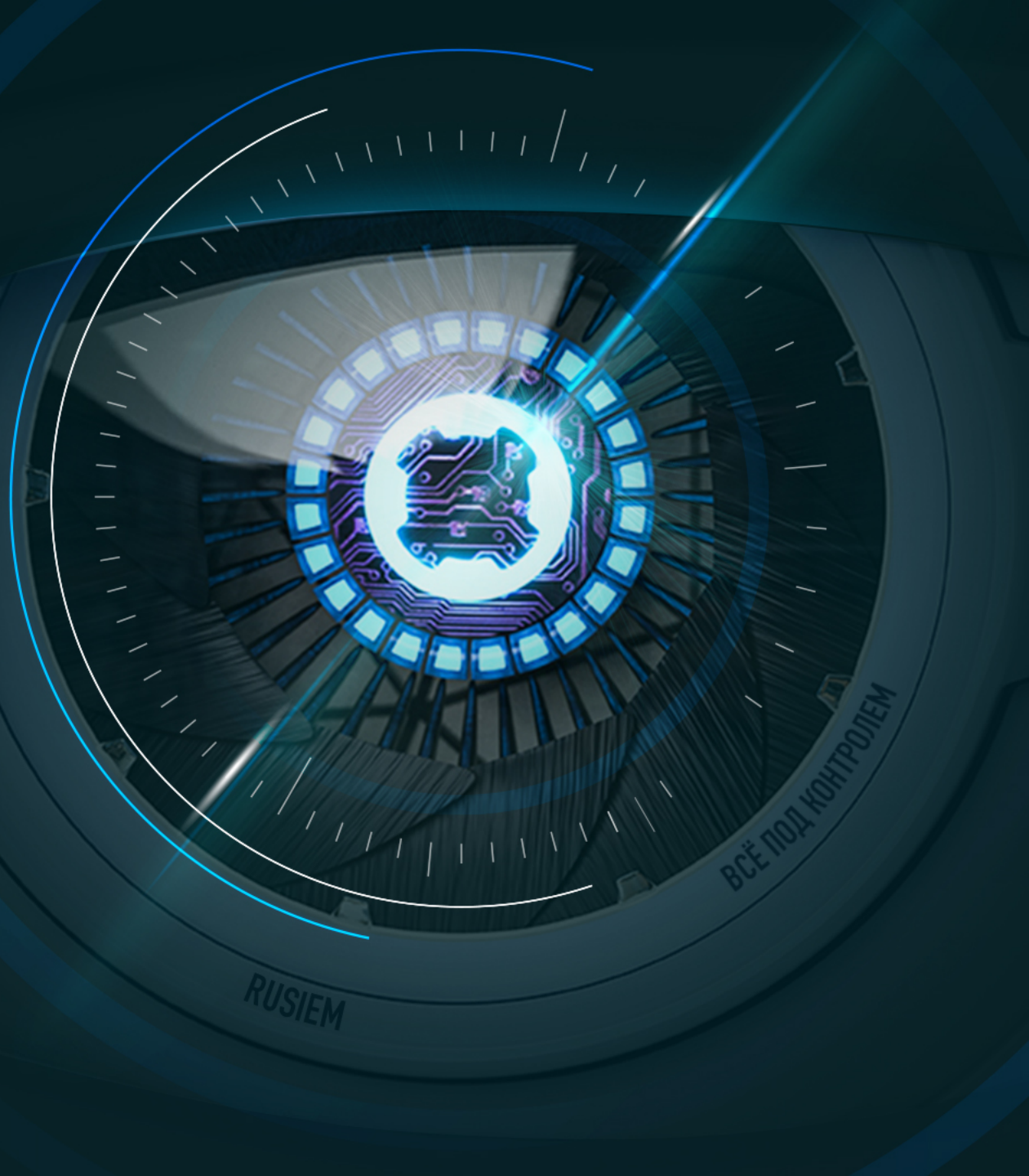
RUSIEM

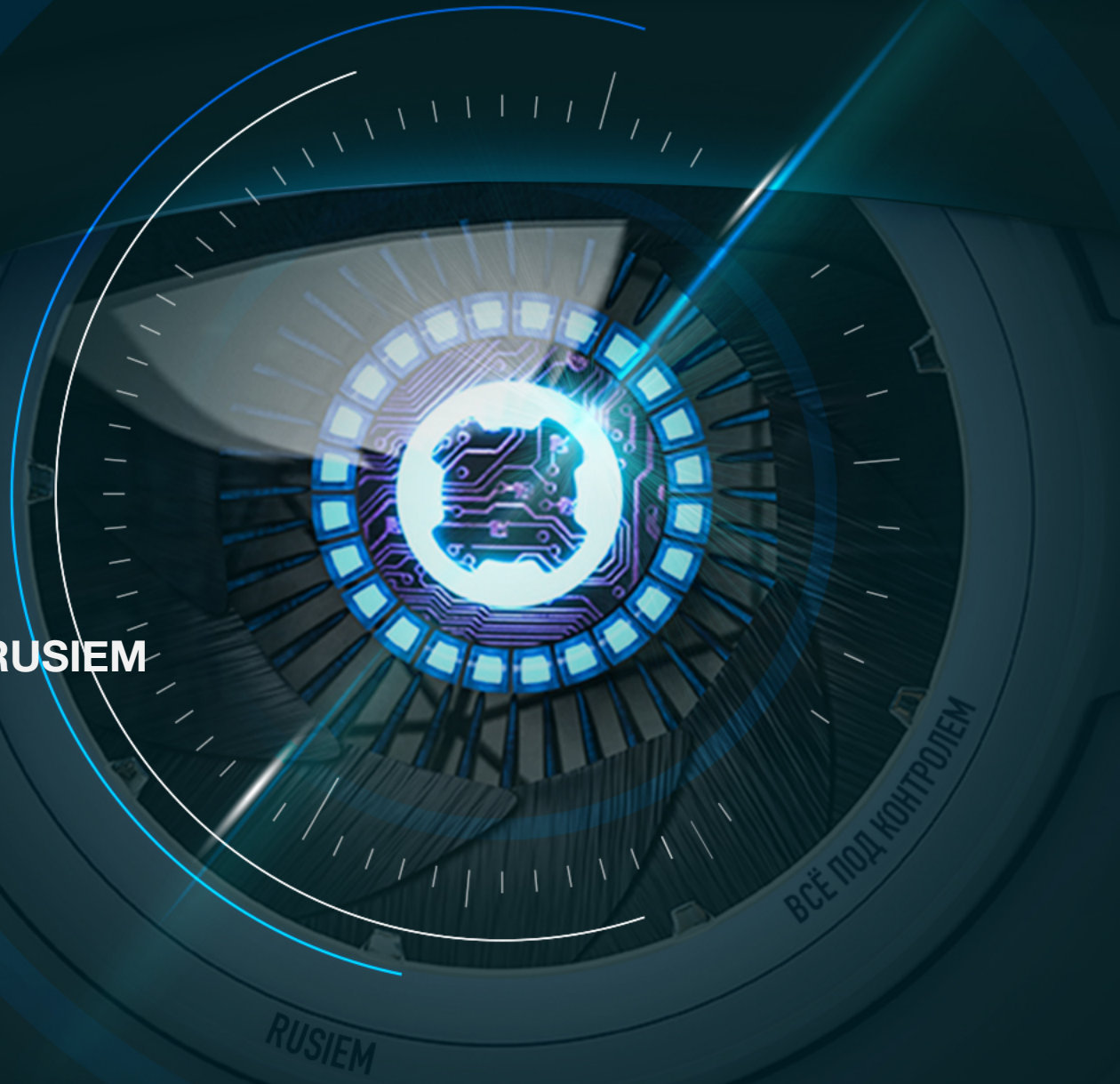
Всё под контролем

Presentación para América Latina y España



RUSIEM

Всё под контролем



- Quiénes somos (sobre nuestra empresa)
- ¿Por qué tu empresa necesita RUSIEM?
- Principio de funcionamiento del sistema RUSIEM
- Arquitectura de la solución RUSIEM
- Ventajas de la solución RUSIEM

Sobre la empresa RUSIEM

El código del programa se desarrolló en Rusia

2014

Iniciamos nuestro desarrollo

Sk Сколково

Miembro de Skolkovo

Diferentes países

Diferentes paises

+ 530

Nuestros socios principales

El producto está incluido en el Registro Único de Software Nacional.

Certificado FSTEC de Rusia

ГОССОПКА

Integrada a GosSOPKA"

RUSIEM
Всё под контролем

¿Qué es SIEM?

- Estaciones de trabajo
- Firewall
- Enrutadores
- Comunicadores de red
- Servidores
- Computadoras centrales
- Sistemas de detección y prevención de intrusos

SIEM

- Advertencias
- Paneles de control
- El registro de incidencias
- Informes
- Supervisión

RUSIEM
Всё под контролем

Cómo funciona RuSIEM

Colección incidentes de seguridad

- Control de la infraestructura de la empresa.

Normalización de eventos

- Reducción a un solo tipo de representación

Enriquecimiento y sintomatología.

- Comparar los síntomas y agregar ponderaciones de eventos

Correlación incidentes de seguridad

- Reglas de correlación de incidencias

Identificación incidentes de seguridad

- Elaboración de cadenas de eventos y evaluación de riesgos.

RUSIEM
Всё под контролем

Eventos de entrada de varias fuentes de datos

- Cortafuegos
- IPS
- DNS logs
- Sistemas automatizados de control de procesos de producción
- sistemas de control de acceso de personal
- Varios sensores
- Antivirus
- Dispositivos de red

- Windows event log
- Web servers
- App servers
- Load balancing
- Network flow
- Network payload
- Sistemas postales
- Aplicaciones de negocios

RUSIEM
Всё под контролем

Rubros de los productos de RUSIEM

RvSIEM (free)
Prueba gratuita de nuestra solución

RuSIEM
Versión comercial de la clase SIEM.

RuSIEM Analytics
Módulo de análisis de eventos basado en aprendizaje automático.

RuSIEM IoC
Indicador de compromiso

RuSIEM Monitoring
Módulo de monitoreo sistemas de información, nodos, aplicaciones

RUSIEM
Всё под контролем

¿Cómo adquirir nuestra licencia?

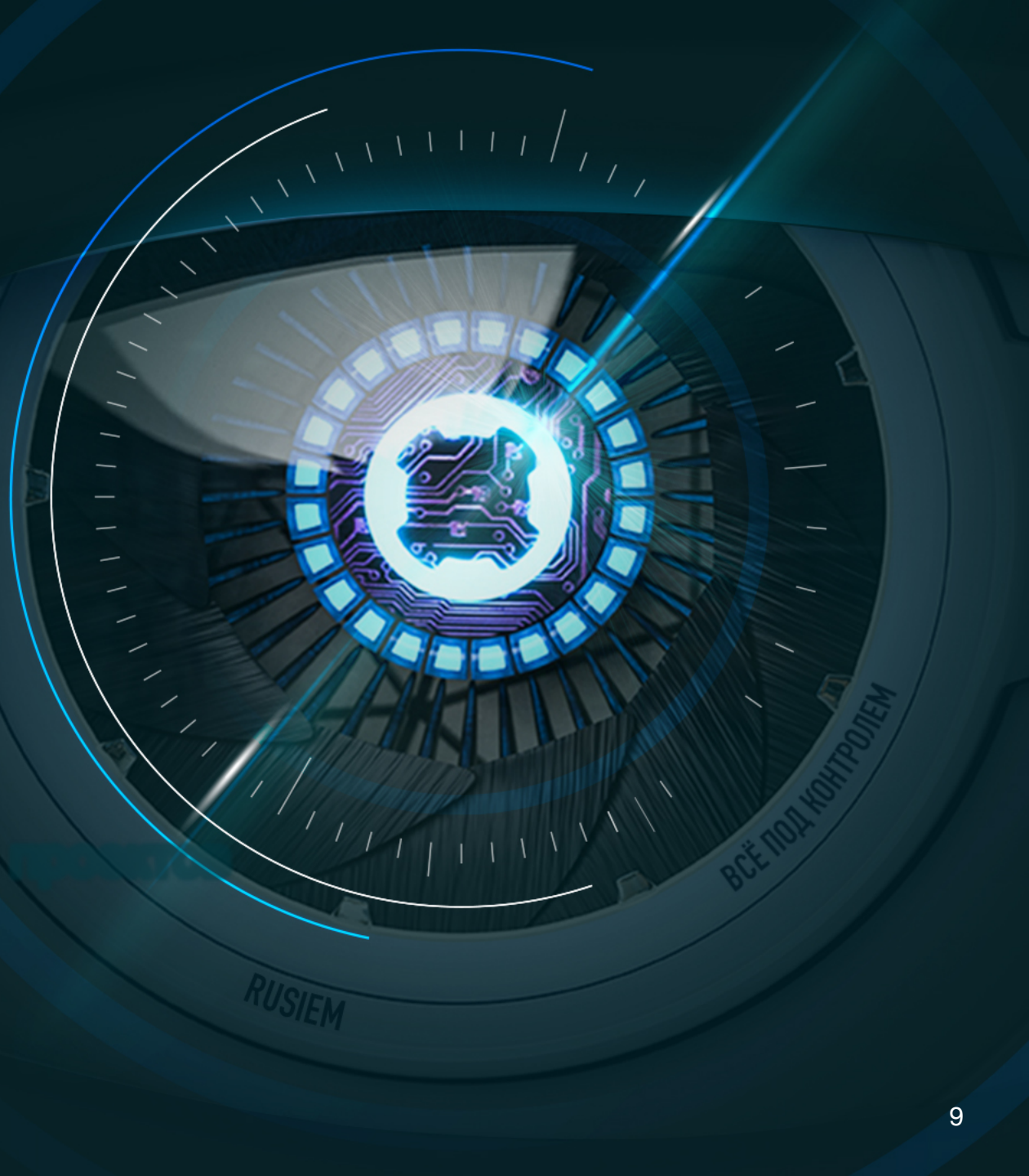
- *Licencias perpetuas (licencia de período indeterminado)*
- *Licencias de duración determinada*
- *Desarrollo de analizadores complejos*
- *Desarrollo de reglas de correlación.*

Número de eventos por Segundo
(Event per second)

2000 eps
3000 eps
4000 eps
5000 eps
7500 eps
10000 eps
12500 eps
15000 eps
20000 eps
…

RUSIEM
Всё под контролем

Construcción de un centro de monitoreo de seguridad de la información SOC



SOC con RuSIEM

МЕГАФОН МОБИЛЬНЫЙ ОПЕРАТОР №1 ПО СКОРОСТИ И ПОКРЫТИЮ by OOKLA 2022

ЭР-ТЕЛЕКОМ

информационный центр

@СТРАЛ БЕЗОПАСНОСТЬ

RUSIEM
Всё под контролем

Para más información (precios, presentación, etc.), contáctenos en nuestro sitio web.

¡Gracias por su atención!