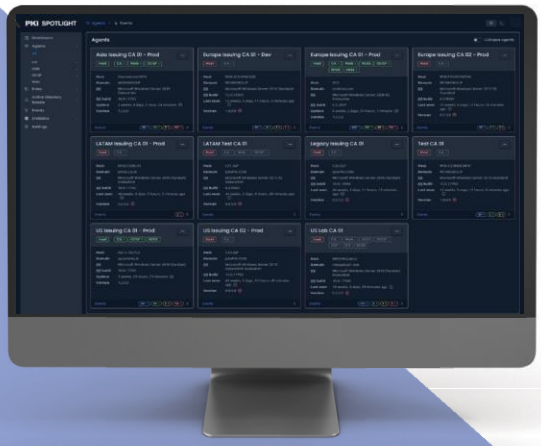
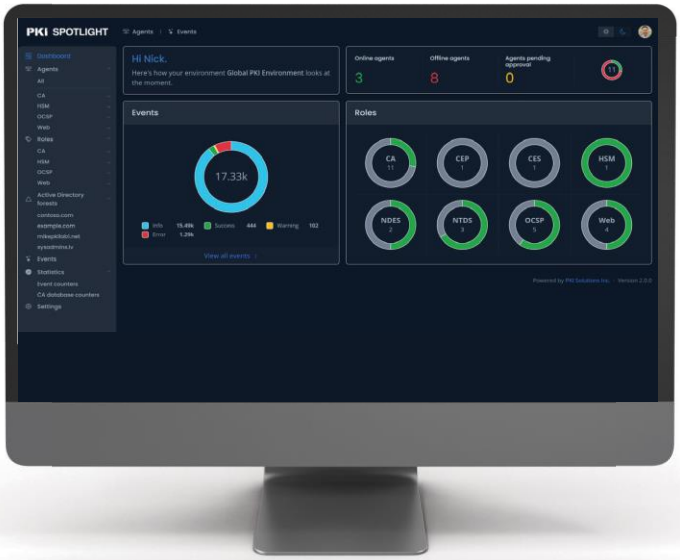
PKI SPOTLIGHT®





See the Unseen

Real-time monitoring and alerting of the availability, configuration, and security of Microsoft and non-Microsoft PKI and HSM environments - consolidated, and at your fingertips.

Why?

The distributed nature of Public Key Infrastructure (PKI) poses operational challenges that are not addressed by certificate lifecycle management or monitoring products. Most organizations struggle to manage their PKIs.

These factors increase an organization's risk to business disruption, lurking threats, and chances of making the news for the wrong reasons.

OPERATIONAL RESILIENCE

Improve the uptime, availability, and recoverability of your Microsoft and non-Microsoft PKIs and Hardware Security Modules (HSM)

SECURITY POSTURE MANAGEMENT

Maintain the security and integrity of your PKIs with visibility into configurations that can impact identity and encryption systems

THREAT DETECTION

Quickly spot any abnormal activity, vulnerabilities and exploitable misconfigurations in your PKI Environments

BEST PRACTICES INCLUDED

By Design: Review, and refine your PKI operational and configuration practices

CORE CAPABILITIES

- Real-time PKI and HSM alerting and notifications for critical PKI functions, events, activity, and configuration changes with support for Microsoft ADCS, HashiCorp Vault
- Email-based integration into Incident Management and Service Management solutions
- Best Practice Out of The Box (OOTB) rules to continually check the status of PKI and HSM configurations and events against security and operational best practices
- Certificate Revocation List (CRL) Monitoring and pre-failure CRL error detection
- Is Alive tests for Certificate Authority (CA) and Microsoft Network Device Enrollment Service (NDES)
  - Checklist of dependencies to detect pre-failure conditions and to ensure that the CA is servicing requests.
  - Scheduled and automated 7 granular health checks on NDES and associated IIS servers
- Real-time Detection and Remediation Recommendations to mitigate threats from vulnerabilities starting with PetitPotam (CVE-2021-36942)
- Real-time checks for exploitable certificate template misconfigurations to prevent escalation of privileges and man in the middle attacks

REQUEST A DEMO!

PKISPOTLIGHT.COM

+1 971 231-5523
info@pkisolutions.com

PKI SPOTLIGHT®

Operational Resilience

With consolidated PKI wide system configuration and events at their fingertips, PKI admins and operations teams can at any time

- Check events for signs of availability, pre-failure, and failover states
- Get proactive alerts on CA's ability to sign requests
- Get alerted on CRL errors and detect pre-failure CRL states
- Stay on top of Microsoft NDES availability and HashiCorp Vault
- Verify against desired operational state across network segments and Microsoft Active Directory forests
- Observe and get alerted on operational status faults for Entrust nCipher Hardware Security Modules
- Get notified in real-time through alerts and integrations into Incident and Service

Threat Detection

Protect your PKI against malicious activity

- Real-time alerts on the presence or absence of PKI vulnerabilities
- Real-time alerts for exploitable Certificate Template misconfigurations
- Spot unusual CA permission and revocation activities
- Identify out of the ordinary activities in Active Directory, cryptography, and policy modules
- Detect unrevoked certificates to quickly pinpoint any anomalies
- Get notified of PKI-related service shutdown events

LEARN MORE!
PKISPOTLIGHT.COM

SECURITY POSTURE MANAGEMENT

Identify misconfiguration issues that affect the Security and Integrity of identity, access and data

- Configuration of Hardware Security Modules
- Cryptographic provider configurations
- Service Principal Names (SPN) and TLS bindings for Microsoft NDES IIS application pools
- Certificate Revocation Checking configuration
- Password and dynamic password enforcement for all Microsoft NDES roles
- Key Recovery Agent status and configurations
- PKI Server Firewall modifications and operational state

BEST PRACTICES

Methodically and by design: Review, and refine relevant configurations any time

- Visibility across PKI component settings and operations for alignment with organizational or industry standards
- Keep up with best practices required to keep your PKIs and HSMs functional, available and secure.
- Centralized view to ensure components are configured and operating per design
- Alerting and notification integration to enable enterprise scale remediation services
- Optional Co-Management support to provide subject matter expertise on demand to triage and remediate issues
- Trusted advisory services for reactive issues and unlimited support for the PKI