NETENRICH

Intelligent SOC

Smarter Ops for Smarter Security

Today's Security Operations Center (SOC) plays a vital role in stopping malware, spear phishing, malicious insiders, zero-day, and distributed denial of service (DDoS) attacks. Intelligent SOC from Netenrich expands on the traditional model to increase efficiency, bridge skills gaps, and right-size SOConomics.

Intelligent SOC starts with target outcomes and applies automation and expertise to reduce noise, speed resolution, demonstrate value, and shrink your digital attack surface.

Powered by Netenrich's Resolution Intelligence, Intelligent SOC operationalizes technology, people, and processes and adds proprietary threat intelligence to enrich alerts with highly actionable context. Intelligent SOC includes threat models, playbooks, historical data, use cases, and a notable addition to the mix, integrated Threat & Attack Surface Intelligence.

40%	noise reduction		Enhanced detection
35%	reduction in SOC cost		Elastic consumption
50%	faster onboarding		Only contract the business outcomes you need

Start with outcomes

Building a SOC from the ground up costs nearly $3 million and takes 2 to 3 years to roll out. Netenrich Intelligent SOC-as-a-Service fast-tracks the onboarding process to deliver results and normalize your ongoing expense right away.

Intelligent SOC features 24x7 security monitoring of your end-client environment. We detect and respond to incidents quickly, escalating tickets with actionable context and proven insights to speed remediation.

Intelligent SOC delivers:

Monitoring

24x7 monitoring of logs and audit trails used to locate security events and detect known and unknown attacks.

Major incident response

For major incidents, Intelligent SOC follows standard procedures for escalation, ticket creation, and tracking.

SIEM management

Intelligent SOC includes onboarding and configuration of the Security Incidents and Events Management (SIEM) solution to drives efficiencies. Netenrich partners with IBM QRadar to deliver best-in-class SIEM capabilities. Along with streamlined onboarding and configuration, deployments feature rule packs tuned and tweaked to achieve higher operational efficiencies than out-of-the-box deployments.

Netenrich's partnership with IBM QRadar provides value-added SIEM integration and management featuring:

- Setup and configuration
- Customization to match compliance requirements
- Support for hybrid cloud deployments
- Tuning of collector, processor, and console modules
- Integration with IBM QRadar's X-Force threat intelligence
- Integration with external ticketing system
- Executable dashboards
- Custom reporting
- Back-ups

Incident management

Enables restoration of services quickly by communicating actionable guidelines and remediation actions. We apply best practices and best-in-class tools to manage your environment to agreed-upon service levels, continuously monitoring KPIs and ensuring control points with threshold levels are defined properly.

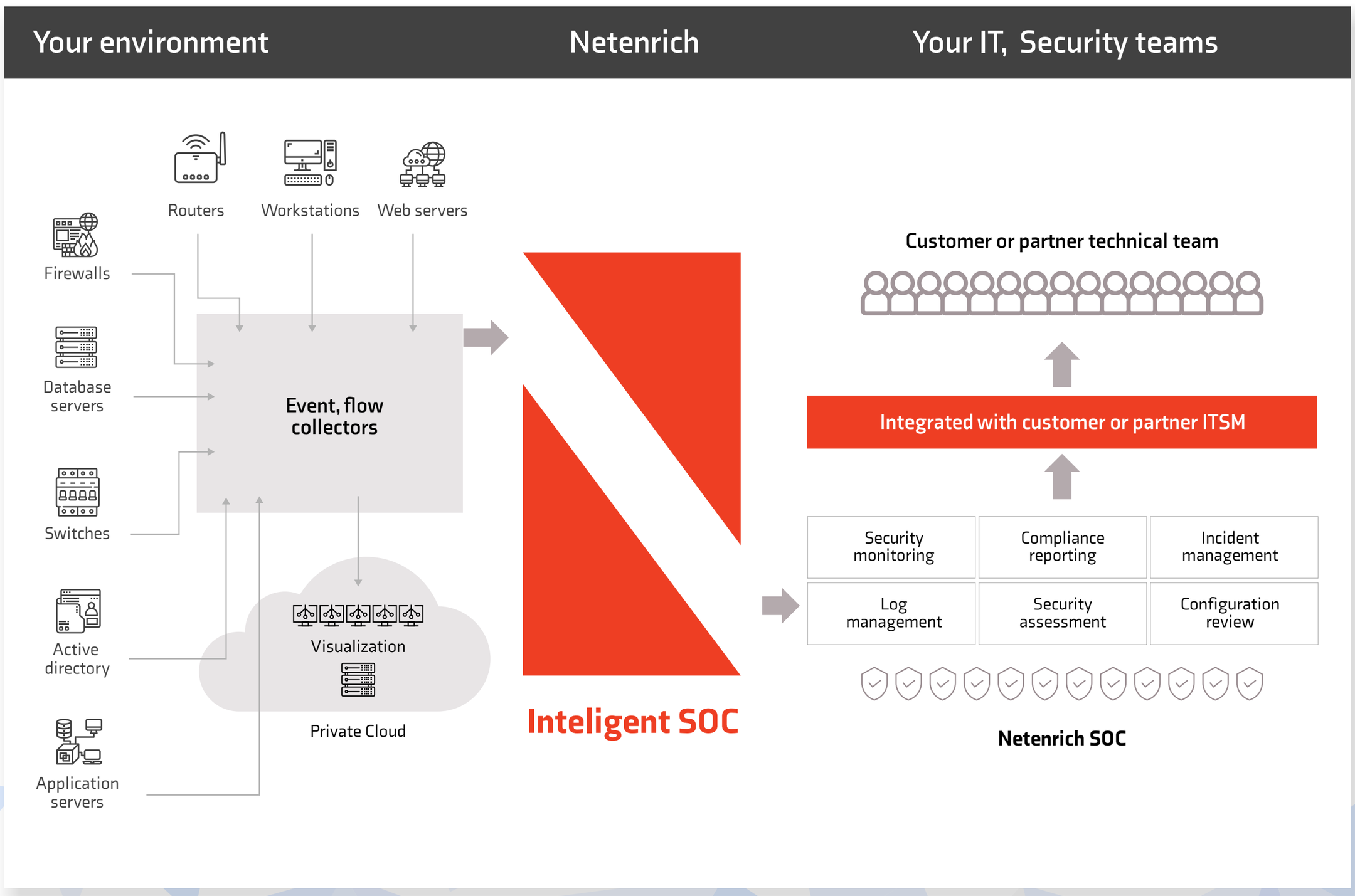
Log management

Log management includes processes and policies used to administer and facilitate generation, transmission, analysis, storage, archival, and ultimate disposal of log data:

- Monitoring log health
- Analysis and correlation of logs in context
- Log retention and on-demand access
- Regular log monitoring reports

- Threat & attack surface intelligence
- Dark web analytics
- Cloud, SaaS protection
- Advanced threat modeling
- Breach & attack simulation
- Insider threat detection
- Rapid onboarding to IBM QRadar SIEM
- Custom SIEM rules built as needed
- L1, L2, L3 triage and response
- Log management
- Monthly external security assessment
- Monthly compliance reporting
- Monthly review call

Intelligent SOC workflow



Specifications

STANDARD ENTITELMENTS

CATEGORY	SUB-CATEGORY	ENTITLEMENTS
Monitoring and escalation	Security monitoring	24x7 real-time monitoring of security events that satisfy alert polices and use cases
	Incident escalation	24x7 real-time incident management through security tickets created in real-time by Netenrich SOC analysts
	Events of interest	Events that do not satisfy predefined alert policies but are discovered based on techniques such as contextual misuse and anomaly detection
	Log management	Capture and aggregate millions of logs generated every day from disparate data sources Ensure security and compliance requirements for log collection, storage, and reporting Support effective log retention settings Retain logs for one year
	Remediation and mitigation guidelines	Detailed steps for ticket remediation Actionable steps and procedures for use by problem management and/or IT teams to resolve issues Monthly report summarizes all incidents and events of interest
Threat intelligence	Integrated	IBM QRadar X-Force threat intelligence module Netenrich threat intelligence modules
SIEM tool integration & administration	IBM QRadar setup with Nenenrich onboarding shipper	Install, stabilize, tune, and administer IBM QRadar solution Create, fine-tune and modify alert policies Install, configure, and administer Netenrich Shipper collectors at end-client locations
Status review calls	Monthly	Discussion and consulting on security and health trends of end-client setup and top incidents.

ADDITIONAL MODULES	
Vulnerability assessment and web application scanning	Vulnerability assessments
	Web application scanning
IBM QRadar advanced analytics and intelligence	Flow-based analysis
	IBM Watson analysis
Netenrich Threat & Attack Surface Intelligence	Attack Surface Intelligence (ASI)
	Knowledge NOW (KNOW) threat intelligence
Third-party threat intel	Enabled feeds and "bring your own" intelligence
Endpoint detection and response	Service integration and solution management
Dark web analytics	Weekly trend report with dark web context Automated investigation Attack Surface Intelligence (ASI) reporting

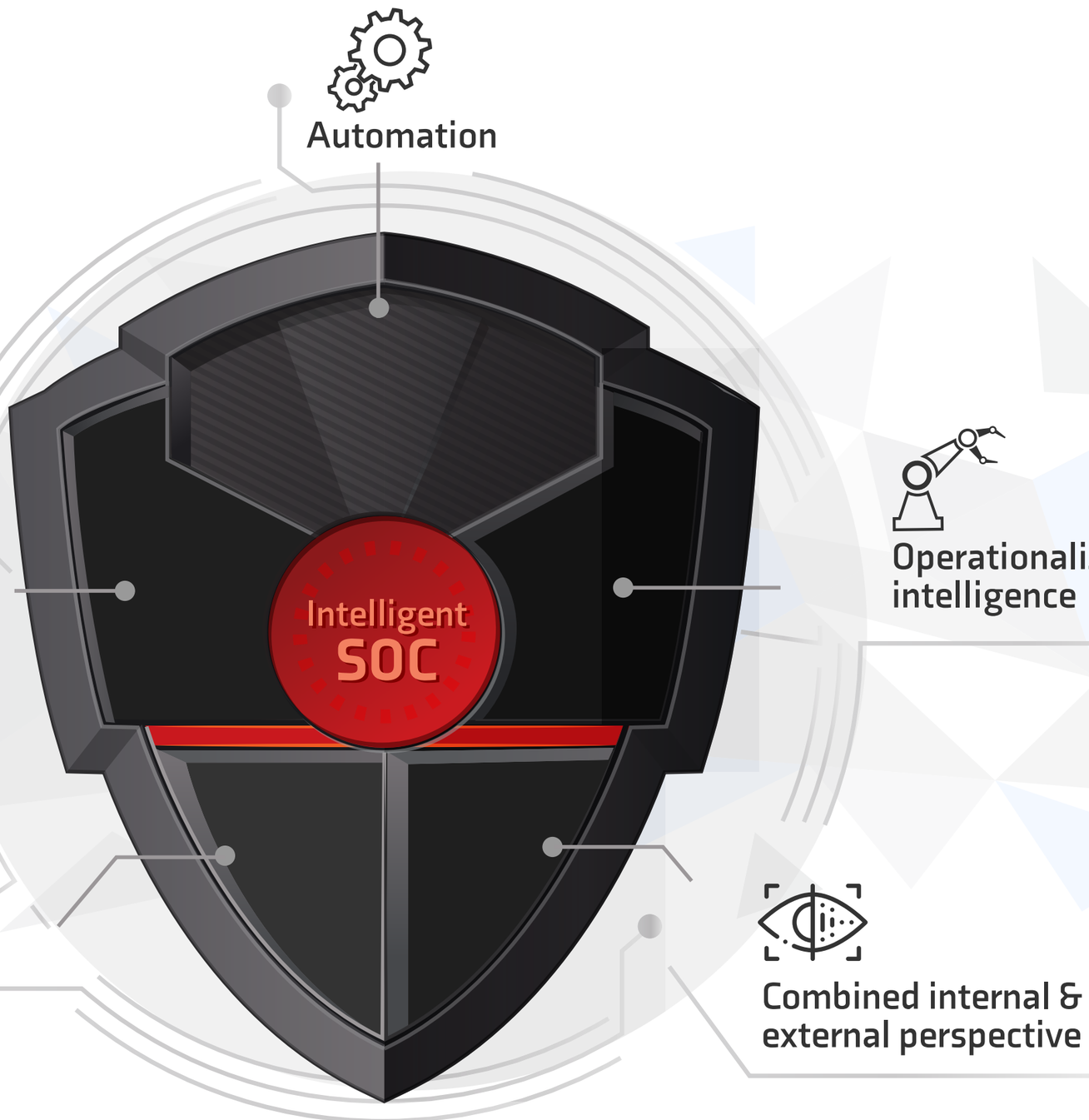
Proven expertise

Netenrich brings more than a dozen years' digital ops expertise and a proven heritage of cybersecurity innovation. Offloading repetitive tasks to our team frees your analysts to uplevel Security Operations (SecOps) activities and fast-track response to critical threats.

Beyond resolution

At the end of the day, investments in SOC should have a transformative impact on cybersecurity operations, IT, and the business itself. Along with faster resolution, Intelligent SOC is architected to significantly reduce run cost, combat alert fatigue, promote compliance, and make SecOps more efficient.

Transformation also includes being able to demonstrate higher return on investments (ROI) in security and IT, and a stronger, more proactive and scalable security posture that supports innovation and protects your brand.



Try it now and start shrinking your attack surface FREE.

Intelligent SOC goes beyond traditional capabilities to help proactively shrink your attack surface. Try Intelligent SOC now and receive a free trial of Netenrich Attack Surface Intelligence (ASI) to reduce external risk from digital brand exposure, vulnerabilities, and misconfigurations. Visit **netenrich.com/isoc** today.

About Netenrich

Netenrich delivers complete Resolution Intelligence to transform digital operations into smarter business outcomes. With 15+ years' innovation across IT, NetOps and SecOps, Netenrich applies a dynamic mix of machine and expert intelligence through a wide range of products and SaaS-based offerings. More than 6,000 customers and organizations worldwide rely on Netenrich to help drive digital transformation, mitigate brand exposure, increase efficiencies, and bridge skills gaps. Netenrich is based in San Jose, California.

NETENRICH