Sergey Rogatnev

CYBERSECURITY ARCHITECT · SECURITY LEAD · PRODUCT MANAGER

25+
YEARS IT

20+
YEARS CYBERSEC

15+
YEARS NETWORKING

12+
YEARS PALO ALTO

PROFESSIONAL SUMMARY

Senior Cybersecurity Architect & Lead with 25+ years of IT experience, including 20+ years in cybersecurity and 15 years of core network engineering — building data centers across the globe. Deep hands-on expertise with Palo Alto Networks (12 yrs), Cisco, and Check Point platforms; architecting Zero Trust, SASE, NGFW, and SD-WAN solutions across Finance, Healthcare, Entertainment, Manufacturing, and Government verticals. Proven track record translating advanced threat intelligence and AI-driven security automation into quantifiable business outcomes. Seeking an Architect, Lead, or Manager role to drive next-generation security strategy.

AI THREAT DEFENSE & SECURITY

Defending Against AI-Powered Attacks | LLM / Prompt Injection Defense | GenAI Risk Management | OWASP LLM Top 10 | MITRE ATLAS | AI Threat Modeling | Shadow AI Detection & Control | AI-Augmented SOC / SIEM / SOAR | Adversarial ML Defense | MLSecOps | NIST AI RMF | Security Automation (Python / Ansible / Terraform)

KEY ACCOMPLISHMENTS

FINANCIAL SERVICES
Secure cloud infra deployment → **30% ↓** security incidents & **25% cost savings**

HEALTHCARE
Zero Trust Architecture → **20% ↓** breach risk; full HIPAA compliance

TECHNOLOGY
SASE deployment → **40% ↑** network perf & **15% ↓** OPEX

MANUFACTURING
SD-WAN rollout → **50% ↑** bandwidth efficiency, **20% ↓** network costs

RETAIL
Threat prevention + IAM → **35% ↓** unauthorized access incidents

PRODUCT DEVELOPMENT
Cybersecurity product suite launch → **20% ↑** annual revenue

REMOTE ACCESS · HYBRID WORKFORCE
Prisma Access / ZTNA deployment replacing legacy VPN → **60% ↓** attack surface & **45% ↑** remote user performance

SECURITY POSTURE
Enterprise-wide exposure reduction program → **55% ↓** critical vulnerabilities; elevated security posture score from C to A within 6 months

GOVERNMENT · DEFENSE
NGFW + Panorama centralized policy rollout across 30+ sites → **70% ↓** policy drift & full NIST CSF compliance

ENTERTAINMENT · MEDIA
GlobalProtect + Prisma Access SASE migration → eliminated perimeter exposure gaps, **40% ↓** incident response time

LEGAL · PROFESSIONAL SERVICES
Attack surface audit + micro-segmentation → **50% ↓** lateral movement risk & achieved SOC 2 Type II readiness

AUTOMATION & SCRIPTING
Python + Ansible + Terraform security automation → **80% ↓** manual provisioning time & zero-touch compliance enforcement

INDUSTRY EXPERIENCE

Palo Alto Networks, Paramount Pictures, UCLA, Kaiser Permanente, M Health Fairview, Bank of America, City National Bank, Logix FCU, PaymentPass, Jacobs Engineering, Yellowpages, and engagements across Legal, Insurance, Defense, Telecom, and International Technology sectors globally.

SECURITY PLATFORMS

Palo Alto NGFW | Panorama | GlobalProtect | Prisma Cloud | Cortex XDR | Cisco ASA | Firepower / FTD | AnyConnect | Check Point | Fortinet | CrowdStrike | McAfee / DLP

CLOUD & ARCHITECTURE

Zero Trust | SASE | AWS Security | Azure Security | GCP | Kubernetes | Docker | NSX / VM-FW | CSPM | DevSecOps | IaC / Terraform

NETWORKING

SD-WAN | MPLS | BGP / OSPF | LAN / WAN | Nexus / Arista | IPSec / VPN | 5G / WiFi | Datacenter Build

DETECTION & RESPONSE

SIEM / Splunk | SOAR | Threat Hunting | Incident Response | Vulnerability Mgmt | MITRE ATT&CK | EDR

IDENTITY & COMPLIANCE

OKTA / MFA / Duo | PKI / RADIUS | IAM / LDAP | PCI DSS | NIST CSF | ISO 27001 | HIPAA | COBIT

CERTIFICATIONS

CCIE	Security #17313
PCNSC	Palo Alto Networks Security
PCNSE	Palo Alto Networks Engineer
CCSP	Cloud Security Professional
CCNP	Enterprise Networking
INFOSEC	NSA/CNSS 4013 Pro
MCSE	Microsoft Infrastructure
MCDBA	SQL Server Admin

EDUCATION

M.S. Electrical Engineering