

Overview:

The Proficio Security Operations Center Service for healthcare industry clients is designed to provide the strongest level of security to protect patient records, proprietary medical research and other sensitive data and information.

Key Advantages:

- Affordable 24x7 expert security event monitoring
- Next-generation Proactive Threat Defense identifies the early stages of attacks and suspicious insider behavior before breaches result in loss of PHI
- Provides actionable intelligence that enables internal IT teams to effectively and quickly resolve issues
- Meets HIPAA compliance requirements for monitoring, logging and forensics
- Provides full visibility to event logs with easy-to-use web portal, powerful reporting, dashboards, and drill down analytics
- Scalable cloud-based deployment - no software or hardware purchases
- Out-of-the-box support for 350+ log sources
- Flexible service model: SOC-as-a-Service, SIEM-as-a-Service, and hybrid on-premise options
- Off-loads IT teams from configuring, tuning, and patching firewalls, NGFWs, IDS/IPS, and WAFs



Security Operations Center for Healthcare – Preventative Medicine Against PHI Data Breaches

Healthcare providers and payers are exposed to a wide range of security and compliance threats. Medical identity theft is growing rapidly as cyber criminals target patient records, SSNs, and credit card numbers. Intellectual property and proprietary medical research are tempting targets for foreign hackers. Inappropriate or malicious actions by employees or partners are also often responsible for data breaches.

In this threat landscape, healthcare organizations need the strongest levels of security, but often lack the budget and in-house expertise to meet their desired goals. Proficio's Security Operations Center Service for the healthcare industry is designed to meet the most demanding security and compliance challenges with next-generation technology and around the clock monitoring and support by security experts.

Security Experts Working for You

Proficio's team of Security Engineers and SOC Analysts are working 24x7 to support our customers. We are constantly tuning correlation rules and use cases, investigating suspicious events, and recommending appropriate action to prevent problems or resolve issues. Proficio services are delivered through our Security Operations Centers (SOCs) and supported 24x7 by our team of US-based security experts. We have managed some of the largest and most respected Security Operations Centers in America and internationally. Proficio off-loads specialized and time consuming tasks from customers, including SIEM administration, log monitoring, compliance reporting, and patching and configuring firewalls, NGFWs, IDS/IPS, and WAFs. In an environment where it is increasingly difficult to recruit and retain qualified specialists, our Security Operations Center Service is highly cost effective and allows in-house IT personnel to focus on other priorities.

Proactive Threat Defense

Despite the best efforts of IT teams, damaging security breaches occur far too regularly. The threat landscape is increasingly complex and hackers are exploiting vulnerabilities across people, processes and technologies. Unlike the visible incursions of the past, new attacks employ slow and low strategies. Attackers are often able to systematically pinpoint security weaknesses and then cover all traces of their presence as they move on to penetrate the other critical IT assets. Employees, contractors, and other insiders are increasingly a source of data breaches.

Proficio's Security Operations Center Service for the healthcare industry uses next-generation Proactive Threat Defense techniques to identify the early stages of attacks and suspicious insider behavior before breaches result in loss of PHI. Multi-vector event correlation techniques, asset modeling, user profiling, and threat intelligence are among the advanced technologies used to identify threats and help prevent security exploits. Examples of events that can be analyzed include:

- Suspicious login attempts by a user into a database outside their department
- PHI access from known malicious IPs
- After-hours access by a systems administrator
- Email with unencrypted patient record numbers, SSNs, or medical terms
- Web surfing to sites that indicate job search behavior
- User ID changes or attempts to mask user identity
- USB files saved
- Suspicious VPN activity

"Proficio's Security Operations Center Service protects our confidential data by analyzing the millions of events that cross our network and prioritizing the critical alerts that require action. This helps me sleep better at night."

Todd Felker, Infrastructure and Security Architect, Torrance Memorial Medical Center.

We Take the Pain Out of SIEM

Our Security Operations Center Service for healthcare customers benefit from using the most advanced SIEM technology to log and correlate security events without the cost and complexity of owning and administering a SIEM system. The ability to accurately prioritize security alerts is critical to enabling an effective and rapid response.

As industry insiders know, the art and science of administering a SIEM application is non-trivial. The experts behind Proficio's Security Operations Center Service are exceptionally skilled in configuring SIEM systems and customizing correlation rules and use cases to identify critical security alerts that are most relevant to each of our customers. Security Operations Center Service is a subscription service that seamlessly scales to meet your growth needs. You never need to worry about hiring, performance tuning, or capacity management – that's our job.

Full Visibility and Access to Security Logs

The Security Operations Center Service Web Portal provides customers with a real-time summary of the state of their security and includes:

- Operational Dashboards
- Reports for security, management, and compliance
- Full access to security event logs
- Active Channels
- Drill down analytics
- Role-based and user-based views
- Case Management

Cloud, On-Premise, Hybrid

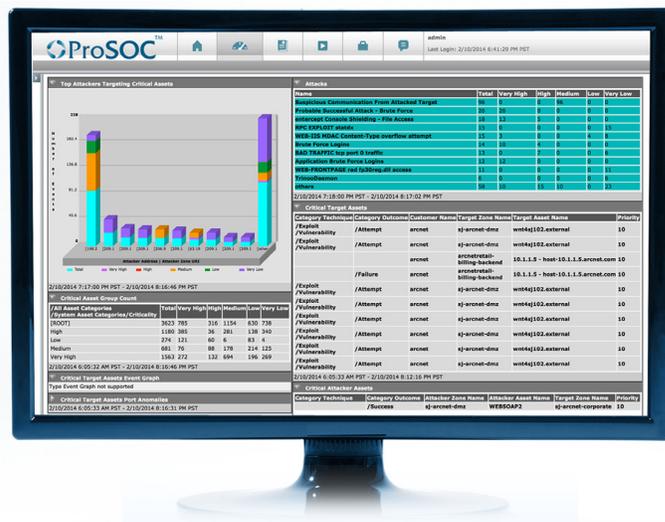
Proficio understands that each of our customers has unique needs and goals. Our Security Operations Center Service service is the most flexible in the industry and can address most deployment models and service permutations customers require.

For example, some organizations prefer to outsource all aspects of SIEM administration, event logging, and 24x7 expert monitoring. Others prefer a hybrid model where we provide a fully managed cloud-based SIEM service and they monitor and remediate their own security events. Still others wish to maintain their own on-premise SIEM system, but are looking for our help to either remotely administer their SIEM or monitor alerts outside normal business hours.

About Proficio

Proficio is an award-winning provider of managed detection and response (MDR) services. Its innovative approach to managed security service delivery is changing the way organizations defend against advanced threats, achieve regulatory compliance, and prevent security breaches.

Proficio's Security Operations Center Service provides highly accurate, 24x7 security monitoring and alerting, advanced threat detection, and automated response services. Proficio is the trusted managed security service provider for some of the world's leading utility, healthcare, industrial and consumer-focused organizations. To take your security to the next-generation, visit www.proficio.com.



Assured HIPAA Compliance

Security Operations Center Service Healthcare fully addresses HIPAA and Meaningful Use compliance requirements. Capabilities include:

- Collection and correlation of security logs
- 24x7 Security Analyst monitoring and support
- Retention of logs, investigations, case histories, and audit reports
- Forensic Investigation
- Dashboards for quick identification of potential security and privacy breaches
- Separation of Duties
- Active monitoring and correlation of patient privacy monitoring tools like Cerner P2Sentinel and FairWarning

Future Ready

Proficio's Security Operations Center Service for healthcare is a next-generation managed security service designed to address the changing threat landscape. WW Security Operations Center Service monitors and protects data and applications stored in cloud infrastructures, like AWS, using virtual relays and cloud-based IDS software. The service helps address issues arising from BYOD and the deployment of wireless applications by monitoring mobile device users and applications for unauthorized or suspicious behavior.

Proficio Headquarters:
1555 Faraday Avenue
Carlsbad, CA 92008
+1-800-779-5042

Proficio Asia:
51 Changi Business Park Central 2
#03-11 The Signature
Singapore
+65-6996-9185

Proficio Europe
11 Travessera De Gracia Floor 2
Barcelona, Catalonia 08021
Spain
+61(0)2-9258-1153

For a free pilot of Security Operations Center Service, please call 800.779.5042 or email info@proficio.com

