SOC AS A SERVICE

THE NEXT GENERATION OF CLOUD-BASED SECURITY SERVICES

Do you have the platform, capability, and resources to provide 24/7 information security for the cloud transformation era? Our SOC as a Service delivers the next generation of cloud-based security services in prevention, detection, response, forensics, and threat-hunting.

THE CHALLENGE

Cybersecurity is becoming too complex to manage in-house

As cyberattacks become more automated and complex, your IT and security departments face an event overload, a shortage of trained and experienced security analysts, lack of time and increasing staff cost.

There is constant pressure to improve visibility, respond faster, and to be able to mitigate threats before damage occurs. Cybersecurity is becoming increasingly difficult to manage in-house. What you need is a solution with clear business outcomes. A solution that reduces the time, cost and complexity of investigating and responding to security events as well as analyzing the root cause. Because after a data breach, the clock is ticking.

THE SOLUTION

SOC as a Service

ON2IT offers a new generation of SOC as a Service. For a fixed monthly fee, you have access to capabilities that go far beyond the traditional managed security services of basic technology support management, basic monitoring and compliance reporting.

Our SOC-as-a-Service solution allows you not only to detect and analyze threats, but to stop them. When a threat is detected, our Zero Trust based cloud platform automates most responses using battle-tested playbooks. If needed, our forensic experts will further investigate incidents that might require you to take action.

And with the increased usage of SaaS applications and public cloud services such as AWS, Google and Microsoft, we help you deal with advanced cyberattacks that most managed security service providers are not able to address.

ZERO TRUST INNOVATOR ON2IT:

We are ON2IT, a global pure-play cybersecurity service provider. ON2IT has more than a decade of experience in developing its Zero Trust AUXOTM platform. Zero Trustis the industry reference in state-of-the-art cybersecurity architectures, and its principles of data protection are used by government agencies and Google.

24/7 access to an elite team of security professionals:

Our next-generation cloud platform gives you 24/7 transparent access to a team of security analysts who respond in real time to disruptive security events, effectively becoming an extension of your in-house IT department.

With the deep integration of our platform across leading vendors including Palo Alto Networks, Fortinet, Cisco, AWS, Azure, Google and VMware, you can leverage your existing cybersecurity software and hardware.

No need to invest in an SIEM. Deep integration with Palo Alto Networks:

Our endpoint protection is based on the award-winning Palo Alto Networks Traps to block security breaches and ransomware attacks that use known or unknown malware and exploits before they can compromise endpoints.

It also builds on the new and revolutionary Palo Alto Networks Cortex XDR to provide our mSOCTM analysts and forensic specialists with rich contextualized log and event data and threat intelligence.

YOUR MONTHLY SOC AS A SERVICE SUBSCRIPTION FEE INCLUDES:

→ ON2IT AUXOTM Platform

→ Threat Event Enrichment, Analysis & Correlation

→ Incident Monitoring, Alerting & RCA

→ Remote Breach Support

→ Security Dashboard

→ Compliance Reporting

→ Automated Rules of Engagement

→ AI-based Threat Hunting*

→ Behavior Baselining*

→ Post-Mortem Investigation*

VALIDATED BY INDEPENDENT RESEARCH

Independent research organization, The MITRE Corporation, recently released the final results of its MITRE ATT&CKTM cybersecurity evaluations. The evaluation, which used the MITRE ATT&CK framework, shows that Cortex XDR Prevent provides the broadest coverage with fewest missed attack techniques among 10 Endpoint Detection-and-Response (EDR) vendors.

Out of 136 attack techniques tested, Cortex XDR Prevent detected 121 techniques, with 93% fewer misses than the next product.

By coupling ON2IT's advanced automation techniques of deep learning, behavioral baselining and Indicators of Good© with these innovative Palo Alto Networks technologies, our AUXOTM platform separates the noise from the relevant alerts. This enables our analysts to focus on identifying and remediating critical security events for you.

WHY LIGHTSTREAM?

Lightstream is a fully-integrated cloud, security, and network connectivity services business, specializing in building and managing secure cloud environments and network solutions. We help you control operating expenses, mitigate security risks, and reduce system complexity to increase operational effectiveness so your organization can focus on innovation and business growth while we help you to have a more effective and secure digital transformation experience.

CLEAR BUSINESS OUTCOMES

→ No concerns about talent and staffing

→ Faster resolve times

→ The right expertise 24/7

→ Cost savings

ON2IT AND PALO ALTO NETWORKS:

ZERO TRUST INNOVATORS

ON2IT's full support for Palo Alto Networks technology since 2009 reflects the importance of true cybersecurity innovation in our DNA.

ON2IT is a Palo Alto Networks ASC Elite, ATP, CPSP, MSSP, CSSP, Diamond Partner, winner of Traps global award and Managed Services Partner of the year.

We offer worldwide managed cybersecurity services for organizations with complex and dynamic IT infrastructures. Our managed services are modular, scalable and cost-effective, and always based on Zero Trust.

We are onto it. Are you?

lightstream

208 N 2100 West, Suite 200
Salt Lake City, UT 84116
Phone: 877-95-LIGHT

Lightstream.tech

Let us tell you more about the amazing things we do.