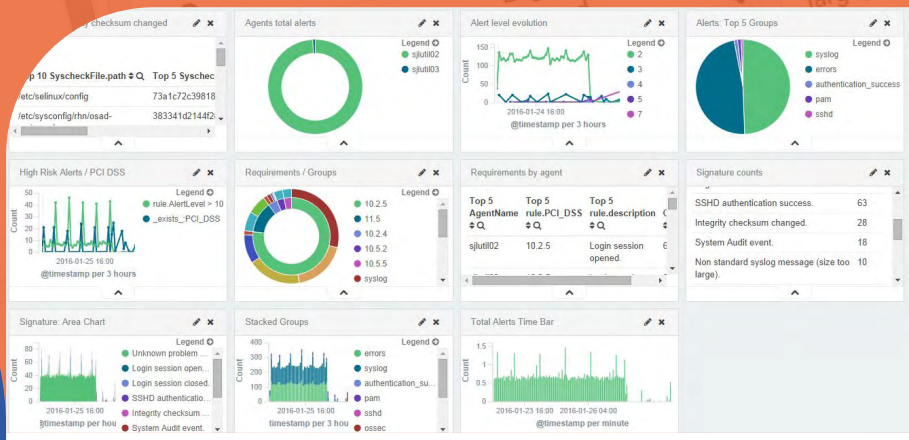
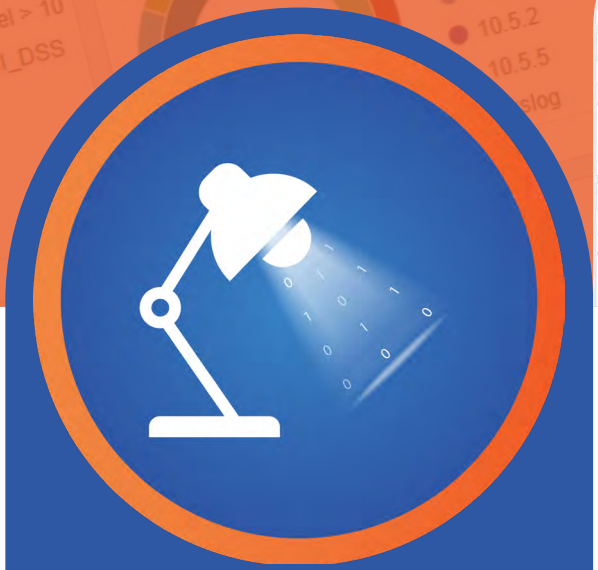
APEX
LUMI PLATFORM

DATASHEET





PRODUCT OVERVIEW

The Apex Lumi Platform is an advanced Managed Detection and Response (MDR) service designed to provide comprehensive and scalable security monitoring, advanced threat detection, and rapid incident response capabilities. This cloud-based solution, hosted in a 100% Dutch datacenter, ensures complete protection for organizations against evolving cyber threats. Leveraging open-source technology allows us to maintain lower costs, making the Apex Lumi Platform particularly suitable for SME companies.

KEY FEATURES

FEATURE	DESCRIPTION
Proactive Threat Detection	Real-time identification and alerting of potential threats through continuous monitoring and advanced detection algorithms.
File Integrity Monitoring	Monitors critical files, detecting unauthorized changes in content, permissions, and ownership to prevent data breaches.
Vulnerability Detection	Automatically identifies known vulnerabilities in software and systems by comparing inventory data against a continuously updated CVE database.
IT Hygiene	Inventory of installed software packages, Windows KB's, Browser extensions, Identities, Processes, Networks and Services.
Log Data Analysis	Centralizes log processing from various sources, enabling comprehensive analysis and visibility into security events across the entire IT environment.
Security Configuration Assessment	Automates the evaluation of system configurations against security policies, continuously monitoring compliance and generating alerts for deviations to help remediate security gaps.

APEX SECURITY

Apex Security B.V.
Galvanistraat 1 6716 AE EDE

+31 (0)85 4896060 info@apexsecurity.nl www.apexsecurity.nl

APEX LUMI PLATFORM DATASHEET

THREAT DETECTION CAPABILITIES

The Apex Lumi Platform excels in detecting a wide range of sophisticated cyberattacks, including:

- **Kerberoasting**: Detects attempts to exploit the Kerberos authentication protocol to extract service account credentials, allowing attackers to gain unauthorized access.
- **Golden Ticket**: Identifies attempts to forge Kerberos ticket-granting tickets (TGTs), enabling attackers to impersonate users and escalate privileges indefinitely.
- **DCSync**: Monitors for DCSync attacks, where an attacker mimics a Domain Controller to extract sensitive data such as user credentials, allowing for unauthorized access to the network.
- **Pass-the-Hash**: Detects attempts to leverage hashed credentials for authentication without needing to crack them. This enables attackers to access systems by using stolen hashes rather than the actual passwords.

EXTENDED SERVICES: HONEYPOT INTEGRATION

To enhance the functionality of the Apex Lumi Platform, we offer the option to integrate honeypot services.

- **Honeypot Deployment**: We install honeypots within customer networks to attract and analyze potential attackers, providing valuable insights into malicious tactics and techniques.
- **Integration into the Lumi Platform**: These honeypots are seamlessly integrated with the Lumi platform, allowing for consolidated monitoring, alerting, and incident response capabilities based on honeypot intelligence.

This integration provides a proactive layer of defense, helping organizations identify threats before they reach critical systems.

ARCHITECTURE

The Apex Lumi Platform integrates seamlessly with:

- **Apex Lumi Agents**: Lightweight software agents deployed on endpoints that collect data, monitor system activities, and forward alerts.
- **Microsoft 365, Azure, AWS, cloud environments and other API supporting platforms**: Information ingested through API connectors
- **Apex Lumi Server**: Centralized management entity that analyzes log data, applies security rules, and orchestrates incident response actions.
- **Apex Lumi Dashboard**: User-friendly interface for visualizing security data, managing alerts, and configuring system settings.

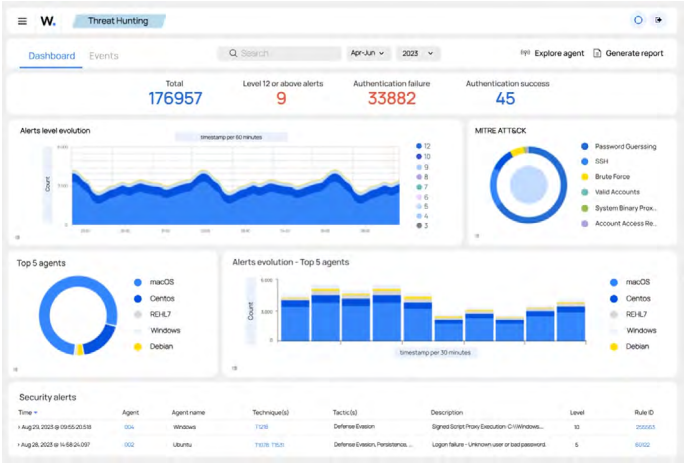
BENEFITS OF THE APEX LUMI PLATFORM

- **Comprehensive Security Solutions**: Combines XDR and SIEM functionalities, providing a unified platform for threat detection and compliance management.
- **Cost-Effective**: Utilizing open-source technology allows for significant cost reductions, making the platform accessible to SME companies.
- **Cloud-Based Flexibility**: Provides scalable and accessible security solutions tailored to businesses of all sizes.
- **Expert Support**: Apex Security ensures exceptional support and consultation to optimize your security investment.

The Apex Lumi Platform is built fully redundant, ensuring high availability and reliability. Critical components are duplicated, minimizing potential downtime and enhancing resilience against failures. This architectural design guarantees uninterrupted service delivery, even in the event of hardware or software issues.

USE CASES

- **Incident Response**: Automated responses and incident management workflows to quickly contain threats and mitigate potential damage.
- **Regulatory Compliance**: Streamlined auditing and reporting capabilities to assist organizations in meeting industry regulations such as PCI DSS, GDPR, and HIPAA.
- **Threat Hunting**: Advanced analytics and customization options empower security teams to proactively identify and neutralize threats before they impact the organization.



APEX SECURITY
Apex Security B.V.
Galvanistraat 1 6716 AE EDE
+31 (0)85 4896060
info@apexsecurity.nl
www.apexsecurity.nl