SQURA
CYBERSEC

powered by
lintasarta

CYBER SECURITY WITH A HEART

BRAND PURPOSE

PROTECTION THROUGH THE POWER OF PEOPLE AND TECHNOLOGY

We aim to empower people with Cybersecurity knowledge, expertise and tools in order to make businesses more digitally secure.

EMBRACING THE HEART CULTURE

HUMANIZED
Connect with consultative and story-telling approach

EMPATHIC
Sense of ownership and empathy to the clients' needs

ADAPTIVE
Responsive and proactive, up-to-date with change and opportunity

RESOURCEFUL
Creatively presents solution and always learning

TRUSTWORTHY
Dependable and to be trusted in making businesses more digitally secure

WHO WE ARE

SQURA is one of Lintasarta Product Solutions, a leading service provider of ICT communication in Indonesia for more than three decades.

WHAT WE DO

Study has shown that 95% of cyber incidents is the result of human error. Recognizing this, we believe that cybersecurity should be the responsibillity of everyone. At SQURA, we aim to increase cybersecurity awareness amongst employees, minimizing complexity through managed service and ultimately delivering a peace of mind.

SQURA

Our brand name, SQURA is thoughtfully named to associate with the words "SECURE" and "SQUARE".

SQURA Solution

Based on NIST Cybersecurity Framework

Identify

- SQURA VulScan
- SQURA PenTest
- SQURA FixPatch
- SQURA Threat Intelligence

Protect

- SQURA NGFW
- SQURA WAF
- SQURA LB OC
- SQURA SASE
- SQURA AntiDDoS
- SQURA EDR
- SQURA EdgeProtect
- SQURA MyMail
- SQURA NDR

Detect & Respond

- SQURA SOC (with SOAR)
- SQURA MDR
- SQURA NOC

Recover

- Deka Vault - Cloud Backup & DR
- SQURA DFIR

SQURA Solution

Identify

Cyber Threat Intelligence Analysis

VAPT

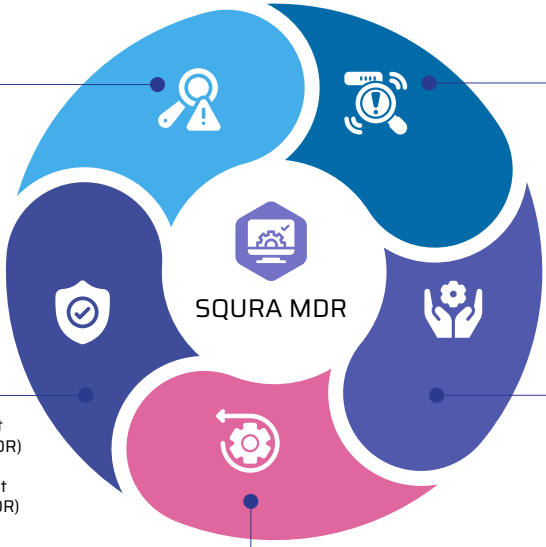
Security Awareness

Audit Support

Detect

24x7 (SOC) Monitoring

Pro-active Threat Hunting



Protect

Advanced Network Threat Detection & Response (NDR)

Advanced Endpoint Threat Detection & Response (EDR)

Respond

Automated Incident Response

Takedown Services

Malware Sandboxes

Recover

Digital Forensics and Incident Response (DFIR)

Continuous Improvement

SQURA Solution

Banking & Finance

Common industry challenges :

- ✓ Cyber-attacked 700 times a week
- ✓ Phising scams and DoS attack
- ✓ Secure connectivity for branches
- ✓ Enable secure remote workforce
- ✓ Complexity of security operation

Our suggested services:

- SQURA EdgeProtect
- SQURA WAF
- SQURA NGFW
- SQURA SOC

GOV & PUBLIC SECTOR

Common industry challenges :

- ✓ The biggest target
- ✓ Huge volume of threats
- ✓ Lack of cybersecurity awareness
- ✓ Change in the way they work

Our suggested services:

- SQURA VulScan
- SQURA WAF
- SQURA NGFW
- SQURA SOC

Education & Healthcare

Common industry challenges :

- ✓ Most targeted industry in 2021
- ✓ Malware and ransomware attacks
- ✓ Least resource than other industry
- ✓ Manage unique information

Our suggested services:

- SQURA VulScan
- SQURA NGFW

Our Tech Partner :

Cisco Partner, LogRhythm, paloalto, FORTINET, VERSA, f5, NETSCOUT, CYFIRMA, tenable, eset, DARKTRACE, proofpoint

Detect and remediate vulnerabilities proactively

SQURA VulScan

USPs from the Tech side:

- Provides complete visibility into an organization's attack surface.
- Offers continuous monitoring to detect vulnerabilities and threats in real-time.
- Includes automation capabilities that help reduce manual effort.
- Integrate with a wide range of 3rd party tools such as SIEMs and SOARs.
- Includes pre-built compliance templates to meet regulatory requirements.

USPs from the Service side:

- Security as a Service (SECaaS) from MSSP company with a subscription model.
- Service sizing is based on the number of assets. Start from 65 IPs for the organization's infrastructure and 1 FQDN for the organization's web apps.
- Provides regular performance reports, allowing the organization to make improvements as needed.
- Experienced and certified security professionals who have expertise in different areas of cybersecurity.
- Organizations can avoid the cost of purchasing, maintaining, and upgrading security infrastructure and software.

Automated pentesting for continuous security testing

SQURA PenTest

USPs from the Tech side:

- Provides automated testing techniques to simulate attacks
- Reduce the time and resources required for manual penetration testing.
- Allow for more frequent testing with consistent results.
- Generates a detailed report that provides recommendations for remediation.
- Can not completely replace manual penetration testing by humans.

USPs from the Service side:

- Security as a Service (SECaaS) from MSSP company with a subscription model.
- Service sizing is token-based licensing. Start from 10 token IPs for the organization's infrastructure and 5 token FQDNs for the organization's web apps.
- Provides regular performance reports, allowing the organization to make improvements as needed.
- Experienced and certified security professionals who have expertise in different areas of cybersecurity.
- Organizations can avoid the cost of purchasing, maintaining, and upgrading security infrastructure and software.

Patch smarter, not harder: Automated patch management

SQURA FixPatch

USPs from the Tech side:

- Automated patching to streamline the patching process.
- Reduce the time and effort to keep systems up-to-date.
- Customizable patching policies include patching schedules and ensuring that critical patches are deployed first.
- Support for a wide range of OS and applications.

USPs from the Service side:

- Security as a Service (SECaaS) from MSSP company with a subscription model.
- Service sizing is based on the number of endpoints. Start from 100 endpoints.
- Provides regular performance reports, allowing the organization to make improvements as needed.
- Experienced and certified security professionals who have expertise in different areas of cybersecurity.
- Organizations can avoid the cost of purchasing, maintaining, and upgrading security infrastructure and software.

You Can't Control What You Can't See.

SQURA Threat Intelligence

Key Features:

Attack Surface Intelligence:
Identifies external vulnerabilities, including weak configurations, vulnerable ports, and cloud instances, aligning them with potential cybercriminal interest.

Vulnerability Intelligence:
Provides insights into vulnerabilities targeted by cybercriminals, offering contextual information on threats specific to your industry or technology.

Brand Intelligence:
Monitors for brand infringement, fake profiles, and social sentiments, protecting your brand's integrity online.

Digital Risk Discovery and Protection:
Detects exposed sensitive data, including CII, PII, IP, and potential sources of data leaks like emails and source code.

Takedown Services:
Facilitates the legal removal of malicious online assets, significantly reducing their reach and mitigating their effects on your organization.

Key Benefits:

Enhanced Visibility:
Gain a comprehensive view of your digital threat landscape, understanding your vulnerabilities from a hacker's perspective.

Strategic Countermeasures:
Knowledge of your adversaries enables targeted defenses against the most relevant threats, moving from reactive to proactive security.

Brand Protection:
Safeguards your brand's reputation by monitoring and addressing potential infringements and impersonations.

Predictive and Contextual Intelligence:
Delivers early warnings and personalized insights, allowing for preemptive action against emerging threats.

IDENTIFY

Next-gen security for modern threats

SQURA NGFW

USPs from the Tech side:

- Provide granular visibility and control over various application usage.
- Leverage ML and automation to prevent threats including 0-day attacks and APTs.
- Meet the needs of organizations of all sizes, from SMBs to large enterprises.
- Integrate with other security solutions to provide a comprehensive security ecosystem.

USPs from the Service side:

- Security as a Service (SECaaS) from MSSP company with a subscription model.
- Service sizing is based on the number of endpoints. Start from 100 endpoints.
- Provides regular performance reports, allowing the organization to make improvements as needed.
- Experienced and certified security professionals who have expertise in different areas of cybersecurity.
- Organizations can avoid the cost of purchasing, maintaining, and upgrading security infrastructure and software.

Next-gen security for remote access

SQURA SASE

USPs from the Tech side:

- Built using cloud architecture to allow organizations to deploy and manage their network security infrastructure in a more agile and flexible way.
- Comprehensive sets of security features, including NGFW, ZTNA, SWG, and many more.
- Helps organizations secure and optimize their branch office dan WFA employees' connectivity.
- Allows organizations to monitor their networking and security infrastructure from a single console.

USPs from the Service side:

- Built using cloud architecture to allow organizations to deploy and manage their network security infrastructure in a more agile and flexible way. **The SASE PoP is in Indonesia to support fast and stable connections.**
- Service sizing is based on bandwidth. Start from 100 Mbps.
- Provides regular performance reports, allowing the organization to make improvements as needed.
- Experienced and certified security professionals who have expertise in different areas of cybersecurity.
- Organizations can avoid the cost of purchasing, maintaining, and upgrading security infrastructure and software.

Next-Gen Endpoint Security Made Simple

SQURA EdgeProtect

USPs from the Tech side:

- Reliable and easy-to-use endpoint protection for devices such as PCs and File Servers
- Provides advanced endpoint protection against various types of malware threats, including viruses, spyware, and many more.
- The application will work quickly without slowing down computer performance.
- Designed with an intuitive and user-friendly interface.

USPs from the Service side:

- Security as a Service (SECaaS) from MSSP company with a subscription model.
- Service sizing is based on the number of endpoints. Start from 100 endpoints.
- Provides regular performance reports, allowing the organization to make improvements as needed.
- Experienced and certified security professionals who have expertise in different areas of cybersecurity.
- Organizations can avoid the cost of purchasing, maintaining, and upgrading security infrastructure and software.

Bulletproof protection for your web presence

SQURA WAF

USPs from the Tech side:

- Comprehensive protection against a wide range of web application attacks.
- Offers granular control over HTTP and HTTPS traffic.
- Meet the needs of organizations of all sizes, from SMBs to large enterprises.
- Integrate with other security solutions to provide a comprehensive security ecosystem.

USPs from the Service side:

- Security as a Service (SECaaS) from MSSP company with a subscription model.
- Service sizing is based on the number of devices. Start from 1 device.
- Provides regular performance reports, allowing the organization to make improvements as needed.
- Experienced and certified security professionals who have expertise in different areas of cybersecurity.
- Organizations can avoid the cost of purchasing, maintaining, and upgrading security infrastructure and software.

SQURA MFA

USPs from the Tech side:

- Rapid deployment and seamless integration with existing IT infrastructure and minimizing disruption.
- Seamless and user-friendly authentication experience that enhances security without compromising on convenience
- Adopt a Zero Trust approach with DUO, ensuring that every access request is thoroughly verified.
- Meet regulatory compliance requirements robust security controls and comprehensive audit trails.

USPs from the Service side:

- Security as a Service (SECaaS) from MSSP company with a subscription model.
- Service sizing is based on the number of Users. Stars from minimum 100 Users.
- Provides regular performance reports, allowing the organization to make improvements as needed.
- Experienced and certified security professionals who have expertise in different areas of cybersecurity.
- Organizations can avoid the cost of purchasing, maintaining, and upgrading security infrastructure and software.

Secure Your Network with Volumetric DDoS Protection

SQURA AntiDDoS

USPs from the Tech side:

- Designed to provide protection against Distributed Denial of Service (DDoS) attacks.
- Comprehensive protection against volumetric DDoS attacks.
- Real-time detection and mitigation techniques to quickly identify and stop volumetric DDoS attacks.
- Scalable solution to fit your specific business needs.

USPs from the Service side:

- Security as a Service (SECaaS) from MSSP company with a subscription model.
- Service sizing is based on bandwidth. There is no minimum subscription **as long as the internet connection is provided by Lintasarta.**
- Provides regular performance reports, allowing the organization to make improvements as needed.
- Experienced and certified security professionals who have expertise in different areas of cybersecurity.
- Organizations can avoid the cost of purchasing, maintaining, and upgrading security infrastructure and software.

Email Security that Goes Beyond Expectations

SQURA MyMail

USPs from the Tech side:

- Comprehensive and advanced email security solution
- Advanced protection against malicious attachments or links and malware-free threats.
- Identify and secure sensitive information sent in email using a policy-driven data loss prevention filter.
- Helps keep your business communications up and running at all times.

USPs from the Service side:

- Security as a Service (SECaaS) from MSSP company with a subscription model.
- Service sizing is based on the number of email users. Start from 100 email users.
- Provides regular performance reports, allowing the organization to make improvements as needed.
- Experienced and certified security professionals who have expertise in different areas of cybersecurity.
- Organizations can avoid the cost of purchasing, maintaining, and upgrading security infrastructure and software.

SQURA LB OC

USPs from the Tech side:

- A load balancing and application delivery controller (ADC) solution designed to improve the performance, availability, and security of applications.
- Uses intelligent traffic steering capabilities to ensure that traffic is directed to the most appropriate application server, based on factors such as performance and availability.
- Meet the needs of organizations of all sizes, from SMBs to large enterprises.
- Add-on service for Cloudeka customers, to enhance their application security.

USPs from the Service side:

- Security as a Service (SECaaS) from MSSP company with a subscription model.
- Service sizing is based on the number of FQDN. Start from 1 FQDN.
- Provides regular performance reports, allowing the organization to make improvements as needed.
- Experienced and certified security professionals who have expertise in different areas of cybersecurity.
- Organizations can avoid the cost of purchasing, maintaining, and upgrading security infrastructure and software.

Advanced Solutions for Intelligent Endpoint Security

SQURA EDR

USPs from the Tech side:

- Provides a highly effective and comprehensive endpoint security solution
- Provides real-time visibility into endpoint activity and allows for immediate response to security incidents.
- Built on cloud-native infrastructure, allowing it to be easily deployed across large and complex organizations.
- A lightweight agent that has a minimal impact on endpoint performance.
- Integrates seamlessly with other security solutions such as SIEM, providing a comprehensive security posture to an organization.

USPs from the Service side:

- Security as a Service (SECaaS) from MSSP company with a subscription model.
- Service sizing is based on the number of endpoints. Start from 100 endpoints.
- Provides regular performance reports, allowing the organization to make improvements as needed.
- Experienced and certified security professionals who have expertise in different areas of cybersecurity.
- Organizations can avoid the cost of purchasing, maintaining, and upgrading security infrastructure and software.

PROTECT DETECT RESPOND

Complete network detection and response through NDR

SQURA NDR

USPs from the Tech side:

- Continuously monitors an organization's network, learning the normal behavior of devices, users, and applications.
- Allows to detect deviations from the norm that may indicate a security breach or threat.
- Provides autonomous response capabilities to automatically respond to threats.
- Integrates seamlessly with other security solutions such as SIEM and endpoint protection, providing a comprehensive security posture to an organization.

USPs from the Service side:

- Security as a Service (SECaaS) from MSSP company with a subscription model.
- Service sizing is based on the number of IPs. The read-only dashboard will be provided by request.
- Provides regular performance reports, allowing the organization to make improvements as needed.
- Experienced and certified security professionals who have expertise in different areas of cybersecurity.
- Organizations can avoid the cost of purchasing, maintaining, and upgrading security infrastructure and software.

PROTECT DETECT RESPOND

SQURA SOC

USPs from the Tech side:

- Analyze data from various sources, including network traffic, log files, and user activity, to identify anomalous behavior that may indicate a security threat.
- Automates many of the tasks associated with threat detection and response, such as incident investigation and response.
- Helps organizations to comply with various regulatory requirements by providing real-time monitoring and reporting capabilities.
- Integrates seamlessly with other security features such as SOAR, FIM, UEBA, Threat Intelligence, and NTA.

USPs from the Service side:

- Security as a Service (SECaaS) from MSSP company with a subscription model.
- Service sizing is based on the number of messages per second. Start from 500 MPS. The read-only dashboard will be provided.
- Provides regular performance reports, allowing the organization to make improvements as needed.
- Experienced and certified security professionals who have expertise in different areas of cybersecurity.
- Organizations can avoid the cost of purchasing, maintaining, and upgrading security infrastructure and software.

DETECT RESPOND

Seamless monitoring for network availability

SQURA NOC

USPs from the Tech side:

- Allowing users to monitor network performance, identify issues, and troubleshoot problems quickly.
- Automatically discover devices and interfaces on the network, reducing the time and effort required to set up and configure the monitoring system.
- Real-time alerts when network performance thresholds are breached, allowing users to take proactive measures to prevent downtime and network outages
- Add-on service for Cloudeka customers, to enhance their network monitoring capability.
.

USPs from the Service side:

- Security as a Service (SECaaS) from MSSP company with a subscription model.
- Service sizing is based on the number of nodes. Start from 1 node.
- Provides regular performance reports, allowing the organization to make improvements as needed.
- Experienced and certified security professionals who have expertise in different areas of cybersecurity.
- Organizations can avoid the cost of purchasing, maintaining, and upgrading security infrastructure and software.

Secure your digital frontier with SQURA DFIR - your elite defense against cyber threats

SQURA DFIR

Key Features:

Comprehensive Digital Forensics:
Deep analysis of digital evidence to uncover the specifics of cyber incidents.

Advanced Incident Response:
Swift and strategic responses to mitigate and prevent future cyber threats.

Clear Visibility:
Provides comprehensive insights into hacker activities, ensuring no part of the network is left unchecked.

Incident Impact Assessment:
Evaluates the severity and potential impact of incidents, aiding in prioritizing response efforts.

SQURA DFIR

Key Benefits:

Enhanced Security Posture:
Proactively identifies vulnerabilities, strengthening defenses against cyber attacks.

Operational Continuity:
Minimizes downtime and operational disruptions following cyber incidents, ensuring business processes continue smoothly.

Regulatory Compliance:
Helps organizations meet legal and regulatory requirements by providing thorough investigation and reporting capabilities.

Informed Decision-Making:
Offers insights into threat landscapes, aiding in strategic security planning and investment.

SQURA XDR

USPs from the Tech side:

- integration across various security layers, providing a holistic approach to threat detection and response.
- customizable dashboards and detailed reporting features that provide actionable insights.
- 24/7 managed services support of security experts is continuously monitoring and protecting environment.
- Leverage cutting-edge AI and machine learning algorithms to detect and respond to sophisticated threats in real-time.

SQURA XDR

USPs from the Service side:

- Security as a Service (SECaaS) from MSSP company with a subscription model.
- Service sizing is based on the number of endpoint and network size.
- Provides regular performance reports, allowing the organization to make improvements as needed.
- Experienced and certified security professionals who have expertise in different areas of cybersecurity.
- Organizations can avoid the cost of purchasing, maintaining, and upgrading security infrastructure and software.

SQURA MDR

24x7 Security Operations Center (SOC) Monitoring

- Correlation & Verification (Alert Validation)
- Suggestion & Remediation Report
- Bi-Weekly / Monthly Meeting
- Client Support and Communication

Advanced Network Threat Detection & Response (NDR)

- Behavioral Network detection using Machine Learning & Artificial Intelligence

Advanced Endpoint Threat Detection & Response (EDR)

- Behavioral Endpoint detection using Machine Learning & Artificial Intelligence

Automated Incident Response

- Using SOAR
- Integrating all security and Network tools

Cyber Threat Intelligence Analysis

- Attack Surface Discovery / Attack Surface Management (ASM)
- Vulnerability Intelligence
- Brand Intelligence
- Dark Web & Digital Risk Discovery Intelligence
- Situational Awareness
- Cyber Intelligence
- Malware Sandbox
- Takedown Services
- Early Warning
- Security Bulletin / Security Advisory Report

Pro-active Threat Hunting

Searches for hidden threats to ensure they are identified early.

Support Audit

Helps organizations by Providing necessary data during audit requirements.

IDENTIFY | PROTECT | DETECT | RESPOND | RECOVER

SQURA MDR

Digital Forensics and Incident Response (DFIR)

Focuses on investigating incidents, containing the damage, eradicating the threat, and recovering from incidents to improve security and capabilities.

Vulnerability Assessment

- Scan Regular
- Scan On-Demand

Penetration Testing

- White Box
- Grey Box
- Black Box

Security Awareness

- Phising Simulation
- Security Awareness Training
- Cyber security awareness report

Continuous Improvement

- Post-Breach Lesson Learned
- Quarterly Security Improvement Plans
- Annual Security Posture Review

IDENTIFY PROTECT DETECT RESPOND RECOVER

SQURA
CYBERSEC

Consult with us to find the best solution for your business

SQURA CYBERSEC

Menara Thamrin 12th Floor

Jl. M. H. Thamrin Kav. 3 Jakarta 10250 14052

+6221 230 3567

info@squracybersec.id

www.squracybersec.id