Palo Alto

COMPLIANCE INTERVIEW QUESTIONS GUIDE

One Step Closer Towards Your Dream Job...
Q1. HOW DOES THE NEXT-GENERATION SECURITY PLATFORM CONTRIBUTE TO GDPR COMPLIANCE?

The vast majority of GDPR requirements center around data management, namely data collecting and processing. There are obligations to provide notice when collecting personal data, prohibitions on unauthorized data processing, requirements to keep records of data processing, a duty to appoint a data protection officer in certain instances, and rules regarding transfer of personal data to third parties and third countries, among others.

But this should not overshadow the fact that data security is also a pillar of GDPR. GDPR has specific security-related language, as described in detail below. Further, a key component of protecting personal data is keeping it secure - both from exfiltration by cyber adversaries and from internal leakage. Thus, as they prepare for the GDPR, it is imperative that organisations’ investments in compliance activities and information management processes and technologies be complemented with appropriate investments in cybersecurity.
Q2. HOW DOES PALO ALTO NETWORKS HELP IN A ORGANISATION'S SECURITY AND DATA PROTECTION EFFORTS RELATED TO GDPR COMPLIANCE?

1) Securing Personal Data:
GDPR requires security of data processing, accounting for the state of the art. Palo Alto's Next-Generation Security Platform provides just that: security at the application, network and endpoint level.

2) Data Breach Prevention:
Prevention of data breaches, whether a result of hacking or accidental leakage, is crucial for compliance with the GDPR. Proper cybersecurity is essential to ensure your organisation’s personal and business-critical data and applications remain protected. Our Next-Generation Security Platform is built for prevent

3) Data Breach Notification:
In the unfortunate instance of a data breach, it must be reported. Palo Alto's Next-Generation Security Platform can help determine what personal data was compromised, and contribute key facts about measures taken to address the breach.
Securing Personal Data
GDPR requires security of data processing, accounting for the state of the art. Palo Alto Networks platform secures data at the application, network and endpoint level, as well as in the cloud.

State-of-the-Art Technology
The Palo Alto Networks Next-Generation Security Platform combines network and endpoint security with threat intelligence to provide automated protection and prevent cyberattacks, not just detect them.

Data Breach Prevention
The Palo Alto Networks Platform enables four key prevention techniques relevant to data security, simultaneously contributing to GDPR compliance.
- Complete Visibility
- Reduce the attack surface
- Prevent known threats
- Prevent unknown threats
Q3. WHAT ARE THE ADDITIONAL FEATURES AND CAPABILITIES PROVIDED BY PALO-ALTO? (Continued...)

Manage Security Processes Centrally
Panorama™ network security management empowers organisations with easy-to-implement, consolidated policy creation and management of our next-generation firewalls. With Panorama, you can implement both centralised and regional policy, and easily delegate to regional admins as needed or preferred.

Prevent Data Exfiltration or Leakage
With Palo Alto’s Next-Generation Security Platform, each critical stage within the attack lifecycle is met with a defence model to prevent data exfiltration – from the attacker’s initial attempt to breach the perimeter, to delivering malware or exploiting the endpoint, to moving laterally through the network until the attacker reaches the primary target and attempts to exfiltrate personal and sensitive data.

Data Breach Notification
The Palo Alto Platform can help maintain compliance with this GDPR requirement in the event of a breach. For example, AutoFocus provides the analytics details needed for remediation, helping to understand who the user was, what the threat was, the impact and the level of risk. All of this can help with notification requirements.

To read in detail about all the above, visit the link below:
Q4. HOW TO BREAK THE CYBER ATTACK LIFE CYCLE?

To protect a company’s network and data from attack, prevention must occur at each stage to block the attackers’ ability to access and move laterally within the organization or steal sensitive data. The following are the different stages of the attack lifecycle and steps that should be taken to prevent an attack at each stage.

1) Reconnaissance

2) Weaponization and Delivery

3) Exploitation

4) Installation

5) Command and Control

6) Actions on the Objective

To read in detail about all the above, visit the link below:
Q5. WHAT IS A ZERO TRUST ARCHITECTURE?

In Zero Trust, you identify a “protect surface.” The protect surface is made up of the network’s most critical and valuable data, assets, applications and services – DAAS, for short. These protect surfaces are unique to each other because it contains only what’s most critical to an organization’s operations, the protect surface is orders of magnitude smaller than the attack surface, and it is always knowable.

With your protect surface identified, you can identify how traffic moves across the organization in relation to protect surface. Understanding who the users are, which applications they are using and how they are connecting is the only way to determine and enforce policy that ensures secure access to your data. Now you should put controls in place as close to the protect surface as possible, creating a micro-perimeter around it. This micro-perimeter moves with the protect surface, wherever it goes. You can create a micro-perimeter by deploying a segmentation gateway, more commonly known as a next-generation firewall, to ensure only known, allowed traffic or legitimate applications have access to the protect surface.

The segmentation gateway provides granular visibility into traffic and enforces additional layers of inspection and access control with granular Layer 7 policy based on the Kipling Method, which defines Zero Trust policy based on who, what, when, where, why and how. The Zero Trust policy determines who can transit the microperimeter at any point in time, preventing access to your protect surface by unauthorized users and preventing the exfiltration of sensitive data. Zero Trust is only possible at Layer 7.

To continue reading....kindly click on the link below:
https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecture
Designed from the outside in, 20th-century hierarchical networks have traditionally relied on classifying users as “trusted” and “untrusted.” Unfortunately, this methodology has proven to be unsecure. With increased attack sophistication and insider threats, operating on the assumption that everything inside an organization’s network can be trusted is no longer viable.

Enter Zero Trust. Rooted in the principle of “never trust, always verify,” a Zero Trust network offers a different approach to security. By taking advantage of micro-segmentation and granular perimeters of enforcement around your most critical data, Zero Trust combats the exfiltration of sensitive data and prevents threats from moving laterally within a network.

Unfortunately, the design paradigms of legacy security models leave companies reluctant to adopt Zero Trust as it’s thought to be difficult, costly and disruptive. In fact, it’s much simpler to deploy than its legacy counterparts. To shift how we think about security design and eradicate some of the stigmas around deploying Zero Trust, it’s important to understand security as it predates the introduction of Zero Trust.

To continue reading click below:
https://www.paloaltonetworks.com/cyberpedia/what-was-there-before-zero-trust
Q7. HOW TO IMPLEMENT ZERO TRUST USING THE FIVE-STEP METHODOLOGY?

Using a five-step model for implementing and maintaining Zero Trust, you can understand where you are in your implementation process and where to go next. These steps are:

1) Define the Protect Surface:
With Zero Trust, rather you determine your protect surface. The protect surface encompasses the critical data, application, assets and services—DAAS—most valuable for your company to protect. Once defined, you can move your controls as close as possible to that protect surface to create a micro-perimeter with policy statements that are limited, precise and understandable.

2) Map the Transaction Flows:
The way traffic moves across a network determines how it should be protected. Thus, it’s imperative to gain contextual insight around the inter-dependencies of your DAAS. Documenting how specific resources interact allows you to properly enforce controls and provides valuable context to ensure the controls help protect your data, rather than hindering your business.

3) Architect a Zero Trust Network:
You can now map out the Zero Trust architecture, starting with a Next-Generation Firewall. The NGFW acts as a segmentation gateway, creating a microperimeter around the protect surface. With a segmentation gateway, you can enforce additional layers of inspection and access control, all the way to Layer 7, for anything trying to access resources within the protect surface.
Q7. HOW TO IMPLEMENT ZERO TRUST USING THE FIVE-STEP METHODOLOGY? (Continued...)

4) Create the Zero Trust Policy:
Once the network is architected, you will need to create Zero Trust policies using the “Kipling Method” to whitelist which resources should have access to others. Kipling, well known to novelists, put forth the concept of “who, what, when, where, why and how” in his poem “Six Serving Men.”

5) Monitor and Maintain the Network:
This final step includes reviewing all logs, internal and external, all the way through Layer 7, focusing on the operational aspects of Zero Trust. Since Zero Trust is an iterative process, inspecting and logging all traffic will provide valuable insights into how to improve the network overtime.

Once you have completed the five-step methodology for implementing a Zero Trust network for your first protect surface, you can expand to iteratively move other data, applications, assets or services from your legacy network to a Zero Trust network in a way that is cost-effective and non-disruptive.

To read in detail about The Five Step Methodology, click on the link below:
Looking for Networking Training?

Join our CCNA, CCNP, CCIE, F5, Checkpoint, Palo Alto & Fortinet Certification Courses

Click here to Sign Up for a Free Demo Session

REGISTER FOR FREE DEMO