I-MEDITA

Training | Development | Placement

Palo Alto

CYBER SECURITY

INTERVIEW QUESTIONS GUIDE

One Step Closer Towards Your Dream Job...

Q1. WHAT IS CYBERSECURITY?

Cybersecurity refers to a set of techniques used to protect the integrity of an organization’s security architecture and safeguard its data against attack, damage or unauthorized access.

Q2. WHY IS CYBERSECURITY REQUIRED?

At its core, cybersecurity involves protecting information and systems from cyberthreats. Cyberthreats take many forms, such as application attacks, malware, ransomware, phishing and exploit kits. Recent technological advancements have opened up new possibilities for cybersecurity, but unfortunately, adversaries have benefited from these advancements, as well. Taking advantage of automation, attackers can deploy large-scale attacks at significantly reduced costs. Further, the cybercrime economy makes sophisticated attacks easy to deploy and available to a wide variety of motivated adversaries. Cybersecurity tools and technologies should incorporate automation, machine learning and shared threat intelligence to help organizations get ahead and stay on the cutting edge to combat advanced threats, such as:

- **DNS Tunneling:**

Domain Name System is a protocol that translates human-friendly URLs into machine-friendly IP addresses. Cybercriminals know that DNS is widely used, trusted and often un-monitored. DNS tunneling exploits the protocol to transfer malware and other data through a client-server model.

- **Malicious Cryptomining:**

Browser-based Cryptomining attacks are possible when an attacker has found a way to inject JavaScript into a website that allows them to hijack the processing power of site visitors' devices to mine cryptocurrency, such as bitcoin. In the case of malware-based Cryptomining, a user's entire device is taken over and its CPU used at a higher level to mine currency.

- **Ransomware:**

Ransomware is the focus of a criminal business model that installs malicious software on a device and holds valuable files, data, or information ransom. With its low barrier to entry and high revenue potential, ransomware is the largest threat facing organizations

.

Q3. HOW TO MAINTAIN EFFECTIVE CYBERSECURITY?

Enabling automation, machine learning and shared threat intelligence in their security architecture will help organizations keep pace with the growth of sophisticated cyberattacks. Machine learning can help accurately identify variations of known threats, recognize patterns, predict the next steps of an attack, and inform automation tools to create and implement protections across the organization, all in near-real time. With shared threat intelligence, anything one user sees, identifies or prevents benefits all other members of the shared community. More comprehensive prevention, attainable more quickly, reduces overall cybersecurity risk to something easier to manage.

Organizations should consider a natively integrated, automated security platform specifically designed to provide consistent, prevention-based protection for endpoints, data centers, networks, public and private clouds, and software-as-a-service environments.

The Palo Alto Networks Security Operating Platform was designed to help your teams operate simply and efficiently to protect your organization. It prevents successful attacks, including attacks in progress, to secure the enterprise, the cloud and the future.

Secure the Enterprise

Built for simplicity, our tightly integrated innovations are easy to operate, delivering consistent protection across network, cloud and mobile users.

Secure the Cloud

Prisma is the industry’s most complete cloud security offering. Accelerate your cloud journey with a product suite designed to secure today's complex IT environments.

Secure the Future

Cortex is the industry's only open and integrated AI-based continuous security platform that constantly evolves to stop the most sophisticated threats.

Q4. 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.

Q4. 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:
https://www.paloaltonetworks.com/cyberpedia/zero-trust-5-step-methodology

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, click on the link below:
https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecture


I-MEDITA
Training | Development | Placement
INDIA'S MOST TRUSTED
NETWORKING TRAINING COMPANY
CCNA

Q6. WHAT IS SECURITY OPERATING PLATFORM?

First, the various elements of a Security Operating Platform must be implemented in the correct positions within a security architecture to be able to enforce security rules across an organization’s security posture. Second, the platform must be agile and have the ability to very quickly turn unknown threats into known threats, on a global level, and automatically share the new threat data. What’s more, a Security Operating Platform should be able to automatically extend new protections within an organization’s security posture based on this new data to stop the spread of an attack.

Q7. WHY A SECURITY OPERATING PLATFORM?

Legacy security systems, made up of cobbled-together point solutions, have proven themselves inadequate in preventing the rising volume and sophistication of cyberattacks. Too many security tools depend too heavily on manual intervention, which is slow by nature and can't provide new protections quickly enough to make a meaningful impact on an ongoing targeted attack. Manual detection and remediation does little to reduce risk, as it is mainly done after the fact, with limited visibility and manual correlation of the different attack elements. Not only is this approach expensive in terms of time and money, it makes it very difficult to see the attack as a whole and distracts from the identification of true threats, leaving organizations vulnerable.

Truly reducing cyber risk requires having integrated, automated, and effective controls in place to detect and prevent threats, both known and unknown, at every stage of the attack lifecycle. A Security Operating Platform, built from the ground up for prevention, offers full visibility of traffic–throughout the network, cloud and endpoints–enabling organizations across the globe to protect themselves against cyberattacks, based on how or where applications and data reside or are utilized.

Visibility into all traffic, classified by application, user and content, provides the context necessary to enforce dynamic security policy and reduce the attack surface, based on the assessed risk. Leveraging information from other security-related events to prevent all known threats, followed by detection and prevention of new threats based on a correlated and holistic view of the attack, are crucial to successfully preventing a breach. Producing detailed threat intelligence, analysis and protections that are capable of preventing both known and unknown threats and automatically populating this new information across the security posture is a fundamental need. The power of a Security Operating Platform comes from the sum of all components, fueled by a global threat intelligence engine that leverages the network effects of thousands of customers, technology partners and researchers sharing threat information.

Q8. WHAT IS THE FRMEWORK OF A SEURITY OPERATING PLATFORM?

A Security Operating Platform's prevention architecture allows organizations to reduce threat exposure by first enabling applications for all users or devices in any location, and then preventing threats within application flows, tying application use to user identities across physical, cloud-based and software-as-a-service (SaaS) environments.

To enable the prevention of successful cyberattacks, a Security Operating Platform must offer four key capabilities:

1. **Full visibility.** To understand the full context of an attack, visibility of all users and devices is provided across the organization's network, endpoint, cloud and SaaS applications.
2. **Reduce the attack surface**. Best-of-breed technologies that are natively integrated provide a prevention architecture that inherently reduces the attack surface. This type of architecture allows organizations to exert positive control based on applications, users and content, with support for open comunication, orchestration and visibility.
3. **Prevent all known threats, fast.** A coordinated security platform accounts for the full scope of an attack, across the different security controls that compose the security posture. This allows organizations to quickly identify and block known threats.
4. **Detect and prevent new, unknown threats with automation.** Building security that simply detects threats and requires a manual response is too little, too late. Automated creation and delivery of near-real-time protections against new threats to the different security products in the organization's environments enable dynamic policy updates. These updates are designed to allow enterprises to scale defenses with technology, rather than people.

A true security platform will be able to minimize the spread of attacks, leveraging the network effects of a comunity of comprehensive global threat data.

Q9. WHAT IS IT-OT CONVERGENCE?

The Convergence of IT and OT

Historically, IT and OT were managed by separate organizational silos without any interdependence on one another. However, over the past decade, a slow yet steady paradigm shift has taken place.

OT systems are increasingly being provisioned with networking and computational technologies. The two worlds of IT and OT are converging, with groundwork being laid for Industrial IoT, or IIoT – a matrix of interconnected sensors, instruments and devices that collect and share data for use across many industries, such as manufacturing, oil and gas, transportation, energy/utilities, and others.

IIoT is set to play a key role in the fourth Industrial Revolution, with converged IT/OT ecosystems serving as conduits that will deploy IIoT into the 4IR ecosystem.

The merger of IT with OT is driven by the need to optimize the collection and exchange of data between machines, infrastructure assets and applications while interoperably scaling processes across physical and virtual systems. The integration promises numerous benefits: improved flow of information, process automation, advances in the management of distributed operations and better adherence to regulatory compliance.

Baldev Singh
CCIE SECURITY #37094

Saurabh Yadav
Triple CCIE (R&S, Sec, SP) #46962

Sudhanshu Bhat
CCIE VOICE #41212

Surendra Singh
CCIE R&S #60346

GET TRAINED BY CERTIFIED AND WORLD CLASS TRAINERS

I-MEDITA
Training | Development | Placement

Q10. WHAT IS THE IMPACT OF IT-OT CONVERGENCE ON ICS SECURITY?

Impact of Convergence on ICS Security

However, as the lines of distinction between IT and OT continue to fade, the attack surface of interconnected IT/OT systems continues to widen. The most common attack vector for hackers to infiltrate these systems is via the internet.

With the arrival of IIoT, every ICS sensor, instrument and device accessible over an IT/OT network is susceptible to intense weaponization with botnets that are used to launch targeted attacks on critical infrastructure, such as energy grids, power plants, water and waste management systems, food processing plants, and transportation networks.

The human-machine interface, or HMI, that connect human operators to industrial control systems are also typically networked to various IT infrastructures. The accessibility to HMIs from internet-facing business networks poses a grave risk to ICS security, making HMIs susceptible to IP-based vulnerabilities, such as authentication bypass, weak session management, unsecured ICS communication protocoling and insufficient control traffic encryption.

Attackers typically infiltrate ICS systems with both generic malware and malware designed specifically to target and attack critical infrastructure. These infiltrations often result in denial-of-service, or DoS, attacks that paralyze or entirely halt industrial operations. ICS and connected IIoT devices are also high-value targets for hackers looking to collect ransoms or sabotage rival nations by gaining access to confidential data.

Q10. WHAT IS THE IMPACT OF IT-OT CONVERGENCE ON ICS SECURITY? (Continued...)

The following table provides a basic comparison between IT and OT systems from the point of view of connectivity and security requirements.

	IT	OT
Connectivity Mechanisms	Via Telco, Wi-Fi	Via Telco, Radio, Satellite, Powerline Carrier, Wi-Fi
Security Priority	Data security with high confidentiality	Operational uptime with high availability, safety, and integrity
Security Standards	ISO-17799, 27001, NIST SP 800-53	ISA99, NERC CIP 002-009, NIST SP 800-53, NIST SP 800-82
Security Patching	Frequent	Slow to impossible
Cyber Forensics	Available	Limited, if any
Overall Impact from Security Breaches	Business impacts	Business impacts, process fluctuations, equipment damage, environmental release, personnel safety

Q11. WHAT WAS THERE BEFORE 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

Q12. WHY DO YOU NEED STATIC ANALYSIS, DYNAMIC ANALYSIS, AND MACHINE LEARNING?

Below are 3 threat identification methods that, working in conjunction, can prevent successful cyberattacks:

Dynamic Analysis

The Only Tool That Can Detect a Zero-Day Threat

With dynamic analysis, a suspected file is detonated in a virtual machine, such as a malware analysis environment, and analyzed to see what it does. The file is graded on what it does upon execution, rather than relying on signatures for identification of threats. This enables dynamic analysis to identify threats that are unlike anything that has ever been seen before.

For the most accurate results, the sample should have full access to the internet, just like an average endpoint on a corporate network would, as threats often require command and control to fully unwrap themselves. As a prevention mechanism, malware analysis can prohibit reaching out to the internet and will fake response calls to attempt to trick the threat into revealing itself, but this can be unreliable and is not a true replacement for internet access.

Malware Analysis Environments Are Recognizable and the Process Is Time-Consuming

To evade detection, attackers will try to identify if the attack is being run in a malware analysis environment by profiling the network. They will search for indicators that the malware is in a virtual environment, such as being detonated at similar times or by the same IP addresses, lack of valid user activity like keyboard strokes or mouse movement, or virtualization technology like unusually large amounts of disk space. If determined to be running in a malware analysis environment, the attacker will stop running the attack. This means that the results are susceptible to any failure in the analysis. For example, if the sample phones home during the detonation process, but the operation is down because the attacker identified malware analysis, the sample will not do anything malicious, and the analysis will not identify any threat. Similarly, if the threat requires a specific version of a particular piece of software to run, it will not do anything identifiably malicious in the malware analysis environment.

Q12. WHY DO YOU NEED STATIC ANALYSIS, DYNAMIC ANALYSIS, AND MACHINE LEARNING? (Continued...)

It can take several minutes to bring up a virtual machine, drop the file in it, see what it does, tear the machine down and analyze the results. While dynamic analysis is the most expensive and time-consuming method, it is also the only tool that can effectively detect unknown or zero-day threats.

Static Analysis

Swift Results and No Requirements for Analysis

Unlike dynamic analysis, static analysis looks at the contents of a specific file as it exists on a disk, rather than as it is detonated. It parses data, extracting patterns, attributes and artifacts, and flags anomalies.

Static analysis is resilient to the issues that dynamic analysis presents. It is extremely efficient – taking only a fraction of a second – and much more cost-effective. Static analysis can also work for any file because there are no specific requirements, environments that need to be tailored, or outgoing communications needed from the file for analysis to happen.

Packed Files Result in Lost Visibility

However, static analysis can be evaded relatively easily if the file is packed. While packed files work fine in dynamic analysis, visibility into the actual file is lost during static analysis as the repacking the sample turns the entire file into noise. What can be extracted statically is next to nothing.

Q12. WHY DO YOU NEED STATIC ANALYSIS, DYNAMIC ANALYSIS, AND MACHINE LEARNING? (Continued...)

Machine Learning

New Versions of Threats Clustered With Known Threats Based on Behavior

Rather than doing specific pattern-matching or detonating a file, machine learning parses the file and extracts thousands of features. These features are run through a classifier, also called a feature vector, to identify if the file is good or bad based on known identifiers. Rather than looking for something specific, if a feature of the file behaves like any previously assessed cluster of files, the machine will mark that file as part of the cluster. For good machine learning, training sets of good and bad verdicts is required, and adding new data or features will improve the process and reduce false positive rates.

Machine learning compensates for what dynamic and static analysis lack. A sample that is inert, doesn't detonate, is crippled by a packer, has command and control down, or is not reliable can still be identified as malicious with machine learning. If numerous versions of a given threat have been seen and clustered together, and a sample has features like those in the cluster, the machine will assume the sample belongs to the cluster and mark it as malicious in seconds.

Only Able to Find More of What Is Already Known

Like the other two methods, machine learning should be looked at as a tool with many advantages, but also some disadvantages. Namely, machine learning trains the model based on only known identifiers. Unlike dynamic analysis, machine learning will never find anything truly original or unknown. If it comes across a threat that looks nothing like anything its seen before, the machine will not flag it, as it is only trained to find more of what is already known.

Q12. WHY DO YOU NEED STATIC ANALYSIS, DYNAMIC ANALYSIS, AND MACHINE LEARNING? (Continued...)

Layered Techniques in a Platform

You need layered techniques – a concept that used to be a multivendor solution. While defense in depth is still appropriate and relevant, it needs to progress beyond multivendor point solutions to a platform that integrates static analysis, dynamic analysis and machine learning. All three working together can actualize defense in depth through layers of integrated solutions.

Palo Alto Networks Next-Generation Security Platform integrates with WildFire® cloud-based threat analysis service to feed components contextual, actionable threat intelligence, providing safe enablement across the network, endpoint and cloud. WildFire combines a custom-built dynamic analysis engine, static analysis, machine learning and bare metal analysis for advanced threat prevention techniques. While many malware analysis environments leverage open source technology, WildFire has removed all open-source virtualization within the dynamic analysis engine and replaced it with a virtual environment built from the ground up. Attackers must create entirely unique threats to evade detection in WildFire, separate from the techniques used against other cybersecurity vendors. For the small percentage of attacks that could evade WildFire's first three layers of defenses – dynamic analysis, static analysis and machine learning – files displaying evasive behavior are dynamically steered into a bare metal environment for full hardware execution.

Within the platform, these techniques work together nonlinearly. If one technique identifies a file as malicious, it is noted as such across the entire platform for a multilayered approach that improves the security of all other functions.

I-MEDITA
Training | Development | Placement

WORLD CLASS INFRASTRUCTURE

Q13. WHAT IS FedRAMP AND WHY SHOULD YOU CARE ABOUT IT?

FedRAMP is a standardized approach to security assessment, authorization and continuous monitoring for U.S. government agencies' use of cloud-based products and services. Federal agencies use this program to protect the confidentiality and integrity of their data when adopting private-sector security-, infrastructure- or platform-as-a-service technologies, abbreviated SaaS, IaaS and PaaS, respectively. Vendors of cloud services – what the program calls cloud service providers, or CSPs – follow prescribed paths to certification. Third-party assessment organizations conduct thorough assessments while the FedRAMP Program Management Office offers oversight and advice in addition to reviewing submissions and making authorization decisions.

Advantages of FedRAMP for Federal Agencies

The program offers a standardized, “do once, use many times” framework to save federal agencies time, effort and money when assessing security. At the same time, agencies retain control of the level of cybersecurity risk they are willing to accept for a particular cloud service. Agencies can evaluate authorized cloud vendors’ submission packages and decide for themselves whether the risk posture is acceptable for their needs or if they want to make changes.

Other Parties That May Be Interested in FedRAMP

A FedRAMP-authorized cloud service has applicability beyond federal agencies, including state and local governments as well as corporations that do business with federal agencies, which have similar requirements around data security and cybersecurity. They often have similar objectives, as well: to simplify operations, reduce operational overhead and improve agility by moving services to the cloud. A cloud service that receives FedRAMP authorization has met rigorous criteria for security standards, and broader public sector and public-sector affiliated corporations can confidently take advantage of such a service, knowing it is a secure alternative to using their own resources to manage and deploy infrastructure.

Q14. WHAT IS THE DIFFERENCE BETWEEN FISMA AND FedRAMP?

FISMA and FedRAMP have the same high-level goals of protecting government data and reducing information security risk within federal information systems. Both are also built on the foundation of NIST Special Publication 800-53A controls. However, there is a distinct contrast between the two in terms of federal policy, security controls and authorization.

What Is FISMA?

Enacted in 2002, FISMA – the Federal Information Security Management Act – covers the compliance parameters on storage and processing of government data. It requires federal agencies and their private-sector vendors to implement information security controls that ensure data security postures of federal information systems are protected. All private-sector firms that sell services to the federal government must comply with FISMA requirements.

The primary framework for FISMA compliance is NIST SP 800-53. Put simply, for vendors to become FISMA-compliant, they must implement recommended information security controls for federal information systems as identified in the NIST SP 800-53. FISMA assessments are traditionally focused on information systems that support a single agency.

FISMA-compliant vendors receive Authority to Operate, or ATO, only from the particular federal agency with which they are doing business. If a vendor has business contracts with multiple federal agencies, the vendor must obtain ATO from each agency because security controls may differ in accordance with the specific data security needs of each agency.

Q14. WHAT IS THE DIFFERENCE BETWEEN FISMA AND FedRAMP? (Continued...)

Let's Talk About FedRAMP

By enacting FedRAMP, the government aimed to make the cloud service provider procurement process easier on agencies. On the most basic level, FedRAMP is aimed more specifically at cloud service providers. Systems evaluated under FedRAMP for use by government agencies are commercial cloud-based systems (e.g., IaaS, PaaS, SaaS) used by private-sector enterprises.

Information systems evaluated under either FISMA or FedRAMP are categorized in accordance with FIPS 199 as high, moderate, or low based on a few different criteria. Then, based on the security categorization, applicable security controls from NIST SP 800-53 are applied to the information system as high impact, moderate impact or low impact. FedRAMP requirements include additional controls above the standard NIST baseline controls in NIST SP 800-53 Revision 4. These additional controls address the unique elements of cloud computing to ensure all federal data is secure in cloud environments.

Federal agencies know a cloud-based service is safe to use once it's awarded the FedRAMP stamp of approval, and unlike FISMA, FedRAMP ATO qualifies a cloud service provider to do business with any federal agency.Due to its wider scope, the FedRAMP certification process is also far more rigorous. The authorization program requires cloud providers to undergo an independent security assessment conducted by a third-party assessment organization, or 3PAO, to sell government cloud services to federal agencies.

Conclusion

Federal agencies looking for a FedRAMP-compliant product or service will likely also expect it to be FISMA-compliant. Cloud service providers should comply with both FISMA and FedRAMP regulations to maintain an ATO from the U.S. government.

Q15. WHAT IS 5G SECURITY?

Today’s cyberattacks can already evade mobile network security, and simply making legacy security run faster isn’t an effective maneuver. Legacy approaches that depend on disparate security elements will not scale or be able to adequately prevent successful attacks across 5G networks. 5G radio network deployments include significant expansions of small cells connecting over untrusted networks, device-to-device communications, and devices connecting to multiple cells at once. This evolution expands the threat landscape by increasing the number of intrusion points.

With billions of connected devices and critical enterprise applications relying on 5G networks, MNOs cannot wait to address attacks and security incidents after they have already happened – **they need to adopt a comprehensive end-to-end security strategy that includes:**

- Complete visibility, inspection and controls applied across layers of network including application, signaling and data planes.
- Cloud-based threat analytics combined with advanced big data and machine learning algorithms that can be used across different mobile network locations to provide swift response to known and unknown threats in real time.S
- ecurity functions integrated with open APIs to offer consistent security across software and hardware to support the distributed 5G architectures.
- Contextual security outcomes using data-driven threat prevention to find and isolate infected devices before attacks can potentially take place.

With the above, MNOs can protect their network elements and subscribers while providing differentiated network security services so enterprise verticals can confidently transform their businesses with new 5G applications. Standards and network architectures are still being defined but organizations are looking to service providers for resilient networks to securely connect their customers. Establishing application-layer visibility and consistent security across the mobile network is essential to providing future-proof security.

Q16. HOW TO GET MOST VALUE OUT OF SECURITY INVESTMENTS?

Getting the most value out of your security investments requires security awareness training, reducing legacy solutions, and leveraging automation.

1. Invest in security awareness training across all levels of the organization
Employee awareness and training is key to stopping negligence, as it historically has been a successful attack vector into an organization. Educating company personnel will make an attacker's job harder, and they will be less likely to succeed.

2. Replace duplicate and legacy technology with platforms that natively work together
Since individual, siloed products don't communicate with one another, utilizing them increases costs and creates gaps that can be exploited.

3. Leverage automation in your defenses to reduce the burden on security teams
Security teams can spend a vast majority of their time pouring over alerts and logs. If automation is incorporated into the security platform to enable low-level threats to be blocked, their time is freed up to focus on more critical issues.

I-MEDITA
Training | Development | Placement

SHAPING CAREER

EMPOWERING FUTURE

Rasika Joshi
COMPUCOM

Nakul Sonare
ZENSAR TECHNOLOGIES

Minal Ghubde
ZENSAR TECHNOLOGIES

Ketan Panpate
COMPUCOM

Mayank Chauhan
COMPUCOM

Prakash Datta
TRIOS

Vaibhav Bindu
TATA COMMUNICATIONS LIMITED

Mangesh Dhongade
COMPUCOM

Amol Sankpal
SECURVIEW

Piysuh Shrungare
ZENSAR TECHNOLOGIES

Khyati Sawant
SOPHOS

Abhijeet Kamble
COMPUCOM

Pankaj Sakore
NETSCOUT

Akshita Mankad
COMPUCOM

Amey Malotkar
AGC NETWORKS LIMITED

Arpit Kansal
CRYSTALVOXX

Pravin Valkunde
SECURVIEW

Rohit Naidu
TATA COMMUNICATIONS LIMITED

Hussain Sagwadiya
ZENSAR TECHNOLOGIES

Pravin Kawale
SECURVIEW

Q17. HOW TO REDUCE CYBERSECURITY RISK AT BOARD LEVEL?

The pervasiveness of data breaches has firmly placed the topic of cybersecurity on the agenda of the Board of Directors. It is part of their responsibility as members of the board to understand the threat landscape, current best practices, and what the company is doing to protect the employees, customers, constituents and shareholders. This has led to the creation and administration of cyber committees, working alongside other risk committees. Having a separate cyber risk committee allows for the appropriate level of focus and oversight to be integrated into enterprise risk management and planning, without overloading the audit committee with work. The below are some of the key things the Board of Directors and the cyber risk committee need to do to minimize risk and approach security with a prevention mindset:

- **Induct** security awareness training across all levels of the organization.
- **Establish** reporting protocols and systems of attestation for transfer agents and third-party vendors.
- **Replace** duplicative and legacy technology with platforms that natively work together.
- **Implement** tools that strip malicious code and links from emails, block control-and-command exploits, and hunt for malware and confidential files on sanctioned SaaS services.
- **Segment** different parts of your network into different risk zones. This can provide visibility regarding which users and applications are trying to move between them.
- **Leverage** automation in your defenses to reduce the burden on security teams.
- **Restrict** access to SaaS based tools for employees who have no business justification for using them.
- **Perform** periodic risk assessments and/or cyber audits to determine whether social engineering or additional vulnerabilities exist; pay particular attention to the safeguards and controls around employee records.

Q18. WHAT IS PCI DSS?

The Payment Card Industry (PCI) Data Security Standard (DSS) is an information security standard developed to enhance cardholder data security for organizations that store, process or transmit credit card data. Its primary purpose is to reduce vulnerability of cardholder information and prevent credit card fraud by increasing controls where cardholder data is stored, processed, or transmitted. Organizations that maintain a cardholder environment data include retailers, retail branches on any business in any industry, online payment services, banks that issue credit cards, and service providers that offer online cloud services for payment processing.Compliance to the PCI DSS is achieved by meeting a minimum set of requirements. In PCI DSS 3.0, there is about 300 requirements grouped in 12 categories as represented in the following table:

PCI Data Security Standard – High Level Overview

Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

PCI DSS compliance is mandatory to all organizations that participate in the storage, processing, or transmission of cardholder data.

To attain compliance, organizations must pass an assessment that audits all parts of the network that interact with cardholder environment. In some areas, the PCI Security Standards Council (SSC) is very prescriptive in the type of technologies and products that need to be deployed, and how these need to the deployed.

In other areas, there is no specific prescribed approach or structure for the implementation of a compliant system.

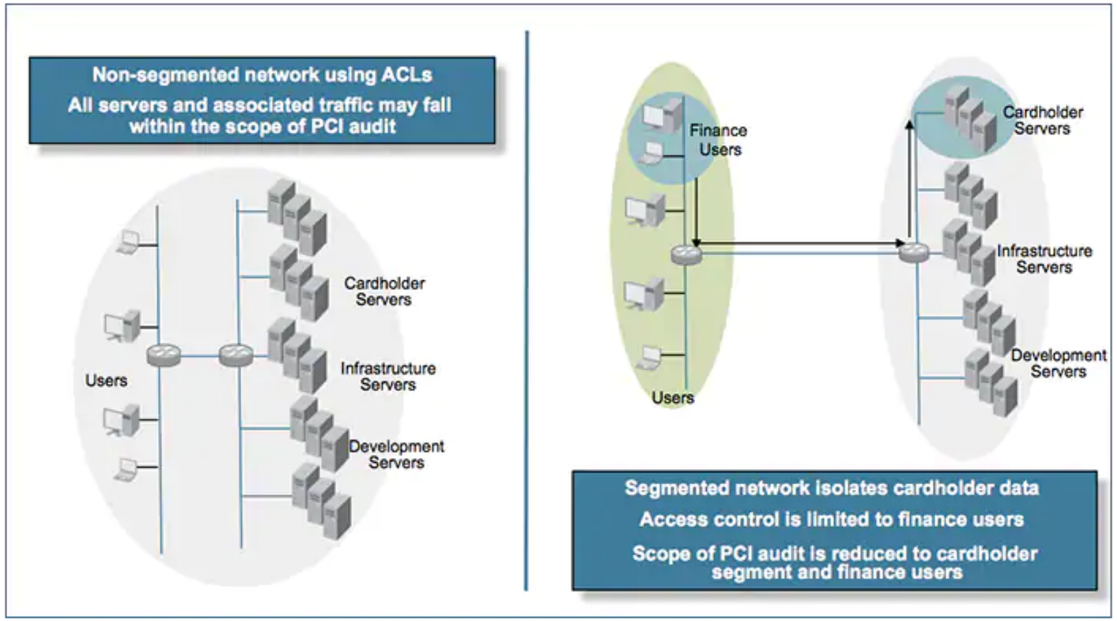
Q18. WHAT IS PCI DSS? (Continued...)

Network SegmentationAmong the methods for developing and implementing PCI compliant information security, network segmentation has emerged as a best practice for its significant impact in reducing cost and complexity of PCI compliance. Network segmentation isolates cardholder data to specific servers or areas of the network, narrowing the scope of the network subject to PCI DSS compliance. The resulting benefits are dramatic reduction in:

- PCI DSS assessment costs
- Costs of compliance implementation and maintenance
- Effort required to develop and apply security policies
- Risk to the organization, as a result of minimized exposure of cardholder data and ease of controlling the segment
- Forensic costs in the event that a security incident occurs, due to simplicity of locating and investigating traffic

The reduced cost and complexity of network segmentation results in a highly secured network at a fraction of the potential cost. Without network segmentation, the entire network is within scope of the PCI audit and at risk. The following diagram juxtaposes the non-segmented and segmented network:

Q18. WHAT IS PCI DSS? (Continued...)



On the left is a flat network, in where the entire network is subject to PCI audit. On the right, cardholder data is isolated in a security zone with authorized users being the only group who can access the data.

Network SegmentationAmong the methods for developing and implementing PCI compliant information security, network segmentation has emerged as a best practice for its significant impact in reducing cost and complexity of PCI compliance. Network segmentation isolates cardholder data to specific servers or areas of the network, narrowing the scope of the network subject to PCI DSS compliance. The resulting benefits are dramatic reduction in:

- PCI DSS assessment costs
- Costs of compliance implementation and maintenance
- Effort required to develop and apply security policies
- Risk to the organization, as a result of minimized exposure of cardholder data and ease of controlling the segment
- Forensic costs in the event that a security incident occurs, due to simplicity of locating and investigating traffic

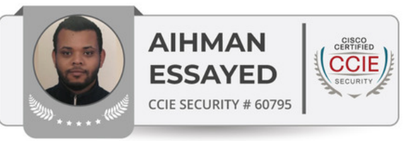
The reduced cost and complexity of network segmentation results in a highly secured network at a fraction of the potential cost. Without network segmentation, the entire network is within scope of the PCI audit and at risk. The following diagram juxtaposes the non-segmented and segmented network:

RECENT CCIE FROM I-MEDITA

AMIT KHARUDE
CCIE SECURITY # 61023

KISHAN PATEL
CCIE R&S #57009

SAGAR PARIKH
CCIE R&S #57008



AIHMAN ESSAYED
CCIE SECURITY # 60795

SUNIL KUMAR
CCIE SECURITY # 60728

S. PATHAK
CCIE SECURITY # 60434

DEEPTIRANJAN
CCIE SECURITY # 60711

PRAKASH
CCIE SECURITY # 60537

MOHIT SONI
CCIE SECURITY # 60793

HASEEB MUSTAFA ALVI
CCIE R&S #59325

HAMID
CCIE R&S # 38970

SANDEEP BISHT
CCIE R&S # 60219

ALI
CCIE R&S # 41838

MALAY
CCIE R&S # 55682

HIKMAT ULLAH
CCIE R&S # 54119

ASMAT ULLAH
CCIE R&S # 55710

SAMEER KOTAK
CCIE R&S # 54932

SUMIT SINGH
CCIE SECURITY # 61271

SAQIB
CCIE SECURITY #61087

SURENDRA SINGH
CCIE R&S #60346

RAVI DHRUV
CCIE R&S # 60014

I-MEDITA
Training | Development | Placement

HELPING STUDENTS BECOME CERTIFIED

Q19. WHAT IS A PAYLOAD-BASED SIGNATURE?

Security tools often utilize signatures based on easily changed variables like hash, file name or URLs to identify and prevent known malware from infecting systems. With this type of signature, identifying threats requires essentially a one-to-one match against the specific variables the signature is looking for.

While once an effective means for identifying malware, it is now a feeble practice, as attackers have adopted more sophisticated means of evading detection. Malware authors can now easily create thousands of variants of existing malware, containing only slight changes, in order to get around signature matching. As legacy signatures require a static one-to-one match for each unique file, these slight changes allow malware to go undetected.

As attackers have evolved, so have protections, and organizations should consider utilizing security protections that leverage payload-based signatures, which detect patterns in the actual content of the file rather than a simple attribute like hash. If a piece of known malware has been altered in any way, resulting in an entirely new hash or other small change, payload-based signatures would still be able to identify and block what would otherwise have been treated as a new unknown threat.

While payload-based signatures require more evidence and larger sets of data to produce, security teams ultimately have fewer signatures to author and deploy, as each signature is more effective at blocking variants and polymorphic malware and provides a wider net of protection. With payload-based signatures, one signature can block tens of thousands of variants from the same malware family. The result is a one-to-many malware detection, with significantly quicker and more successful prevention.

Q19. WHAT IS A PAYLOAD-BASED SIGNATURE? (Continued...)

he Palo Alto Networks Next-Generation Security Platform leverages the Threat Intelligence Cloud, including the detection of unknown threats via WildFire, as well as enforcement from the Threat Prevention subscription, to automatically distribute payload-based signatures across the organization. The platform can uniquely prevent multiple variants of malware, as well as command-and-control traffic, with the high fidelity of its proprietary, signature-based format.

Q20. WHAT ARE 4 WAYS IN WHICH CYBERSECURITY AUTOMATION SHOULD BE USED?

1. Correlating Data

Many security vendors collect substantial amounts of threat data. However, data provides little value unless it is organized into actionable next steps. To do this effectively, organizations first need to collect threat data across all attack vectors and from security technologies within their own infrastructure, as well as global threat intelligence outside of their infrastructure.

Then, they need to identify groups of threats that behave similarly within the massive amounts of data and use that to predict the attacker's next step. When using this approach, more data collected results in more accurate results, and reduces the likelihood that the groups identified merely an anomaly. Consequently, the analysis must also have enough computing power to scale today's threat volume—something that is impossible to do manually. Machine learning and automation allow data sequencing to happen faster, more effectively, and more accurate. Finally, combining this approach with dynamic threat analysis is the only way to accurately detect sophisticated and never-before-seen threats.

2. Generating Protections Faster Than Attacks Can Spread

Once a threat is identified, protections need to be created and distributed faster than an attack can spread throughout the organization's networks, endpoints, or cloud. Because of the time penalty that analysis adds, the best place to stop the newly discovered attack is not at the location where it was discovered but at the attack's predicted next step. Manually creating a full set of protections for the different security technologies and enforcement points capable of countering future behaviors is a lengthy process that not only moves slowly but also is extremely difficult when correlating different security vendors in your environment and not having the right control and resources. Automation can expedite the process of creating protections without straining resources, all while keeping pace with the attack.

Q20. WHAT ARE 4 WAYS IN WHICH CYBERSECURITY AUTOMATION SHOULD BE USED? (Continued...)

3. Implementing Protections Faster Than Attacks Can Progress

Once protections are created, they need to be implemented to prevent the attack from progressing further through its lifecycle. Protections should be enforced not only in the location the threat was identified, but also across all technologies within the organization to provide consistent protection against the attack's current and future behaviors. Utilizing automation in the distribution of protections is the only way to move faster than an automated and well-coordinated attack, and stop it. With automated, big data attack-sequencing and automated generation and distribution of protections, you are more accurately able to predict the next step of an unknown attack and move fast enough to prevent it.

4. Detecting Infections Already in Your Network

The moment a threat enters the network, a timer starts counting down until it becomes a breach. To stop an attack before data leaves the network, you have to move faster than the attack itself. In order to identify an infected host or suspicious behaviors, you must be able to analyze data from your environment backward and forward in time, looking for a combination of behaviors that indicate a host in your environment has been infected. Similar to analyzing unknown threats attempting to enter the network, manually correlating and analyzing data across your network, endpoints, and clouds is difficult to scale. Automation allows for faster analysis and, should a host on your network be compromised, faster detection and intervention.

Q21. WHAT IS MACHINE LEARNING?

Machine learning is when a program takes new data, learns from it and makes changes without being explicitly programmed to do so. Machines perform data sequencing in an automated fashion, combing through sets of data searching for patterns and similarities. Once data patterns and predictive behaviors have been identified, rules must be implemented to take action on learned data. With machine learning, the machine is enabled to create or modify rules to further improve itself and accomplish its primary objectives.

The objectives can vary and have a variety of uses. Machine learning can be used to make routes faster and more efficient for various transportation methods; improve sales conversions through product recommendations or tailoring product content to direct purchasing decision; predict hospitalization based on physical behavior and patient data; improve patient diagnostics based on trends or areas of concern; or determining levels of risk for investments or insurance.

In the times before machine learning, a user must manually provide the program with new sets of rules for any new data in order for any action to occur, as well as decide on what the next step would be to act upon any new rules. With machine learning, the program creates algorithms, or a sequence of instructions, to execute in order to accomplish a desired end result as well as recommend and act upon any suggested next steps. Rather than having to manually parse through copious amounts of data, correlate patterns, create algorithms and execute across systems, users, utilizing automation and machine learning, have been able to improve efficiencies by being more granular and prescriptive, as well as alleviate workload.

Q21. WHAT IS MACHINE LEARNING? (Continued...)

Conditions for Machine Learning

There are a few conditions necessary for machine learning to occur:

1. Data must be consolidated into one place so the machine may be able to access all relevant data necessary to make a decision.
2. The appropriate structure must be in place to analyze the large amounts of data to identify similarities and patterns. Combing through significant amounts of data sets requires powerful computational processing.
3. Basic set of rules must be provided to the machine to serve as a basic guideline, as well as provide the desired outcome.

The Fear of Machine Learning

The caveat with machine learning is the significant level of trust the user must place in the hands of the machine. There is a certain level of fear and trust associated when it comes to machine learning – a trust that the machine will take the appropriate actions, for instance putting their lives in the hands of the Tesla Autopilot or the Google self-driving vehicles – and a a fear machines might evolve into a technological singularity. Watching artificial intelligence takeover movies such as iRobot, Ex Machina, WarGames and Tron will demonstrate this to an extend.

It is important to note that machine learning helps predict behaviors and recognize patterns in a way that humans cannot due to their limited compute capacity. Machines are able to recognize patterns and act much faster than a human. They learn from previous and new conclusions to further develop and improve it's own algorithms. When massive data sets are present, it is impossible to create algorithms at scale. The only way to do this is to utilize machine to process data and learn from experience to improve upon itself. Additionally, although machine learning enables self-implied changes in order to accomplish a specific objective, the objective itself is always set by humans. With this, there must also be an implied trust in the goal set by the user.

Q21. WHAT IS MACHINE LEARNING? (Continued...)

Machine Learning in Cybersecurity

Specific to cybersecurity, it is difficult to keep pace with the constant volume and increasing sophistication of threats and attacks. Cyberattacks have evolved to be heavily automated – 68% of respondents in a recent Ponemon study1 agree that automated tools have made it easier for attackers to execute a successful attack. Our unique approach to cybersecurity incorporates automation and machine learning allows us to get ahead of attackers. Machine learning can help accurately identify variations of known threats, identify patterns, predict the next steps of an attack and automatically create and implement protections across the organization in near real-time. With machine learning, successful cyberattacks can be prevented.

To learn more about next-generation security platforms, visit the link below:
https://www.paloaltonetworks.com/products/designing-for-prevention/security-platform