

Oracle - oracle.com - phone: 650.506.7000,
500 Oracle Parkway, Redwood Shores, CA

Saurabh Verma - Vice President / Architect / Engineering Leader - saurabh.verma@oracle.com, phone: 737.867.1000, 2nd phone: 650.430.4410

Other emails: saurabh.verma@oracle.com, saurabh@oracle.com

LinkedIn: <https://www.linkedin.com/in/saurabhverma4>

Contact 2 Info: Darrin Luke - IT Business Implementation Analyst - Oracle Academy – darrin.luke@oracle.com, 0, 0

Contact 2 LinkedIn: <https://www.linkedin.com/in/darrinaluke>

Other emails: darrin.luke@oracle.com, darrin@oracle.com

Total annual spend for IT and cybersecurity development measures for your company: 10000000

Industry Sector: High Tech

What are key products or services offered by your company? cloud

How many people are employed by your company? 10,000+ employees

What is the current annual revenue for your organization? \$5B+

How many business locations do you maintain company hardware and equipment such as servers...? 60

How many people are in your IT Department? NO

How many people are on your IT security team? NO

Number of Contact Center Seats: NO

What is your current Operating System? NO

Who is your current ERP vendor? NO

Who is your Cloud Service Provider? Oracle

1) Do you have responsibility for Cybersecurity? yes

Do you plan to add or expand cybersecurity initiatives in the next 12 months? yes

Please specify which solutions you are interested in speaking to solution providers about with current and future projects in mind: , Application Security and WAF, API Security, Cloud Security, Critical Event Management Data Loss Protection, Data Center Security, Data Security, DevOps Security Encryption Fraud Prevention / Transaction Security, Identity Access Management, Multi-factor authentication, Zerotrust Managed Security Service Provider, Network Security - Firewall, Network Security - Intrusion Prevention Systems, Network Security - Monitoring forensics, Network Security - Unified Threat Management Penetration Testing and Simulation, Privileged Access Management, Ransomware, Risk Compliance SIEM, SOAR - Security Orchestration Automation and Response, Third Party Cyber Risk Management, Threat Intelligence

Please summarize your top Cybersecurity challenges you need assistance with in the next 3-6 months. Please be as descriptive as possible and provide context around your current needs. (this ensures a relevant schedule): cloud security

2) Do you have responsibility for Cloud software solutions? yes

Do you plan to add or expand cloud solution initiatives in the next 12 months? yes

Please specify which solutions you are interested in speaking to solution providers about with current and future projects in mind: , Business Intelligence, Cloud Migration Services Dev-Ops,

Please summarize your top Cloud Solutions challenges you need assistance with in the next 3-6 months. Please be as descriptive as possible and provide context around your current needs. (this ensures a relevant schedule): secure deletion or sanitization of digital media

1. data breaches -
2. data loss - loss of information, deletion, overwriting, corruption or integrity of data compromise
3. account or service traffic hijacking - methods such as phishing, more recently smishing (sms phishing), spear phishing (targeted phishing attacks), and exploitation of software and other application-related vulnerabilities. allows attackers to monitor and eavesdrop on communications, sniff and track traffic, capture relevant credentials, and access and alter account and user profile characteristics (changing passwords and more).
4. api security -
5. denial of service - prevent users from accessing services and resources from a specified system or location. this can be done using any number of attack vectors available but typically look to target buffers, memory, network bandwidth, or processor power.
6. malicious insiders - disgruntled employees, contractor, or partner
7. abusing cloud services for bad intent - eg execute dictionary attacks, dos attacks, crack encryption passwords, host illegal sw for distribution

3) Do you have responsibility for Digital Solutions?: yes

Do you plan to add or expand digital responsibility initiatives in the next 12 months?: NO

Please specify which solutions you are interested in speaking to solution providers about with current and future projects in mind: Digital Customer Experience Optimization, Digital Transformation, Digital Security Robotic Process Automation (RPA),

Please summarize your top Digital Solutions challenges you need assistance with in the next 3-6 months. Please be as descriptive as possible and provide context around your current needs. (this ensures a relevant schedule): 1. data breaches -

2. data loss - loss of information, deletion, overwriting, corruption or integrity of data compromise
3. account or service traffic hijacking - methods such as phishing, more recently smishing (sms phishing), spear phishing (targeted phishing attacks), and exploitation of software and other application-related vulnerabilities. allows attackers to monitor and eavesdrop on communications, sniff and track traffic, capture relevant credentials, and access and alter account and user profile characteristics (changing passwords and more).
4. api security -
5. denial of service - prevent users from accessing services and resources from a specified system or location. this can be done using any number of attack vectors available but typically look to target buffers, memory, network bandwidth, or processor power.
6. malicious insiders - disgruntled employees, contractor, or partner
7. abusing cloud services for bad intent - eg execute dictionary attacks, dos attacks, crack encryption passwords, host illegal sw for distribution

4) Do you have responsibility for Data Management? yes

Do you plan to add or expand data management initiatives in the next 12 months? NO

Please specify which solutions you are interested in speaking to solution providers about with current and future projects in mind: , BI Dashboard Reporting, Big Data Analytics, Business Intelligence, Business Process Management Data Cleansing, Data Governance MDM, Data Visualization, Data Warehousing Hyper-converged Infrastructure (HCI),

Please summarize your top Data Management challenges you need assistance with in the next 3-6 months. Please be as descriptive as possible and provide context around your current needs. (this ensures a relevant schedule): 1. data

breaches -

2. data loss - loss of information, deletion, overwriting, corruption or integrity of data compromise
3. account or service traffic hijacking - methods such as phishing, more recently smishing (sms phishing), spear phishing (targeted phishing attacks), and exploitation of software and other application-related vulnerabilities. allows attackers to monitor and eavesdrop on communications, sniff and track traffic, capture relevant credentials, and access and alter account and user profile characteristics (changing passwords and more).
4. api security -
5. denial of service - prevent users from accessing services and resources from a specified system or location. this can be done using any number of attack vectors available but typically look to target buffers, memory, network bandwidth, or processor power.
6. malicious insiders - disgruntled employees, contractor, or partner
7. abusing cloud services for bad intent - eg execute dictionary attacks, dos attacks, crack encryption passwords, host illegal sw for distribution

5) Do you have responsibility for Software/Application Development and Management? no

Do you plan to add or expand software / application development initiatives in the next 12 months? NO

Please specify which solutions you are interested in speaking to solution providers about with current and future projects in mind: ,

Please summarize your top Software/ Application Development challenges you need assistance with in the next 3-6 months. Please be as descriptive as possible and provide context around your current needs. (this ensures a relevant schedule): no

6) Do you have responsibility for Communication Systems? no

Do you plan to add or expand communication system initiatives in the next 12 months? NO

Please specify which solutions you are interested in speaking to solution providers about with current and future projects in mind: ,

Please summarize your top Communication Systems challenges you need assistance with in the next 3-6 months. Please be as descriptive as possible and provide context around your current needs. (this ensures a relevant schedule): no

7) Do you have responsibility for Network Systems? no

Do you plan to add or expand network system initiatives in the next 12 months? NO

Please specify which solutions you are interested in speaking to solution providers about with current and future projects in mind: ,

Please summarize your top Network Systems challenges you need assistance with in the next 3-6 months. Please be as descriptive as possible and provide context around your current needs. (this ensures a relevant schedule): no

8) Do you have responsibility for Consulting / Outsourcing? no

Do you plan to add or expand consulting / outsourcing initiatives in the next 12 months? NO

Please specify which solutions you are interested in speaking to solution providers about with current and future projects in mind: ,

Please summarize your top Consulting/Outsourcing challenges you need assistance with in the next 3-6 months. Please be as descriptive as possible and provide context around your current needs. (this ensures a relevant schedule): no

9) Do you have responsibility for IT Leadership, Talent Management and Training? yes

Do you plan to add or expand IT leadership, talent management, and training initiatives in the next 12 months? yes

Please specify which solutions you are interested in speaking to solution providers about with current and future projects in mind: , IT Training Software for staff : Cybersecurity,

Please summarize your top IT Leadership, Talent Management and Training challenges you need assistance with in the next 3-6 months. Please be as descriptive as possible and provide context around your current needs. (this ensures a relevant schedule):

1. data breaches -
 2. data loss - loss of information, deletion, overwriting, corruption or integrity of data compromise
 3. account or service traffic hijacking - methods such as phishing, more recently smishing (sms phishing), spear phishing (targeted phishing attacks), and exploitation of software and other application-related vulnerabilities. allows attackers to monitor and eavesdrop on communications, sniff and track traffic, capture relevant credentials, and access and alter account and user profile characteristics (changing passwords and more).
 4. api security -
 5. denial of service - prevent users from accessing services and resources from a specified system or location. this can be done using any number of attack vectors available but typically look to target buffers, memory, network bandwidth, or processor power.
 6. malicious insiders - disgruntled employees, contractor, or partner
 7. abusing cloud services for bad intent - eg execute dictionary attacks, dos attacks, crack encryption passwords, host illegal sw for distribution
-

