| מושגים עיקריים למועמד לתפקידי תקשורת אבטחת מידע | |
|---|---|
| **יצרניות מובילות בשוק** | |
| **Fortinet** | |
| **Checkpoint** | |
| **Radware** | |
| **F5** | |
| **Juniper** | |
| **HPE** | |
| **Cisco** | |
| **arista** | |
| **Palo alto** | |
| **vmware** | |
| **imperva** | |
| **הסמכות רלוונטיות בתחום** | |
| **CCNA** | הסמכה ראשונית של חברת סיסקו במסלול נטוורקינג .חשוב מאוד להצטייד בה |
| **CCNP** | הסמכה שנייה של חברת סיסקו במסלול נטוורקינג .טוב שיש אותה . |
| **CCIE** | הסמכה שלישית של חברת סיסקו .מבחן בחול .ידועה כהסמכה מאוד קשה ולוקחת למידה של שנה . |
| **CCSA** | הסמכה ראשונית של חברת צקפוניט .טוב להיות איתה |
| **CCSE** | הסמכה שנייה של חברת צקפוניט .טוב להיות איתה |
| **CCSM** | הסמכה שלישית של חברת צקפוינט . לא חובה להיות איתה. |
| **NSE 1-8** | הסמכות של חברת פורטינט . לא חובה להיות איתם . |
| **CISSP** | הסמכה יותר מכוונת לצוותי הנחיה של אבטחת מידע ותפקידי ניהול בכירים יותר .שם מאוד טוב בשוק .הסמכה לא פשוטה. |
| **PCNSE** | הסמכות של חברת פאלו אלטו .לא חובה |
| **AWS** | הסמכות על ענן של Aws של חברת אמאזון .השוק הולך לשם . |
| **azure** | הסמכות על ענן של AZURE של חברת מייקרוסופט .השוק הולך לשם . |
| **תפקידים רלוונטים לתחום הסייבר תקשורת והאבטחת מידע** | |
| **Noc** | |
| **Soc** | |
| **אנליסט SOC /IR** | |
| **מהנדס תקשורת/Network enginner** | |
| **מיישם אבטחת מידע** | |
| **מייישם תקשורת ואבטחת מידע** | |
| **הגנה והנחיה באבטחת מידע** | |
| **CISO** | |
| **ציודים שחייבים להכיר לפני ריאיון עבודה** | |
| **Firewall** | רכיב מרכזי בעבודה של מיישם תקשורת ואבטחת מידע .גורם מקשר ומגן על כלל הרשתות בארגון .עם יכולות של VPN ועוד המון פיצרים נוספים .לדוגמא פיירוואלים של פורטינט,צקפוינט,פאלו .... |
| **waf** | רכיב מרכזי בעבודה של מיישם תקשורת ואבטחת מידע .מגן על האפליקציות בארגון מפני התקפות בLAYERS גבוהה .כמו SQL INJECTION. יצרניות : אימפרבה , F5 |
| **Load balancer** | מחלק עומסים בין שרתים על מנת למנוע עומס על שרת מסויים לאפליקציות .יצרניות:f5, radware |
| **NAC** | מוצר אבטחתי לחסימת כניסה של פורצים או אנשים לא מורשים להתחבר דרך המתגים של הארגון .יצרניות: cisco portnox |
| **Mail relay** | מוצר אבטחתי להגנה על המיילים בארגון .יוצאים ונכנסים.יצרניות: cisco forcepoint |

| | |
|---|---|
| **Proxy** | מוצר אבטחתי לאינספקשן של תעבורה שיוצאת לאינטרנט .יצרניות : forcepoint broadcom |
| **DDOS** | מוצר הגנתי נגד תקיפות בסקייל גבוה על הרשת .יצרניות: radware arbor |
| **Micro segmentation** | מוצר הגנתי למניעת תקשורת בין מחשבים שהם באותו סיגמנט תקשורתי .יצרניות:vmware nsx cisco |
| **Switch** | כמו מפצל חשמלי .אך רק לחיבור למחשבים .בתוכו נגדיר וילאנים .והוא ירכז לנו חיבורים של הקומות בארגון .יצרניות: cisco juniper |
| **Router** | מוצר מרכזי בארגונים שאחראי על יציאה וכניסה לאינטרנט או ניהול תקשורת בין סיגמנטים בארגון .עם עוד המון פיצ'רים נוספים .יצרניות: cisco juniper |
| **GBIC** | משמש לחיבור לראוטרים סוויטצים ופירוואלים .מתאם את אותות הרשת בין ההתקן לבין הכבל שבו אנחנו משתמשים .יכול לנוע בכל מיני מהירויות |
| **Sdwan** | מסייע לחיבור סניפים של ארגון לרשת אחת כוללת .דברים מבוצעים באופן אוטומאטי .יצרניות: hpe aruba cisco |
| **Access point** | רכיב שפרוס בכל רחבי החברה על מנת להעניק WIFI לטווח הקרוב אליו .יצרניות: juniper cisco |
| **EDR** | מנטר ומזהה התקפות על שרתים מחשבים ומכשירים ניידים ולשפר את ההגנה מפני malware, הקתפות ZERO DAY .יצרניות : palo alto sentinel one |
| **XDR** | בעצם הרחבה של איסור האיום מהEDR .מעקב אחרי פעילות חשודה באימייל,בענן ,ביישומים.יצרניות:crowdstrike palo alto |
| **Vpn gateway** | רכיב מרכזי שמשמש חיבור משתמשים בחיבור מאובטח לארגון מרחוק .יצרניות cisco .ivanti |
| **<u>מושגים שצריך להכיר לפני ריאיון עבודה</u>** | |
| **מודל 7 השכבות** | חשוב מאוד לדעת בעל פה.המודל הבסיסי של עולם התקשורת ממה בנויה כל שכבה . |
| **כתובת IP** | כתובת ייחודית שמוקצית לכל רכיב ורכיב ברשת x.x.x.x .חשוב מאוד להכיר סאבנטינג ו default gateway . |
| **LAN** | Local area network .בעצם הרשת הפנימית של ארגון או משתמש ביתי .כביכול סומך עליה .היא לא מנותבת באינרטנט .אלא אם פתחתי גישה לאחד מן הרכיבים.מאופיינת בכתובות פנימיות . |
| **WAN** | Wide area network מחברת בין רשתות וארגונים באינטרנט הגדול .מתאפיינת בכתובות חיצוניות . |
| **TCP** | פרוטוקול להעברת נתונים בצורה בטוחה.פחות מהירות |
| **UDP** | פרוטוקול להעברת נתונים ללא אישור של המקבל בצד השני .לצורך העברה מהירה יותר . |
| **Spanning tree** | פרוטוקול להגנה מפני לופים ברשת |
| **DHCP** | פרוטוקול האחראי על חלוקת הכתובות IP ברשת |
| **DNS** | פרוטוקול המתרגם שמות לIP .זאת אומרת אם יש לי כתובת IP ואני לא זוכר אותה אני לא אכנס אליה ישירות אלא אכנס אליה בשם כמו שנכנסים לדוגמא לYNET |
| **VLAN** | מאפשר לי להפריד רשתות בתוך הארגון שלי בתוך אותה רשת פיזית .לדוגמא הפרדה בין הרשת של המכירות למערכות מידע |
| **HTTP** | פרוטוקול להעברת מידע .לא מוצפן לא מאובטח .בדרך כלל נשתמש בHTTPS |
| **HTTPS** | פרוקטול מאובטח להעברת נתונים .תוקף לא יכול לדעת מה עובר בתווך אלא אם יש לו תעודה |
| **SMTP** | משמש לתקשורת והעברת הודעות דואר אלקטרוני . |

| | |
|---|---|
| **FTP** | שרת אחסון קבצים |
| **SFTP** | שרת אחסון קבצים עם הצפנה |
| **Ping** | כלי המאפשר לי לבדוק קישוריות בין מקום למקום ברשת וטווח זמנים |
| **traceroute** | כלי המאפשר לי לקבל טווח זמנים עד הגעה ליעד ומפרט לי את היעדים של הפאקטה שעוברת בדרך |
| **Site 2 site** | העברת נתונים בין 2 מקומות בצורה מאובטחת |
| **Bgp** | פרוטוקול ניתוב שמעביר מידע בין AS שונים.מחולק לחיצוני ופנימי . ebgp ibgp |
| **Ospf** | פרוטקול ניתוב דינאמי המאפשר העברת מידע בתוך הארגון |
| **Vpc** | טכנולוגיה המאפשרת לי במתגי נקסוס להפוך 2 מתגים ליישות אחת .כך שבמקרה של כשל באחד מהם החיבור השני ימשיך לתפקד . |
| **hsrp** | פרוטוקול של סיסקו המאפשר יצירת גיבוי בין נתבים שונים ואפילו בין וילאנים שונים על אותו נתב . |
| **Port channel** | יצירת בונדינג בין 2 ממשקים על מתג או רכיב פיירואל אחד לדוגמא המאפשר לי לקבל מהירויות יותר גבוהות ושרידות |
| **NAT** | המרה כתובות IP לכתובת אחת או כמה .בדרך כלל נראה את זה ביציאה שלנו מחוץ לארגון .זאת אומרת לא נגלוש עם הכתובת הפנימית אלא כתובת חוקית שהוקצתה מהספק שלנו |
| **ACL** | מנגנון בנתב/מתג של סיסקו לדוגמא שמאפשר לנו הרשאה של מי יכול לגשת לאן ממש ברמת המחשב או רמת הרשת .דומה לפריוואל . |
| **Stateless firewall** | מתייחסת לחוקים שהוגדרו מראש בלבד .מנתר קונקשנים שנמצאים כרגע ולא מבין את מהלך הרשת אלא רק מה שהוגדר.זאת אומרת חוקים יצטרכו להיות מוגדרים רק לבקשה וגם לריספנונס |
| **Statefull firewall** | מבין מהו הקונקשן ומאפשר חוק אחד גם לבקשה וגם לריספונס |
| **radius** | פרוקטול לזיהוי משתמשים AAA .כלי המאפשר לי חיבור לרשתות כמו VPN WIFI |
| **802.1x** | פרוטקול לאימות גישה של משתמשים לרשת .מאפשר גם אבטחתיות חזקה עם תעודות . |
| **DLP** | טכנולוגיה המאפשרת להגן על נתנוים רגישים כמו הגנה על הוצאות חומר רגיש דרך האימייל או דרך העלאה לאינרטנט |
| **<u>מספרי פרוטוקול שרצוי מאוד לדעת</u>** | |
| **ftp-data** | 20 |
| **FTP** | 21 |
| **ssh** | 22 |
| **telnet** | 23 |
| **smtp** | 25 |
| **dns** | 53 |
| **http** | 80 |
| **https** | 443 |
| **Pop 3** | 110 |
| **ldap** | 389 |
| **Ldap over tls** | 636 |
| **rdp** | 3389 |
| **tacacs** | 49 |
| **ntp** | 123 |
| **syslog** | 514 |

| | |
|---|---|
| 161 | **snmp** |
| 162 | **Snmp trap** |
| 5060 | **sip** |