סייבר ישראל
מערך הסייבר הלאומי

עקרונות מנחים
רכש מערך SIEM

יובל סיני

02.10.2019
גרסה 1.0

הרצאה ללא מכשירים ניידים ושות'

המידע במצגת הינו בלמ"ס – רגיש (לא להפצה) - ומבוסס על מקורות גלויים, אך הדיון עשוי להתפתח לכיוונים שונים

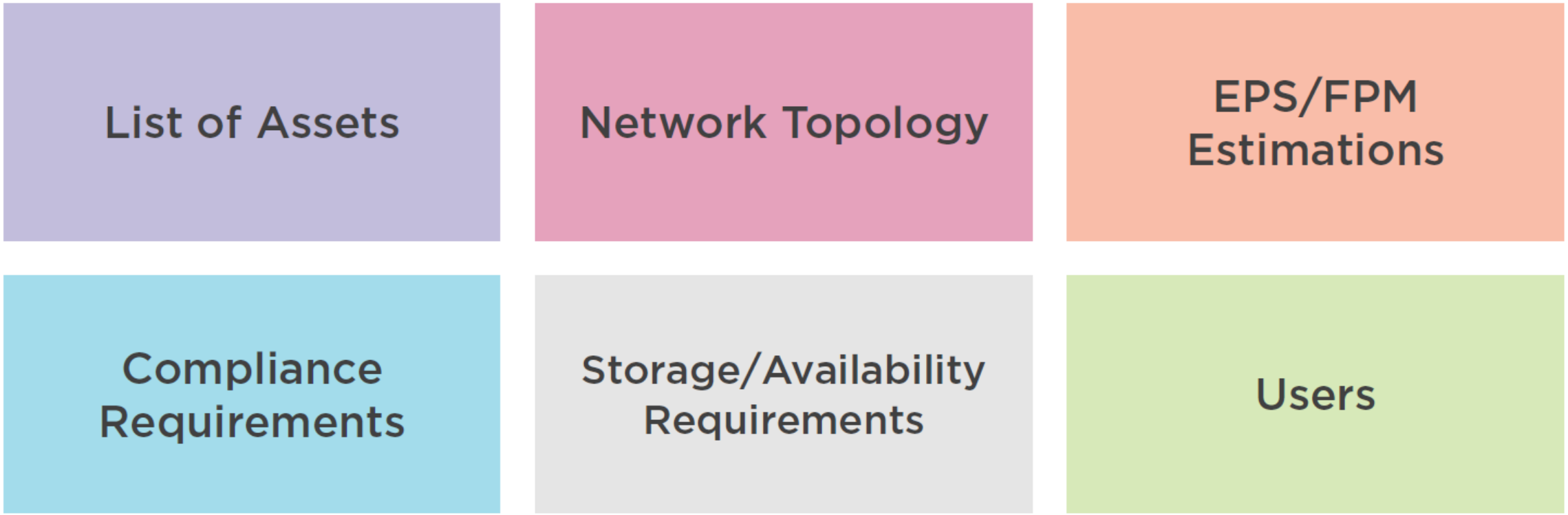
אג'נדה

- ✓ מבוא
- ✓ מיפוי סביבת ההפעלה
- ✓ Events Vs Flows
- ✓ הערכת EPS (Event Per Second)
- ✓ הערכת FPS (Flows Per Second)
- ✓ אורך חיי הלוגים
- ✓ מודולים נלווים (בד"כ מחייבים רישוי ייעודי)
- ✓ UBA Risk Score – דוגמא להמחשה
- ✓ Vulnerability Management
- ✓ ארכיטקטורה לדוגמא ליישום Qradar
- ✓ הון אנושי

מבוא

- ✓ מערך הניטור מהווה בעיקרו בקרה מפצה (Composite Control)
- ✓ מערכת ה-SIEM מהווה עבור ארגונים רבים את ליבת מערך הניטור
- ✓ רכש מערך ה-SIEM הינו תהליך מאתגר
- ✓ הניסיון מלמד כי מרבית הלקוחות רוכשים מערך SIEM שאינו מספק מענה אפקטיבי
- ✓ עולם ה-SIEM עבר בשנים האחרונות שינויים מהותיים, כאשר הפתרונות המתקדמים יותר זמינים בתצורת בענן בלבד

מיפוי סביבת ההפעלה



פרופיל איומים (Threat Profile)

Events Vs Flows

Events	Flows
- Login failures - Unusual successful logins - New processes/services - File creation/deletion - Access to critical files - Resource-intensive processes	- Connections to suspicious IPs - New open ports/services - Large file transfers - Port scans

הערכת EPS (Event Per Second)

Determining the EPS without access to logs or the system:
From my previous experience, a good approximation of EPS is:

Device Type	EPS
Active Directory	15
IIS or Exchange	10
General Windows Server	2
General Windows Workstation	0.5
UNIX/Linux Server	0.5
DNS or DHCP	15
AntiVirus Server	20
Database	1
Proxy	25
Core/Border Firewall	150
Small Firewall	20
IPS, IDS or DAM	5
VPN	5
Routers/Switches	0.25

Calculating the EPS of the whole environment:
Multiply the number of each device by the estimated EPS
Sum the EPS of all kind of devices and you will have the EPS of your whole environment
– *Example:*
*3 Core Routers * 2 IPS - 3x 150 * 2x 5 - 460 EPS*
#Remember to always consider at least 20% margin for buying your license.

ככלל אצבע, מומלץ להתחיל ב-
20,000 EPS ולכלול תמיכה מובנית
בגדילה טבעית של 30% לפחות

הערכת EPS (Event Per Second) - המשך

Log Source Type	Quantity	Estimated EPS	Total
Internal Windows Servers	74	0.7	52
External Windows Servers	6	2	12
Database Log Sources	5	3	15
Core Firewalls	2	150	300
Border Firewalls	2	130	260
Internal Linux Servers	24	0.5	12
Proxy	1	25	25
EPS TOTAL:	ככלל אצבע, מומלץ להתחיל ב- 20,000 EPS ולאפשר גדילה של 30% לפחות		676
Safety Margin (+30%):			880

הערכת EPS (Event Per Second) - המשך

- ✓ מומלץ לוודא כי מקורות הלוגים (Log Providers), דוגמת מערכת הפעלה או מתג תקשורת, מפיקים לוגים ברמת פירוט גבוהה (דוגמת Syslog Severity Level 5 ומעלה)
- ✓ מומלץ להעביר את כל ה-RAW Logs למערך ה-SIEM ישירות וללא שיהוי מיותר, ולא להסתמך אך ורק על קבלת התרעות ספציפיות ממוצרי ההגנה

Severity Level	Level Name	Description
0	Emergencies	System unusable
1	Alerts	Immediate action needed
2	Critical	Critical conditions
3	Errors	Error conditions
4	Warnings	Warning conditions
5	Notifications	Normal but significant conditions
6	Informational	Informational messages only
7	Debugging	Debugging messages

Source:Implementing Cisco Networking Solutions, Harpreet Singh, Packt Publishing, September, 2017
https://www.oreilly.com/library/view/implementing-cisco-networking/9781787121782/683e1bb5-ce1b-470c-9411-ea1a170cc21e.xhtml/system/message/guide/sysmsgd/config.html

הערכת FPS (Flows Per Second)

ככלל אצבע, מומלץ להתחיל ב- 1,200 FPS ולכלול תמיכה מובנית בגדילה טבעית של 30% לפחות

	Non-Peak Time Measurement	Peak Time (Extrapolated)
Traffic (Gb/s)	5.5 Gb/s	9.5 Gb/s
Flows per second (FPS)	1,100 FPS	1,900 FPS

flows per second
Source: https://kb.kentik.com/Fcmth.06

בלמ"ס – רגיש (לא להפצה)

אורך חיי הלוגים

תקנות הגנת הפרטיות (אבטחת מידע), תשע"ז-2017

השפעה מהותית על שטח האחסון

מומלץ להוסיף 30% לטובת גדילה טבעית

בקרה ותיעוד גישה

10. (א) **במערכות של מאגר מידע אשר חלה עליו רמת האבטחה הבינונית או הגבוהה**, ינוהל מנגנון תיעוד אוטומטי שיאפשר ביקורת על הגישה למערכות המאגר (בתקנה זו – מנגנון הבקרה), ובכלל זה נתונים אלה: זהות המשתמש, התאריך והשעה של ניסיון הגישה, רכיב המערכת שאליו בוצע ניסיון הגישה, סוג הגישה, היקפה, ואם הגישה אושרה או נדחתה.

(ב) מנגנון הבקרה לא יאפשר, ככל יכולתו, ביטול או שינוי של הפעלתו; מנגנון הבקרה יאתר שינויים או ביטולים בהפעלתו ויפיץ התראות לאחראים.

(ג) בעל מאגר מידע יקבע נוהל בדיקה שגרתי של נתוני התיעוד של מנגנון הבקרה, ויערוך דוח של הבעיות שהתגלו וצעדים שננקטו בעקבותיהן.

(ד) נתוני התיעוד של מנגנון הבקרה יישמרו למשך 24 חודשים לפחות.

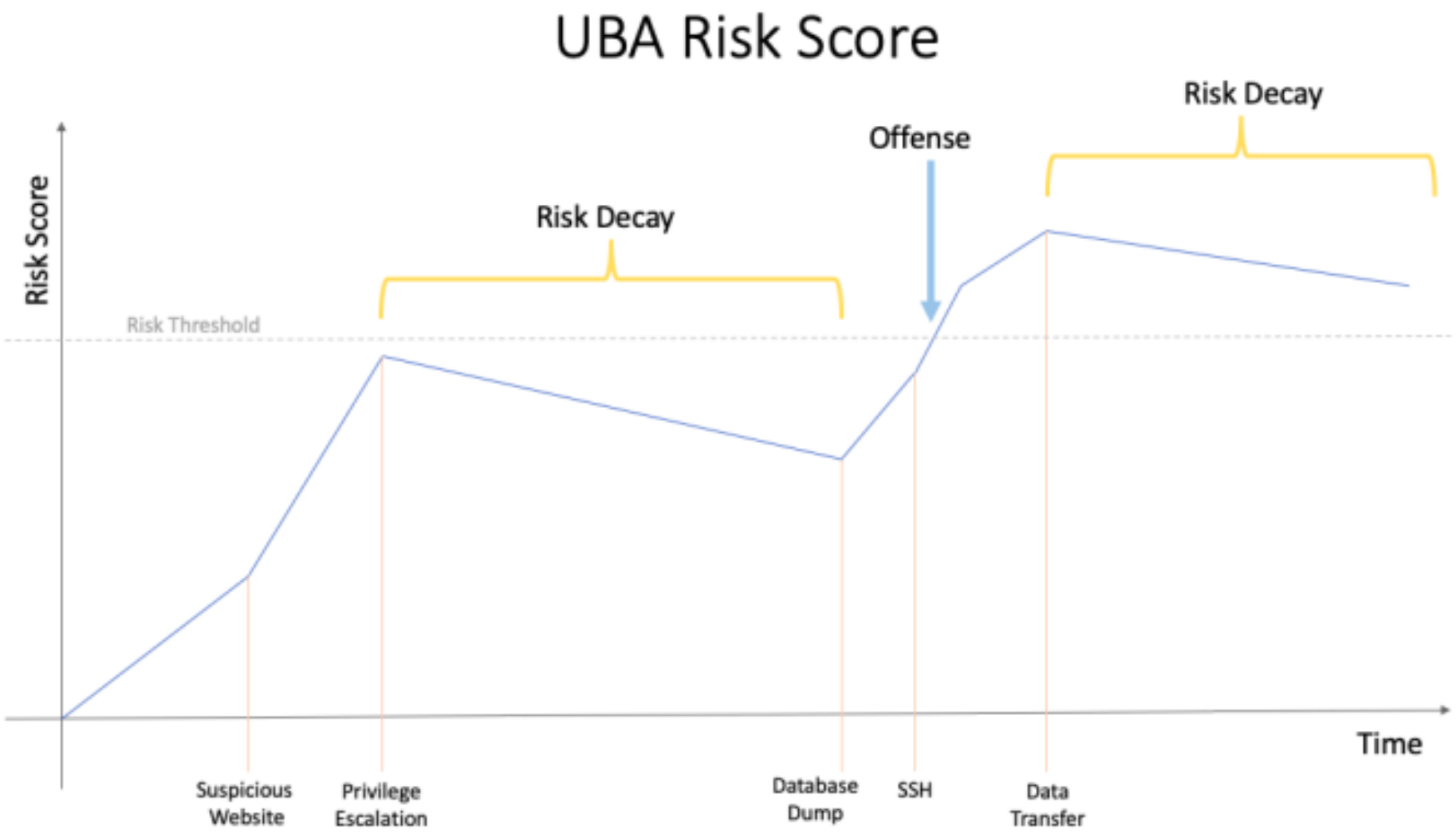
(ה) בעל מאגר מידע יידע את בעלי ההרשאות במאגר בדבר קיום מנגנון הבקרה למערכות המאגר.

flows per second
Source: https://kb.kentik.com/Fcmth.06

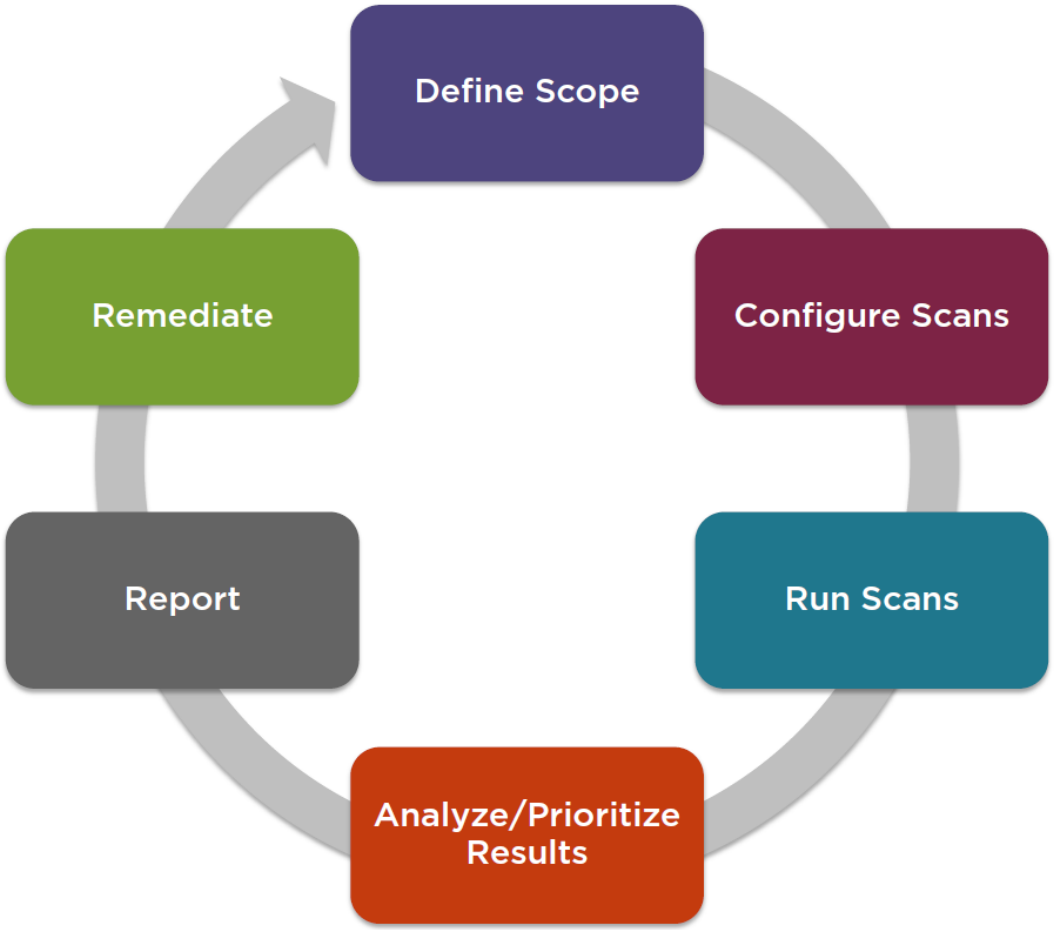
מודולים נלווים (בד"כ מחייבים רישוי ייעודי)

- ✓ **UEBA (User & Entity Behavior Analysis)** - זיהוי אנומליה בפעילות משתמשים וישויות ברשת
- ✓ **Risk Scoring** – קביעת מדרג סיכון לנכס סייבר ברשת הארגון (לרבות משתמשים וישויות)
- ✓ **Vulnerability Management** – זיהוי חולשות (דוגמת העדר הקשחה) ועדכוני אבטחה אשר לא הוטמעו
- ✓ **Incident Investigation** – ניהול חקירה פורזנית או צייד באופן ממוכן (Machine Learnning) ורוחבי בארגון
- ✓ **CTI (Cyber Threat Investigation)** – היתוך מודיעין סייבר לשם קורלציה מתקדמת מול IOCs (לרבות IP, Hash, URL, File Name)
- ✓ **תמיכה ב-MITRE ATT&CK** – בניית Kill Chain פרטני
- ✓ **SOAR (Security Orchestration, Automation and Response)** – יכולות תגובה אקטיבית לפי Playbook מוגדר
- ✓ מודולים נוספים עשויים להיות מוצעים ע"י היצרן ושותפים עסקיים שונים

בלמ"ס – רגיש (לא להפצה)



I - Vulnerability Management



II - Vulnerability Management

Discovery Scan	Patch Scan	Database Scan
Web Scan	PCI Scan	Full Scan

III - Vulnerability Management

Unauthenticated Scans

"Black Box Testing"

Scan the server from an external point of view

Identify and assess externally-available services

Depending on the policy, may miss open services

Authenticated Scans

"White Box Testing"

Use system credentials to scan from an internal point of view.

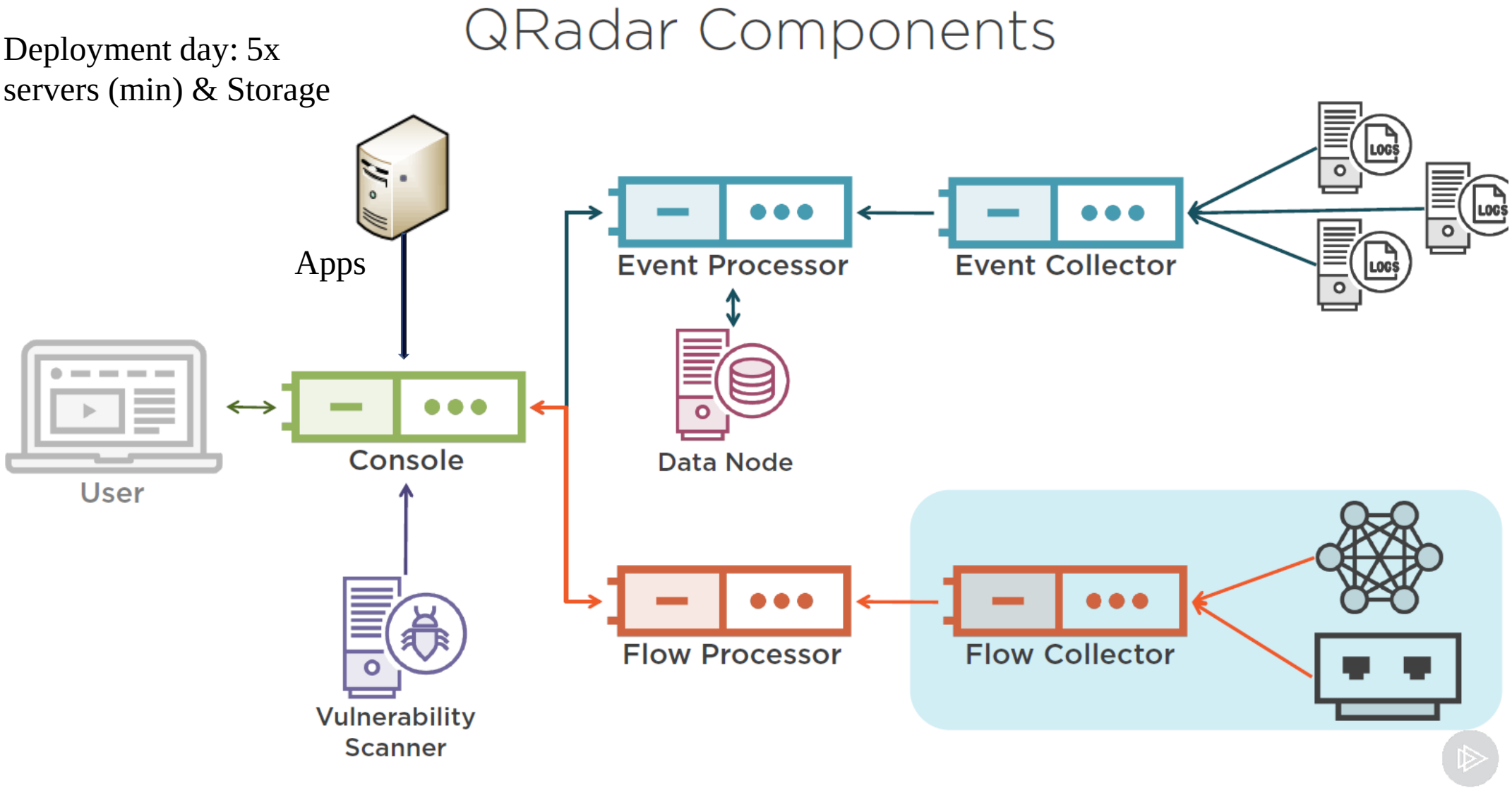
Check installed products and software versions

Detect internal and external vulnerabilities

Provides more accurate results

Faster scans

Deployment day: 5x servers (min) & Storage



הון אנושי

הכרת תהליכים עסקיים

- ✓ יצרני SIEM רבים מציעים הסמכות מקצועיות מטעמם
- ✓ ישנם הסמכות גנריות בעולם ה-SIEM מטעם ארגוני אבטחת מידע, דוגמת CompTIA
- ✓ תחלופת כוח האדם בתחום גבוהה יחסית עקב התפיסה כי המשרות הינן "סטודנטיאליות", ה"עבודה במשמרות" והשכר בד"כ נמוך
- ✓ המוטיבציה של ארגונים (וספקי שירות) לספק הכשרה מקצועית נאותה לעובדים מטעמם נמוכה יחסית
- ✓ עם זאת, ללא הון אנושי טוב האפקטיביות של מערך ה-SIEM תהיה נמוכה

סיכום

- ✓ תכנון נכון של מערך ה-SIEM עשוי לעלות באופן משמעותי את הסבירות כי מערך הניטור יגלה ויזהה את קיומו של אירוע סייבר לפני שיגרום נזק מהותי לארגון
- ✓ שלב היציאה למכרז מהווה את נקודת ההתערבות האופטימלית מצד גורמי ההנחיה
- ✓ רכישת מערך SIEM ללא מודולים מתקדמים משולה בד"כ להתקנת פתרון קוד פתוח לניהול לוגים וקורלציה
- ✓ גם אם הארגון מציג את קיומן של מגבלות משאבים קיימות, מומלץ לכלול במכרז כאופציה "חבילות עבודה"/מודולים נוספים, כאשר בעתיד ניתן יהיה לבצע הטמעה ללא צורך ביציאה במכרז פומבי נוסף
- ✓ POC (הכולל מדדי הצלחה מוגדרים) הינו שלב מהותי בבחינת תאימות מערך ה-SIEM לארגון, ומומלץ לוודא כי הוא חלק מתנאי המכרז
- ✓ ההון האנושי מהווה אבן ליבה בהצלחת מערך הניטור, ומומלץ לוודא כי רמת הכשירות והמוטיבציה שלו עונה לצורכי הארגון

תודה רבה