סוגי התקפות התראות ב Archsight

password guessing – ניחוש סיסמאות, בדר"כ למשתמש root. מתבצע על ידי סקריפט שמבצע brute force

port scanning – סריקת פורטים פתוחים במטרה למצוא פרצה ודרך להיכנס לארגון/לשרת.

Apache shutdown – מטרת התקיפה לבצע חבלה בפורט 80 (HTTP) או 440 (HTTPS)

Web Defacement - שינוי עמוד הבית של אתר אינטרנט

DNS Amplification – ריבוי בקשות משרת DNS תוך כדי זיוף כתובת IP במטרה להעמיס על אותה כתובת IP מזוייפת.

DNS Poisoning – שינוי כתובת בטבלת ה DNS לקישור אחר במטרה למשוך אליו אנשים.
דוגמה: אם כתובת 8.8.8.8 שייכת לגוגל, התוקף משייך את 8.8.8.8 לאתר אחר ומבקש שם להוריד קובץ זדוני על מנת להיכנס לגוגל המקורי.

Trojan Killer – ביצוע מתקפה על ריבוי מחשבים על ידי מחשב אחד. קובץ זדוני שהתחיל ממחשב אחד נשלח אוטומטית למחשבים אחרים וכל מי שפותח את הקובץ נתקף. המידע נשלח בדר"כ על ידי המחשב הנפרץ.

Ping Sweep – שליחת פינג לכל המחשבים בארגון על ידי סקריפט ובדיקה איזה מחשבים מחזירים תשובה (פונג) על מנת לתקוף אותם.

suspicious email activity- חשד לפעילות מיילים (קלבה / שליחה) לא רצויה בארגון.

כללי:

קובץ Autorun – קובץ שמכיל בתוכו סקריפט, מיועד להפעלה אוטומטית בעת הכנסת התקן חיצוני.