1. Amaç

Bu dokümanın amacı, Kurum bünyesinde meydana gelebilecek siber olaylara karşı etkili, hızlı ve koordineli bir müdahale sürecini iş akış diyagramı ile birlikte tanımlamaktır. Bu doküman, "KTÜN Siber Olay Yönetim Politikası" kapsamında hazırlanmış olup, siber olaylara müdahale sürecinin daha iyi anlaşılmasını sağlamayı hedeflemektedir. Kapsam, Dayanak, Tanımlar, Yaptırım, Yürürlük, Yürütme, Sorumluluklar gibi temel hususlar için ilgili politikaya başvurulması gerekmektedir.

2. Tanımlar

2.1. **Kurum:** Konya Teknik Üniversitesi

2.2. **Smoke Screen**(Duman Perdesi) **Saldırısı:** Saldırganların esas saldırıyı gizlemek için dikkat dağıtıcı başka saldırılar gerçekleştirdiği bir tekniktir. Amaç, güvenlik ekiplerinin veya savunma sistemlerinin asıl tehdide odaklanmalarını engelleyerek saldırıyı başarıyla gerçekleştirmektir.

3. Uygulama

3.1. **Riskler:** Yetkili personele ulaşılamaması, acil alınması gereken kararların hızlıca alınmaması, yeterli bilinçlenmenin sağlanamaması.

3.2. **Fırsatlar:** Siber olayların minimum zararla atlatılması. Her olaydan yeni dersler çıkarılarak daha ideal bir yapının sağlanması.

3.3. **Süreç Girdileri (Belgeler):**Siber olay bildirimleri, pentest sonuçları, güvenlik analizleri, log izleme sistemleri.

3.4. **Süreç Sorumlusu:** SOME Yöneticisi (Bilgi İşlem Daire Başkanı).

3.5. **Süreç Çıktıları:** Siber Olay Bildirimi.

3.6. **Süreç Ölçme Kriterleri:**

3.6.1. Siber olay karşısında sistemlerin en az zararla ve en kısa sürede saldırıya kapalı hale getirilmesi.

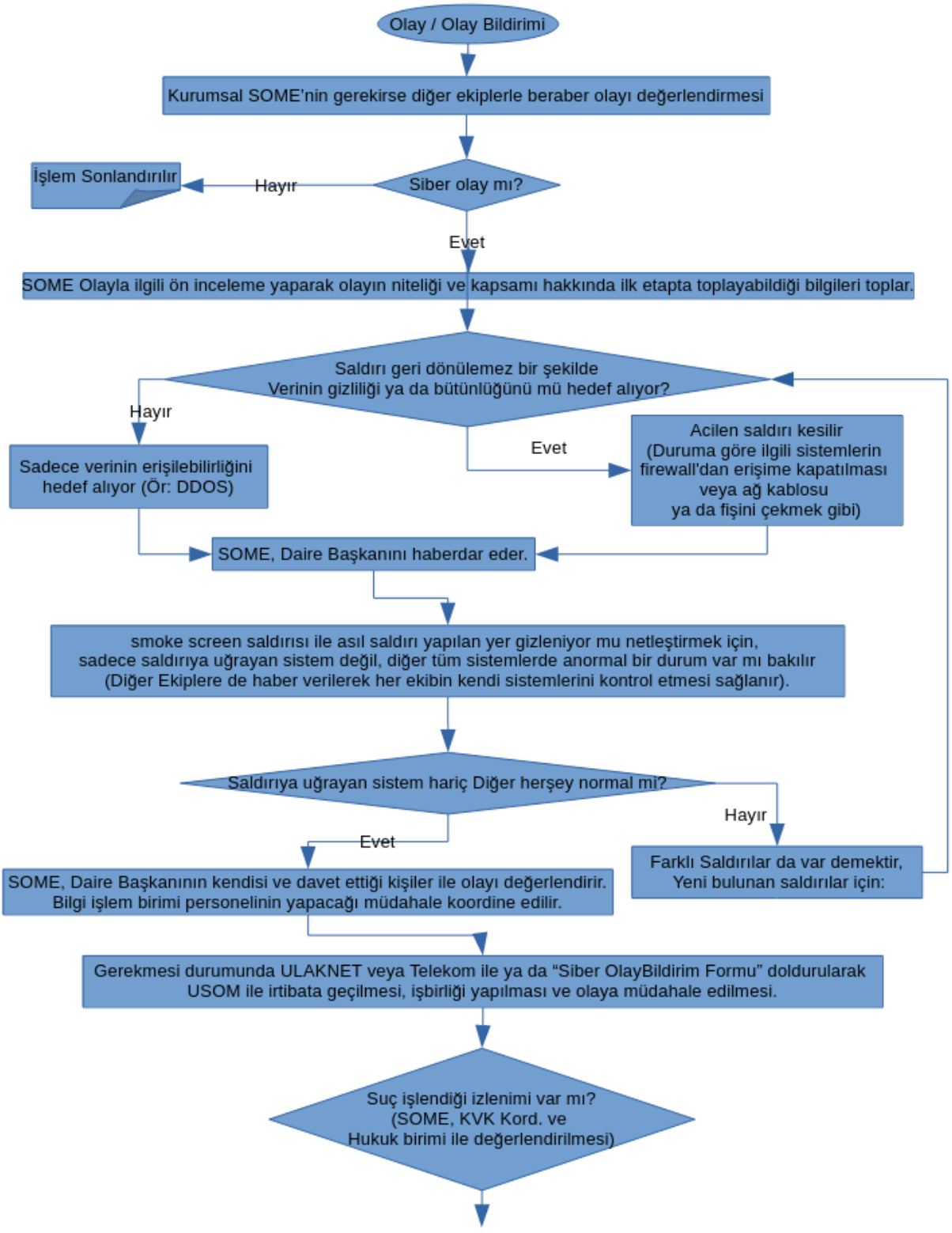
3.6.2. Bilinen tüm zafiyetlerin otomatik araçlarla taranmış olması.

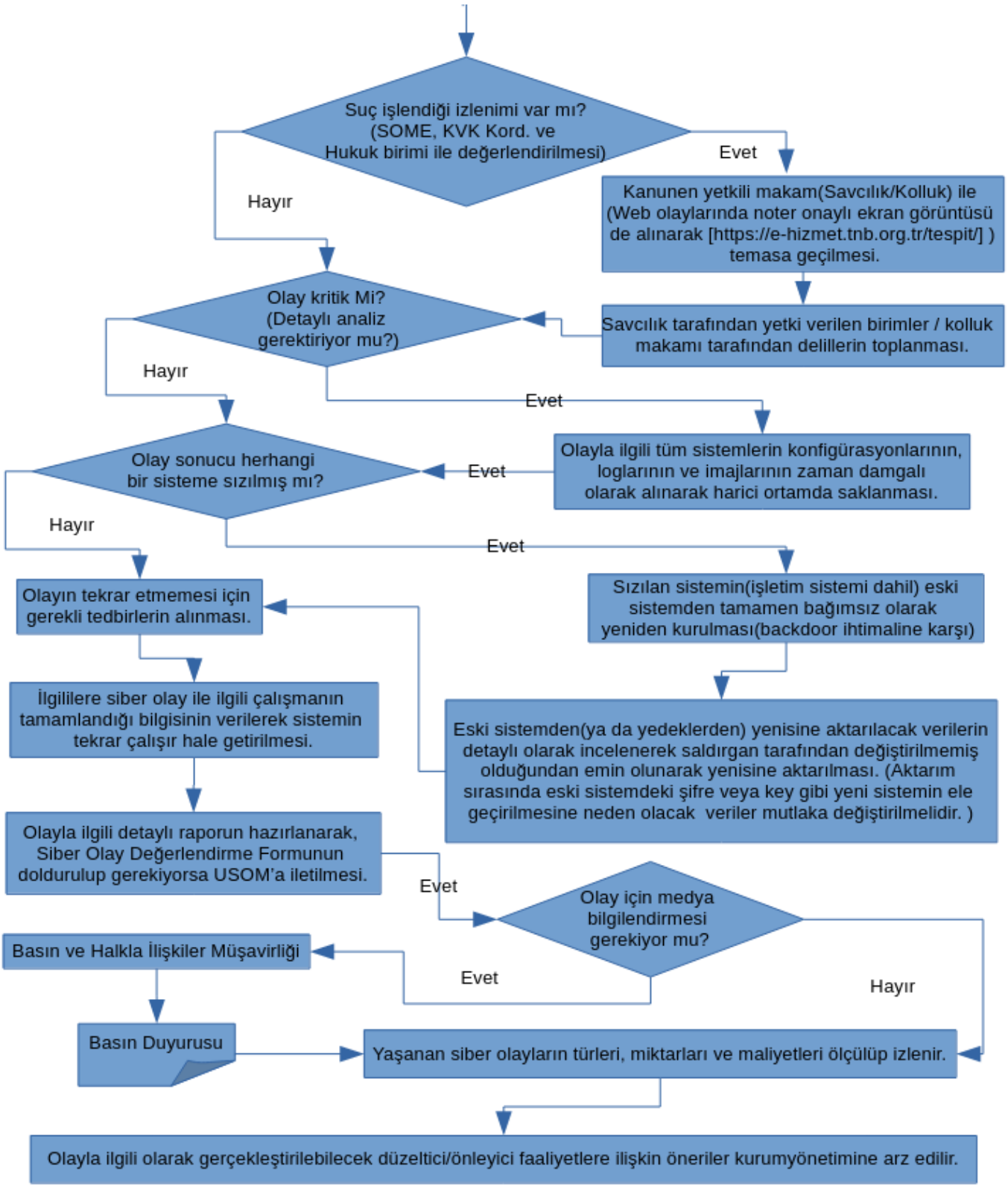
3.6.3. İlgili personelin uyum içinde gerekli müdahale ve bilgilendirmeleri yapması.

3.6.4. Benzer olayların tekrar etmemesi için gerekli önlemlerin alınmış olması.

3.7. **Süreç Periyodu:** Siber olay oluşması durumları.

3.8. İş Akış Şeması




Suç işlendiği izlenimi var mı? (SOME, KVK Kord. ve Hukuk birimi ile değerlendirilmesi)
Evet
Hayır
Kanunen yetkili makam(Savcılık/Kolluk) ile (Web olaylarında noter onaylı ekran görüntüsü de alınarak [https://e-hizmet.tnb.org.tr/tespit/]) temasa geçilmesi.
Olay kritik Mi? (Detaylı analiz gerektiriyor mu?)
Savcılık tarafından yetki verilen birimler / kolluk makamı tarafından delillerin toplanması.
Hayır
Evet
Olay sonucu herhangi bir sisteme sızılmış mı?
Evet
Olayla ilgili tüm sistemlerin konfigürasyonlarının, loglarının ve imajlarının zaman damgalı olarak alınarak harici ortamda saklanması.
Hayır
Evet
Olayın tekrar etmemesi için gerekli tedbirlerin alınması.
Sızılan sistemin(işletim sistemi dahil) eski sistemden tamamen bağımsız olarak yeniden kurulması(backdoor ihtimaline karşı)
İlgililere siber olay ile ilgili çalışmanın tamamlandığı bilgisinin verilerek sistemin tekrar çalışır hale getirilmesi.
Eski sistemden(ya da yedeklerden) yenisine aktarılacak verilerin detaylı olarak incelenerek saldırgan tarafından değiştirilmemiş olduğundan emin olunarak yenisine aktarılması. (Aktarım sırasında eski sistemdeki şifre veya key gibi yeni sistemin ele geçirilmesine neden olacak veriler mutlaka değiştirilmelidir.)
Olayla ilgili detaylı raporun hazırlanarak, Siber Olay Değerlendirme Formunun doldurulup gerekiyorsa USOM'a iletilmesi.
Evet
Olay için medya bilgilendirmesi gerekiyor mu?
Basın ve Halkla İlişkiler Müşavirliği
Evet
Hayır
Basın Duyurusu
Yaşanan siber olayların türleri, miktarları ve maliyetleri ölçülüp izlenir.
Olayla ilgili olarak gerçekleştirilebilecek düzeltici/önleyici faaliyetlere ilişkin öneriler kurumyönetimine arz edilir.