

DAFTAR ISTILAH

Istilah	Deskripsi	Halaman
Eksplorasi	Penggunaan kerentanan dalam sistem komputer untuk memperoleh akses yang tidak sah atau merusak sistem tersebut.	1
Fungsi Kontrol	Mekanisme dan strategi yang diterapkan untuk mengendalikan dan mengelola operasi serta interaksi antara komponen fisik dan dalam suatu sistem.	1
IBM QRadar	Aplikasi SIEM <i>open source</i> untuk membantu organisasi mendeteksi dan merespons ancaman keamanan dengan cepat	1
<i>Threat Behavior</i>	Mendeteksi pola perilaku mencurigakan yang mungkin menjadi indikasi terjadinya serangan.	1
<i>Threat Intelligence</i>	Memberikan wawasan tentang ancaman serangan	1
<i>Brute Force</i>	Serangan yang mencoba semua kombinasi <i>username</i> dan <i>password</i> untuk mendapatkan akses.	2
<i>Network Attack</i>	Tindakan yang dilakukan oleh individu atau kelompok yang berniat jahat untuk mengeksploitasi kelemahan atau celah dalam sistem keamanan.	2
<i>Port Scanning</i>	Teknik yang digunakan untuk mengidentifikasi <i>port</i> terbuka pada sistem target.	2
<i>Profiling</i>	Proses pembuatan representasi rincian dari karakteristik dan perilaku pengguna berdasarkan data yang dikumpulkan.	2
<i>Log</i>	Catatan otomatis dari aktivitas sistem komputer atau jaringan, digunakan untuk pemantauan, analisis keamanan, dan pemecahan masalah.	3
<i>Vulnerability</i>	Kelemahan atau celah dalam sistem informasi yang dapat dieksploitasi oleh ancaman untuk merusak, mencuri, atau mengakses informasi secara tidak sah.	7

Fungsi Deteksi	Proses identifikasi keberadaan objek atau aktivitas tertentu dalam jaringan komputer atau sistem informasi.	9
Metrik <i>Granularity</i>	Tingkat detail yang digunakan dalam pengukuran dan analisis data.	10
Metrik <i>Response Time</i>	Waktu yang dibutuhkan oleh suatu sistem untuk menanggapi permintaan deteksi.	10