USE CASE MÁTRIX MINTA

			Bevonandó adat/ logforrások																																
Use Case Azonosító (ID)	**Use Case Kategória (Category)**	**Use Case Megnevezése (Name)**	**Tevékenység**	Active Directory (Windows AD)	Windows event log	Privilged user monitoring (Netwrix Auditor, Shell Control Box, Wallix AdminBastion)	User Behavior Monitoring	(W,N;H)IDS (Aruba, Cisco, OSSEC, snort, Suricata	Netflow collector (IBM Qflow, nfsen)	DNS	DHCP	DLP (DeviceLock, Digitaguardian)	Linux Server	Wireless contoller (Aruba)	Web gateway (Sophos UTM, Imperva	Mail gateway (Sophos UTM)	Perimeter security appliance (Sophos UTM, Fortigate, Palo Alto)	Memory corruption detection (Sophos Intercept X, EMET)	File Integrity monitoring (Carbon Black, OSSEC)	Anti Virus (Sophos Endpoint, Windows Defender, Kaspersky)	Vulnerability Scanner (Nexpose, Nessus)	Radius Server	Networking devices (Cisco switch)	Authentication solution (multi-factor auth, Sophos, Gemalto, RSA)	Proxy Badge (Entry system)	Web Application Firewall (Imperva, F5, modsecurity)	Threat Intelligence (CTI), honeypot	Hálózati és felhasználói viselkedés elemzés	MDM	Availability monitoring (Nagios, Zabbix)	SIEM	IDM (CyberArk)	**Megjegyzés**
1	Privileged user Monitoring	Excessive Failed Logon Attempts with same Privileged ID	Alert	X		X																X												Watchlist needed
2	Authentication	Excessive Failed Logon Attempts from same Source IP	Alert	X		X		X									X					X												
3	Privileged User Monitoring	Web browsing activity with privileged credentials	Alert		X																														
4	Privileged User Monitoring	Interactive login with system or application accounts	Alert	X	X																														
5	Privileged User Monitoring	Domain Account created from unauthorized user ID	Alert	X	X	X																													
6	Privileged User Monitoring	Logging in as root in Linux/Unix environment	Alert											x																					
7	Privileged User Monitoring	Daily report of sudo commands In Linux/Unix environment	Report																																
8	Privileged User Monitoring	Domain Account created from unauthorized user ID	Alert	X	X																														
9	Privileged User Monitoring	Local Server Account created from an unauthorized user ID	Alert		X																														
10	Authentication	Successful login to honeyword account	Alert	X				X																											
11	Authentication	Attempted login for dormant or inactive accounts	Alert	X				X																											
12	Privileged User Monitoring	Network login to local account	Alert		X																		x												
13	Privileged User Monitoring	Adding a network account to a privileged group from an unauthorized ID	Alert	X																															
14	Privileged User Monitoring	Adding a local account to a privileged group on critical system	Alert	X	X																	X	x	X											
15	Remote Authentication	Excessive Remote Failed Logon Attempts with same ID	Alert	X	X												X					X		X											
16	Remote Authentication	Excessive Remote Failed Logon Attempts from same Source IP	Alert		X			X																											
17	Authentication	Monitoring of default account login attempts	Report	X	X									x		x	x						x												
18	Authentication	Attempted login for administratively disabled accounts	Report	X	X									x																x						
19	Malware	Malware detected on critical system	Alert					X													X														
20	Malware	Antivirus software service stopped/disabled	Alert		X																x														
21	Malware	Malware detected on end-user workstation	Alert					x													x														
22	Malware	Servers and workstations with outdated virus definition	Report																		x														
23	Malware	Infected files not quarantined	Report																		x														
25	Malware	Top 50 Infected hosts	Report																		x														
26	Traffic to Malicious Destination	Network traffic from critical systems to known malicious IP	Alert					X									X																		
27	Traffic to Malicious Destination	Excessive firewall denies on perimeter firewalls by same Source IP	Alert					X									X												X						
28	Traffic to Malicious Destination	Excessive firewall denies on perimeter firewalls to same Dest IP	Alert					X									X												X						
29	Traffic to Malicious Destination	Excessive dropped requests by proxy	Alert														X																		
30	Traffic to Malicious Destination	Top 50 Hosts for dropped traffic on perimeter firewalls	Report					X									X																		
32	Traffic to Malicious Destination	Top 50 TCP/UDP Ports for dropped traffic on perimeter (0-day-threats)	Report					X	X								X																		
33	Traffic to Malicious Destination	Destination IP only visited by single user-agent-string	Report					X							X																				
36	Traffic to Malicious Destination	Internal DNS requests for non-context Intranet FQDNs	Report							X																									
37	Systems Monitoring	New services and assets detected In critical zones	Alert						X	X												X													
38	Loss of Sensitive Data	Pll Data Exfiltration Detected	Alert									X																							
39	Loss of Sensitive Data	High profile data exfiltration detected	Alert									X																							
41	Network Enumeration/Reconnaissance	Internal systems network scan	Alert					X	X																										
42	Network Enumeration/Reconnaissance	Traffic destined to internal honeypot/honeynet IP addresses	Alert					X	X								X																		
43	Network Enumeration/Reconnaissance	External vertical scan followed by successful login from same Src IP	Alert		X	X		X									X																		
44	Network Enumeration/Reconnaissance	External horizontal scan followed by a successful login from same Src IP	Alert		X	X		X									X																		
45	Web Based Attacks	Cross Site Scripting (XSS)	Alert					X						X								X													
46	Web Based Attacks	SQL Infection attempts	Alert					X						X								X													
47	Web Based Attacks	File Inclusion Exploitation attempts	Alert					X				x		X								X													
48	Web Based Attacks	Excessive login attempts from source IP	Alert					X						X																					
49	Web Based Attacks	Website defacement attempts	Alert					x						X																					
50	Remote Authentication	Attempts from known malicious source IP	Alert					X									X																		
51	Remote Authentication	Excessive Failed Login attempts on same Account followed by a success	Alert	X	X												X					X		X											
53	Wireless Intrusions	Multiple channel hopping from the same AP	Alert												X																				
54	Wireless Intrusions	Multiple deauth attemps (limit 3)	Alert					X							X																				
55	Network Enumeration/Reconnaissance	Excessive dataflow from Source IP	Alert						X			X																							
56	Network Enumeration/Reconnaissance	Suspicious SSL certificate connection from a bad IP reputation site on SRC_IP	Alert			X		x									X												X	x					
57	Logging	Data Source stoped logging after X time	Alert																														x		
58	Enironmental awareness	Audit cofiguration changed	Alert	X	X	x											X																		
59	Malware	Malware detected on windows system	Alert		X			X													X														

soc.blackcell.hu