Talence Security

Top Threats Cheat Sheet: Detection, Prevention and Response

Top Threats

Attack Type	Description	Threat Indicators	Areas to Investigate	Prevention & Response Actions
Phishing Attacks	Fraudulent attempts to obtain sensitive information via deceptive emails or websites.	Reports of suspicious emails, unusual login activities.	SIEM, Email Filtering Logs, User Reports, DNS Logs, Web Traffic.	Implement advanced email filters, reputation check and anti-malware scans, conduct phishing simulations, regularly educate users on recognizing phishing.
Ransomware	Malicious software that encrypts data and demands payment for decryption.	Sudden file modifications, ransom notes, EDR & Antivirus alerts, network activities such as C2 connections and data exfiltration.	SIEM, EDR/XDR Platform, Antivirus Logs, System Logs, User Activity Logs, Network Traffic (FW/Proxy), DLP Solution Logs.	Execute antivirus scans, isolate infected system, notify law enforcement, try to decrypt for free*, do not pay ransom, keep undecryptable data if valuable (maybe the data can be decrypted in the future) *(*) Visit NoMoreRansom.org*
Vulnerabilities	Exploiting weaknesses in software or hardware to gain unauthorized access.	Unexpected system behavior (privilege escalation, persistence, etc.), Anti-Exploit reports	Vulnerability Scans, Patch Management Logs, System Audits, Anti-Exploit Logs.	Update and patch systems, conduct vulnerability assessments, implement security best practices, assumes zero-days exist in all your technologies and devices.
Business Email Compromise	Unauthorized access to business email accounts for financial gain or data theft.	Unusual email activity, unauthorized financial transactions, phishing reports.	User's System Logs, Email Logs, Network Traffic, User Reports.	Quarantine affected accounts, reset passwords, educate employees, implement MFA, email authentication (SPF, DKIM, and DMARC)
Cloud Security Breaches	Exploiting vulnerabilities in cloud services to access data or disrupt operations.	Unauthorized access attempts, data leaks, unusual cloud resource usage.	Cloud Service Logs, Access Logs, Network Traffic.	Implement CASBs, implement multi-factor authentication, encrypt data (at rest and in transit), backup your data, conduct regular security assessments, enforce strict identity and access controls (IAM).
Social Engineering Attacks	Manipulating individuals into divulging confidential information or performing harmful actions.	Reports of suspicious interactions, unusual account activities.	User Reports, Communication Logs, Access Logs.	Educate employees on social engineering tactics, implement access control, multi-factor authentication, monitor communications and critical assets and perform regular audits.
Insider Threats	Malicious actions by employees or contractors to steal data or disrupt operations.	Unusual data access patterns, unauthorized data transfers, suspicious behavior.	Employee Activity Logs, Access Controls, Network Monitoring.	Monitor user activity, enforce least privilege access, conduct regular security training for employees.
Denial of Service (DoS/DDoS)	Overloading a service to make it unavailable.	Extremely high network traffic targeting a service or server, possible ransom demands.	Traffic Monitoring, Anti-DDoS Solution Logs, Firewall Logs, System Logs.	If due to vulnerabilities: Implement patches, contact ISP, filter incoming traffic, apply server rate limits, configure rate limits using an edge-network Firewall, use a CDN, do not pay ransom.
Supply Chain Attacks	Targeting of an organization through its supply chain (partners, softwares, libraries, etc.).	Unusual network traffic, unusual endpoints behaviors, alerts from supply chain partners.	Vendor Communications, Network Logs, Systems Access Logs, Systems Activities Logs.	Security policies assume supply chain attacks are possible, monitor and restrict third-party access, conduct regular security audits.
IoT and Industrial IoT Attacks	Exploiting vulnerabilities in Internet of Things devices to gain access or disrupt services.	Unusual device behavior, network anomalies.	IoT Device Logs, Network Traffic, Firmware Updates.	Implement strong authentication, regularly update firmware, segment IoT devices on the network, filter inbound access, do not expose administrator interfaces, regularly review and update IoT device configurations.
Advanced Persistent Threats (APTs)	Prolonged and targeted cyberattacks designed to infiltrate a network and remain undetected.	Persistent network anomalies, data exfiltration, unauthorized account creations.	Network Logs, Access Logs, System Processes, Incident Response Teams.	Preventively and continuously improve the company's security posture, isolate affected systems, initiate a forensic investigation, and escalate incident response.

@TalenceSecurity
www.talencesecurity.com

Version 2.0
August 2024