SSL/TLS Inspection, Mitigation M1020 - Enterprise

Archived: 2026-04-05 15:38:22 UTC

SSL/TLS inspection involves decrypting encrypted network traffic to examine its content for signs of malicious activity. This capability is crucial for detecting threats that use encryption to evade detection, such as phishing, malware, or data exfiltration. After inspection, the traffic is re-encrypted and forwarded to its destination. This mitigation can be implemented through the following measures:

Deploy SSL/TLS Inspection Appliances:

- Implement SSL/TLS inspection solutions to decrypt and inspect encrypted traffic.
- Ensure appliances are placed at critical network choke points for maximum coverage.

Configure Decryption Policies:

- Define rules to decrypt traffic for specific applications, ports, or domains.
- Avoid decrypting sensitive or privacy-related traffic, such as financial or healthcare websites, to comply with regulations.

Integrate Threat Intelligence:

- Use threat intelligence feeds to correlate inspected traffic with known indicators of compromise (IOCs).

Integrate with Security Tools:

- Combine SSL/TLS inspection with SIEM and NDR tools to analyze decrypted traffic and generate alerts for suspicious activity.
- Example Tools: Splunk, Darktrace

Implement Certificate Management:

- Use trusted internal or third-party certificates for traffic re-encryption after inspection.
- Regularly update certificate authorities (CAs) to ensure secure re-encryption.

Monitor and Tune:

- Continuously monitor SSL/TLS inspection logs for anomalies and fine-tune policies to reduce false positives.

Source: https://attack.mitre.org/mitigations/M1020