ICT DIVISION
FUTURE IS HERE

BANGLADESH COMPUTER COUNCIL
COMPUTER FOR EVERYTHING

BGD e-GOV CIRT

TLP:CLEAR

FortiBleed Campaign Exposes FortiGate Devices in Bangladesh with Potential Credential Compromise

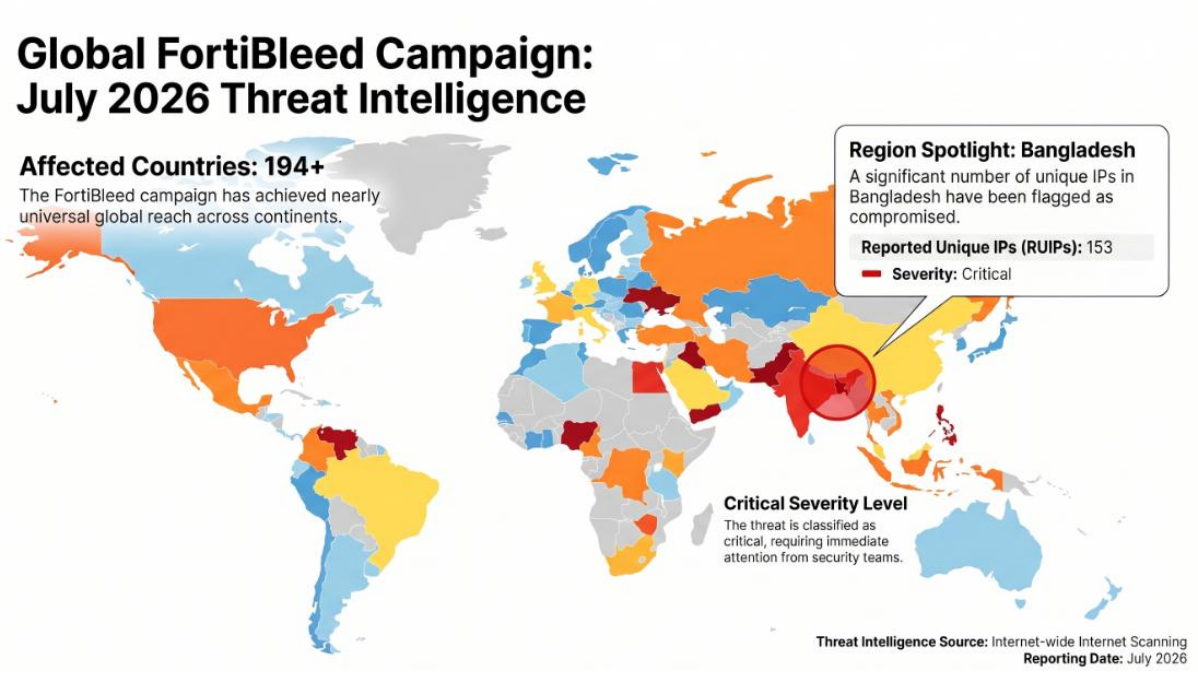
TLP: CLEAR
Distribution: Public
Advisory on: FortiBleed Campaign Exposes FortiGate Devices in Bangladesh with Potential Credential Compromise
Severity: Critical
Threat Type: Credential Theft, VPN Compromise, Active Directory Access
Date: 07 July 2026

Executive Summary

BGD e-GOV CIRT has identified **153 unique Bangladesh IP addresses** associated with the ongoing FortiBleed campaign affecting internet-facing Fortinet FortiGate security appliances. The affected systems have been reported with the "fortibleed" tag, indicating potential exposure to credential theft and unauthorized access resulting from exploitation of FortiGate vulnerabilities.

The campaign targets FortiGate SSL-VPN and management interfaces to obtain sensitive information, including user credentials, session data, authentication tokens, and Active Directory-related artifacts. Analysis conducted by multiple cybersecurity organizations indicates that attackers are actively harvesting credentials from vulnerable FortiGate appliances and leveraging the stolen information to gain persistent access into enterprise networks.

Organizations operating FortiGate devices should immediately verify whether their systems are affected, rotate all credentials associated with FortiGate appliances, review authentication logs, and investigate for evidence of unauthorized access.



Technical Analysis

FortiBleed Campaign Overview

The FortiBleed campaign represents an active large-scale credential compromise operation targeting internet-facing Fortinet FortiGate appliances. Threat intelligence indicates that attackers are exploiting compromised or previously vulnerable FortiGate systems to obtain authentication material and maintain persistent access to enterprise environments.

Unlike traditional remote code execution campaigns, FortiBleed primarily focuses on the exfiltration and operational reuse of authentication artifacts rather than immediate payload deployment. Harvested credentials enable attackers to bypass perimeter defenses and authenticate as legitimate users through FortiGate SSL-VPN services.

The campaign has been observed globally, affecting organizations across **194 countries**, with **153 publicly exposed FortiGate devices** identified in Bangladesh requiring immediate investigation.

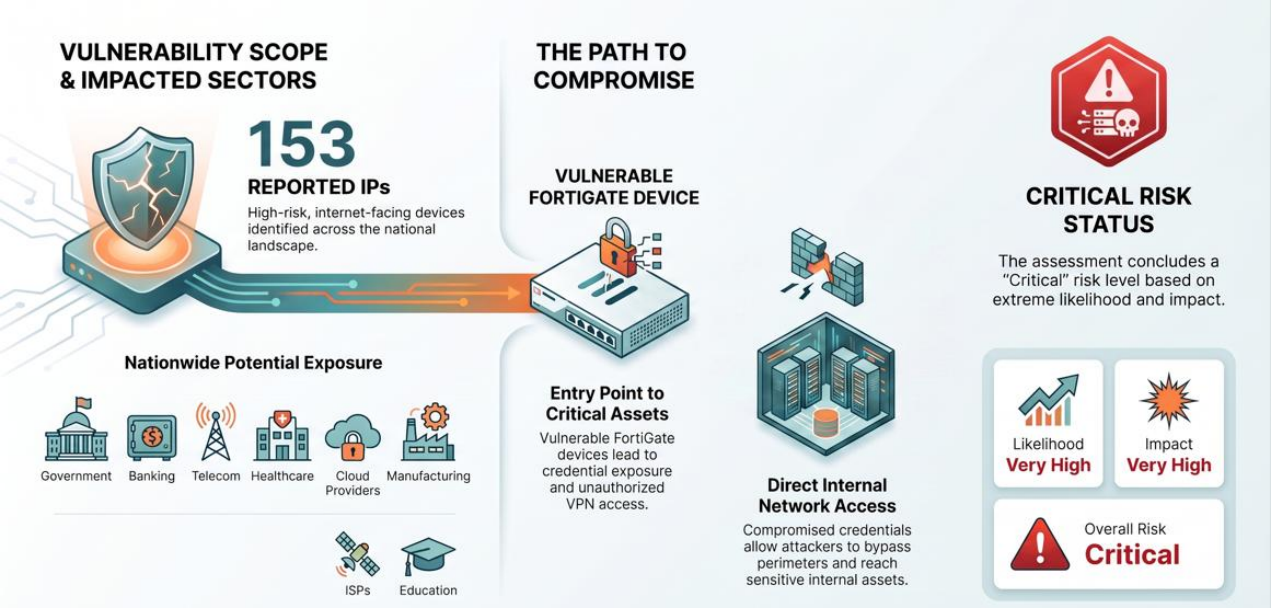


Figure: Bangladesh Risk Assessment

Technical Attack Lifecycle

The observed FortiBleed campaign follows a multi-stage intrusion model.

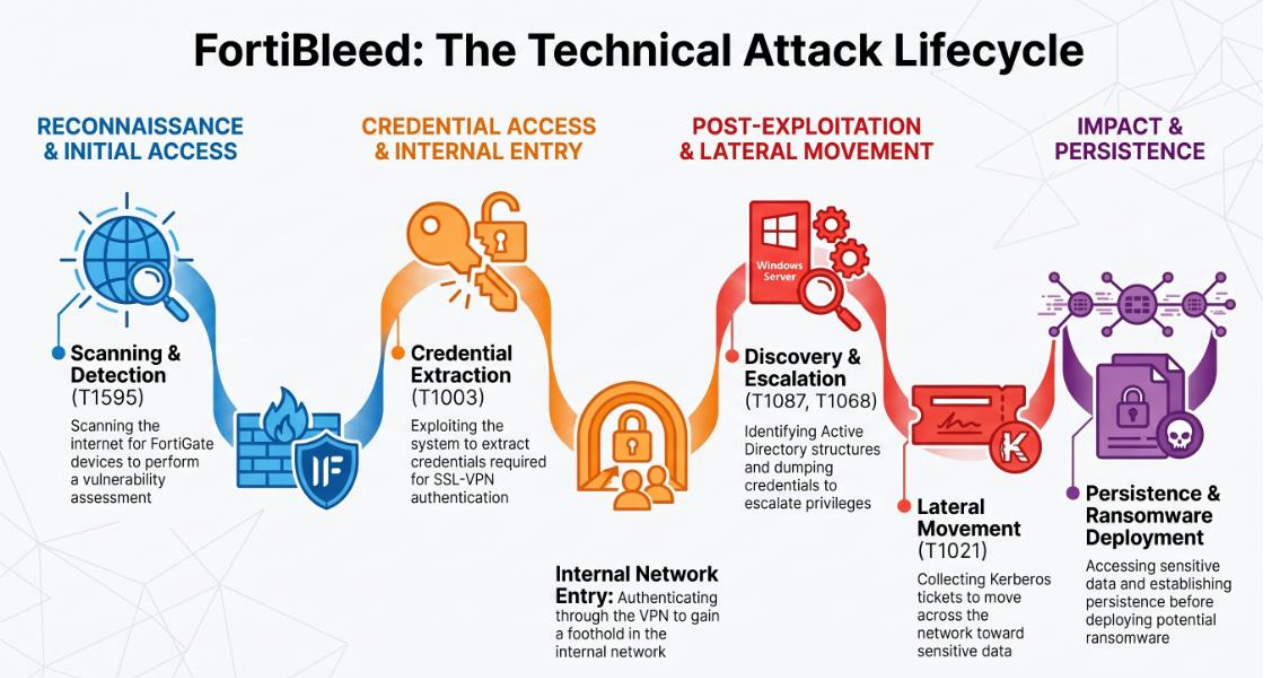


Figure: Multi-Stage FortiBleed Attack Lifecycle from Internet Exposure to Enterprise Compromise

Initial Reconnaissance

Threat actors continuously perform Internet-wide reconnaissance to identify exposed FortiGate appliances.

Reconnaissance typically includes:

- SSL-VPN portal enumeration
- Administrative interface discovery
- FortiOS version fingerprinting
- Certificate enumeration
- Banner grabbing
- Internet-wide scanning using automated frameworks

During this phase, attackers identify devices susceptible to credential extraction or devices that may have previously been compromised.

MITRE ATT&CK

- T1595 Active Scanning
- T1590 Gather Victim Network Information

Authentication Artifact Collection

The primary objective of FortiBleed is the acquisition of authentication material stored within FortiGate appliances.

Potentially exposed information includes:

- SSL-VPN usernames
- Passwords
- Session cookies
- Authentication tokens
- Device configuration
- VPN configuration
- Administrative credentials
- User session information
- Authentication cache

Once extracted, attackers validate harvested credentials against exposed SSL-VPN gateways.

Unlike brute-force attacks, authentication occurs using legitimate credentials, significantly reducing detection opportunities.

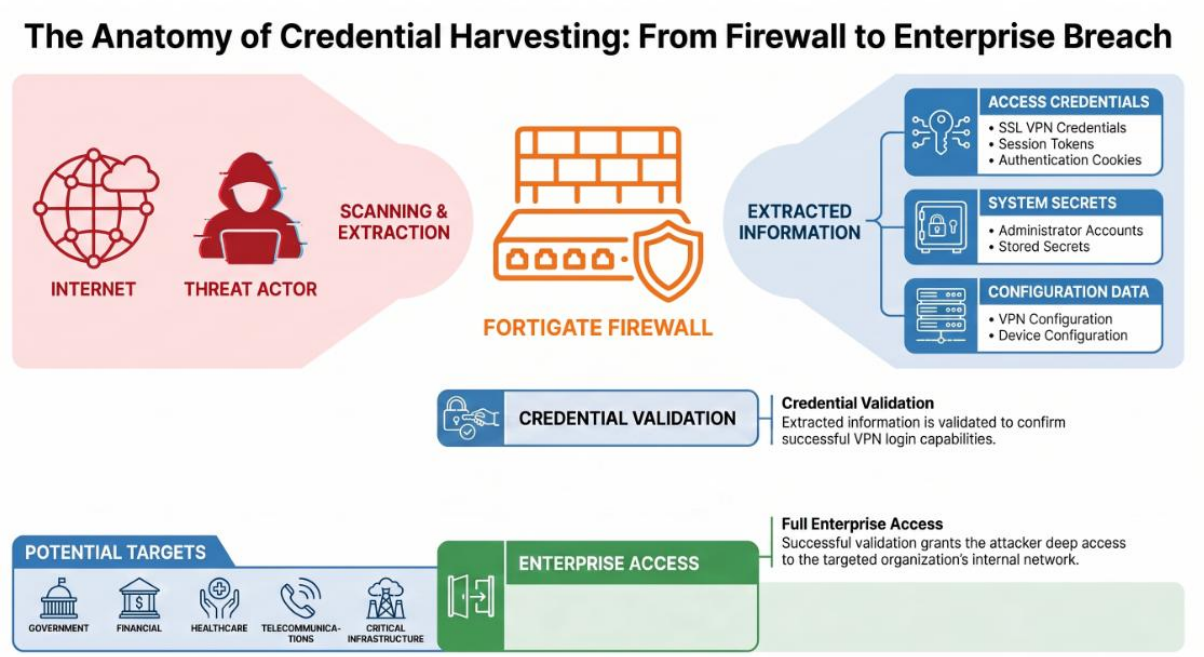


Figure: Authentication Artifact Harvesting Process

SSL-VPN Session Hijacking

Compromised authentication artifacts may allow attackers to hijack active VPN sessions.

- Observed techniques include:
- Session cookie replay
- Authentication token reuse
- VPN credential replay
- Session impersonation

If Multi-Factor Authentication (MFA) is enforced only during initial authentication, possession of valid session identifiers may permit continued access without requiring additional user interaction.

Potential consequences include:

- Remote access to internal networks
- Persistent VPN connectivity
- Stealthy post-compromise operations
- Access to sensitive applications.

Internal Network Reconnaissance

Following successful authentication, attackers initiate reconnaissance activities designed to understand the internal enterprise environment.

Common objectives include:

Active Directory Discovery

- *nltest*
- *net group*
- *net user*
- *net view*
- *dsquery*
- *ldapsearch*

Network Discovery

- Domain Controllers
- File Servers
- Backup Servers
- Hypervisors
- Database Servers
- Exchange Servers

Administrative Discovery

- Local Administrators
- Domain Admins
- Enterprise Admins
- Service Accounts
- Privileged Groups

MITRE

- T1018 Remote System Discovery
- T1087 Account Discovery
- T1482 Domain Trust Discovery

Credential Access and Kerberos Exposure

Once inside the enterprise network, attackers frequently transition toward credential acquisition.

Common techniques include:

LSASS Memory Dumping: (lsass.exe)

Credential dumping utilities:

- Mimikatz
- ProcDump
- NanoDump

Kerberoasting

Service accounts requesting TGS tickets ➞ Extraction of TGS hashes ➞ Offline password cracking

AS-REP Roasting

Accounts configured without Kerberos pre-authentication ➞ AS-REP Hash Collection ➞ Offline cracking

DPAPI Collection

- Attackers may extract
- Browser passwords
- VPN credentials
- Wi-Fi keys
- Windows secrets

MITRE

- T1003
- T1558
- T1555

Privilege Escalation

Attackers attempt to obtain administrative privileges using:

- Cached Administrator Credentials
- Weak Service Account Passwords
- Kerberoasted Accounts
- Misconfigured ACLs
- Token Impersonation

Successful privilege escalation significantly expands the attack surface.

Lateral Movement

Observed enterprise pivot techniques include:

- *RDP*
- *SMB*
- *PsExec*

- *WinRM*
- *Remote PowerShell*
- *WMI*
- *Scheduled Tasks*
- *Remote Services*

MITRE

- T1021
- T1047
- T1053

Potential Ransomware Deployment

Although FortiBleed primarily represents a credential compromise campaign, compromised VPN credentials are commonly leveraged by ransomware operators.

Typical post-compromise sequence

1. Credential Theft
2. Domain Enumeration
3. Privilege Escalation
4. Backup Discovery
5. Security Tool Disablement
6. Data Exfiltration
7. Ransomware Deployment

This attack chain closely resembles recent campaigns conducted by: Akira, LockBit, INC, Play, Black Basta.

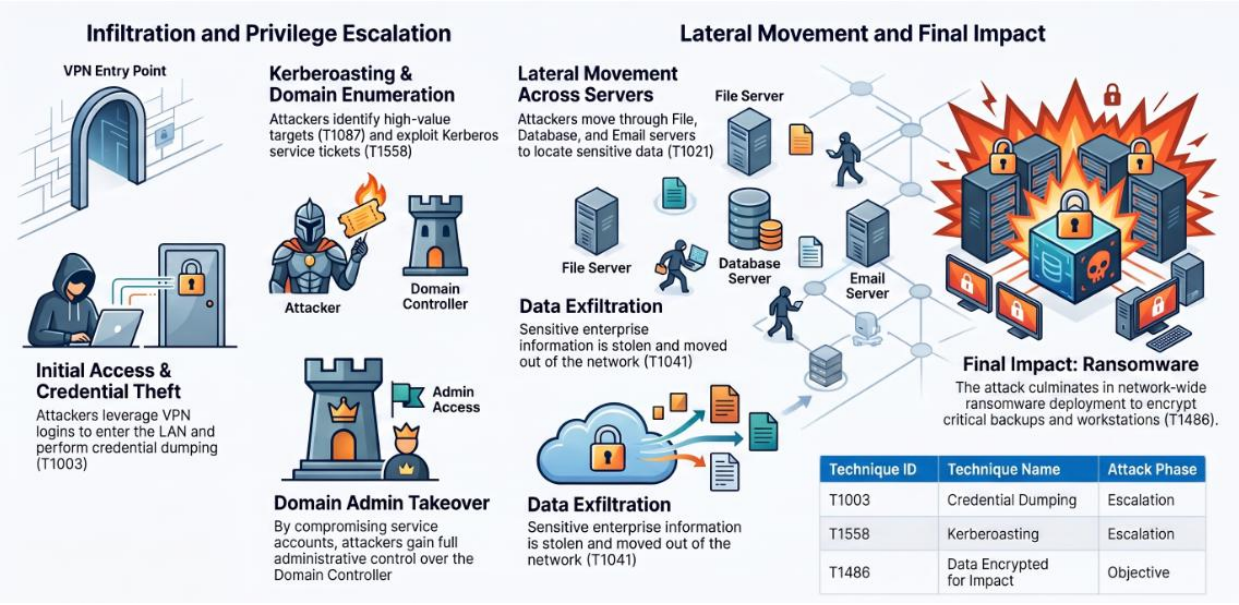


Figure: Representative post-compromise attack path following successful FortiGate credential compromise leading to Active Directory compromise and enterprise-wide lateral movement

Critical Monitoring Points

Monitoring Part	Description
Internet-facing FortiGate appliances	Publicly exposed VPN gateways
SSL-VPN authentication logs	Suspicious remote logins
VPN session identifiers	Unexpected concurrent sessions
Administrative authentication events	Abnormal privileged logins
Authentication cookies	Stolen VPN session artifacts

Behavioral Indicators

- Unexpected VPN logins
- Geographic login anomalies
- Privileged account misuse
- Rapid authentication followed by internal reconnaissance
- Active Directory enumeration
- Kerberos ticket harvesting
- Password spraying
- Credential stuffing
- Remote administrative tool execution

Detection and Monitoring

Organizations should implement continuous monitoring of FortiGate appliances, authentication systems, and Active Directory environments to identify indicators associated with credential compromise, unauthorized remote access, and post-exploitation activities linked to the FortiBleed campaign. Security teams should correlate firewall telemetry, VPN authentication logs, endpoint events, and network traffic to detect abnormal behaviors that may indicate successful exploitation or credential abuse.

FortiGate Device Monitoring

Monitor unauthorized administrator logins, configuration changes, firmware updates, configuration exports, and abnormal authentication activity.

SSL-VPN Authentication Monitoring

Detect VPN logins from unusual locations, impossible travel, concurrent sessions, dormant account usage, and repeated failed logins followed by successful authentication.

Active Directory Monitoring

Monitor domain enumeration, LDAP queries, Kerberos events (4768, 4769, 4771), privileged account changes, Group Policy modifications, and abnormal authentication activity).

Windows Security Events

Event ID	Description
4624	Successful logon
4625	Failed logon
4648	Logon using explicit credentials
4672	Special privileges assigned to a new logon
4688	Process creation
4720	User account created
4728 / 4732	User added to privileged group
4768	Kerberos Authentication Ticket (TGT) requested
4769	Kerberos Service Ticket (TGS) requested
4771	Kerberos pre-authentication failure
4776	NTLM authentication validation

Endpoint Detection

Detect credential dumping (LSASS access, Mimikatz, ProcDump), PowerShell abuse, WMI, PsExec, scheduled task creation, and execution of suspicious binaries.

Network Monitoring

Identify internal network scanning, SMB/RDP/WinRM activity, LDAP enumeration, suspicious DNS queries, and abnormal outbound data transfers.

SIEM Correlation Rules & Threat Hunting

Correlate FortiGate logs, VPN authentication events, Windows Security logs, EDR telemetry, and network traffic to detect post-VPN reconnaissance, Kerberos abuse, privilege escalation, firewall configuration changes, and lateral movement. Regularly hunt for anomalous VPN sessions, credential dumping, and unauthorized administrative activity.

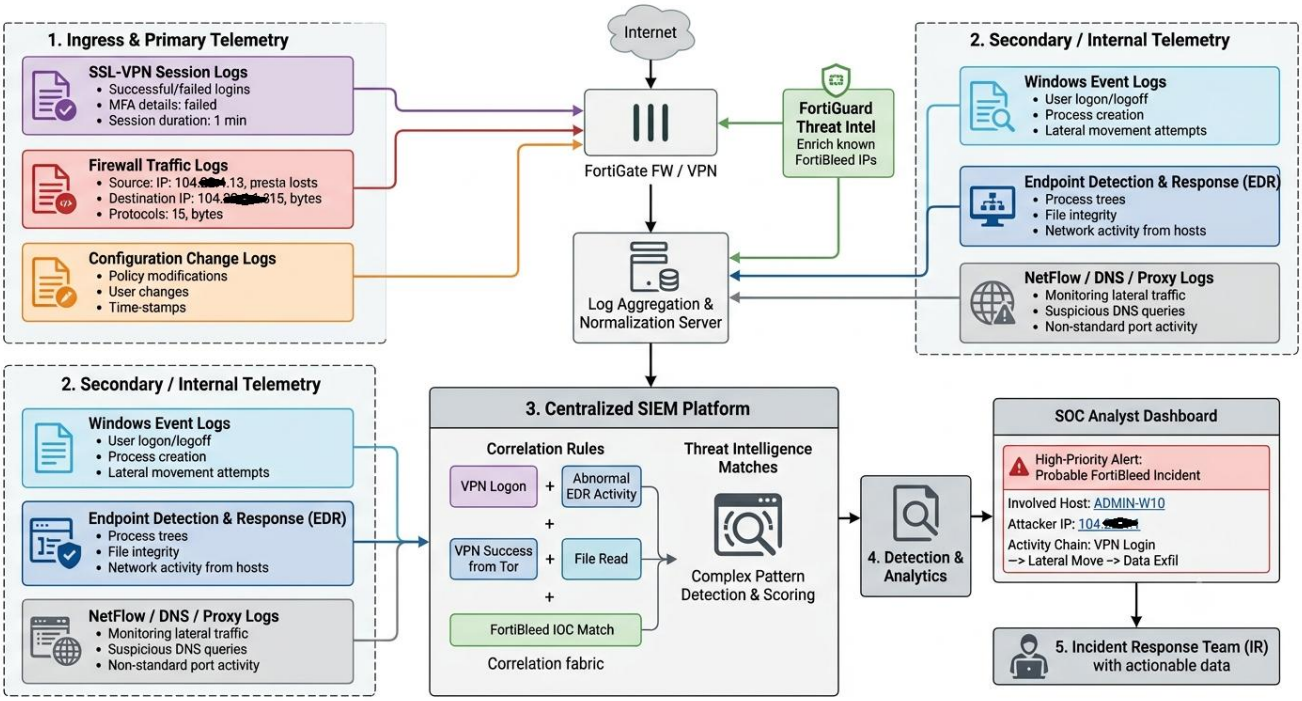


Figure: Recommended Monitoring and Detection Architecture

References:

- Fortinet PSIRT – Analysis of Reported Credential Compromise of FortiGate Devices https://www.fortinet.com/blog/psirt-blogs/analysis-of-reported-credential-compromise-of-fortigate-devices
- Arctic Wolf – Active FortiBleed Campaign Impacting Fortinet Devices Across 194 Countries https://arcticwolf.com/resources/blog/active-fortibleed-campaign-impacting-fortinet-devices-across-194-countries/
- Dataprise – FortiBleed: What Fortinet Customers Need to Know https://www.dataprise.com/resources/blog/fortibleed-what-fortinet-customers-need-to-know/
- Microsoft – Kerberos Authentication Technical Documentation https://learn.microsoft.com/windows-server/security/kerberos/