Crowe

Weekly Cyber Security Bulletin

Threat Advisory & Security News

16 Nov – 22 Nov 2026

Audit/Tax/Consulting

Smart decision. Lasting value.

Summary

Vulnerability Details

- CVE-2026-129448: Apache Roller Unauthenticated XML-RPC Deserialization Remote Code Execution Vulnerability
- CVE-2026-114938: OpenJDK / Oracle Java SE Base64 Decoder Memory Corruption Vulnerability ("Java4Shell") Leading to Potential Remote Code Execution
- CVE-2026-123007: NGINX HTTP/2 Flow Control Window Overflow Leading to Heap Buffer Overflow and Potential Remote Code Execution

Attack Campaigns

- Ipsos: Cybersecurity incident involving an internal information system
- Osaki Electric: Ransomware disrupts manufacturing and shipment operations
- Equinor: Cyberattack against energy sector IT systems

Security News

- Optimizely: Malicious JavaScript injected into customer websites
- Contabo: Unauthorized access to hosting provider infrastructure
- Reka: Cyberattack exposes customer travel data and triggers WhatsApp fraud

2. Vulnerability Details

2.1 CVE-2026-129448: Apache Roller Unauthenticated XML-RPC Deserialization Remote Code Execution Vulnerability

Release Date: 17 November 2026

CVSS Score: 9.8 (Critical)

Affected Products:

Product	Affected Versions
Apache Roller	Versions 4.0.0 through 6.1.4

Summary

CVE-2026-129448 is a critical unauthenticated remote code execution vulnerability in Apache Roller. The application's XML-RPC endpoint accepts vendor extension types and deserializes user-supplied data before authentication occurs. An attacker can exploit this flaw remotely without credentials by sending specially crafted XML-RPC requests containing malicious serialized objects.

Impact

- Execute arbitrary code remotely without authentication.
- Completely compromise the affected Apache Roller instance.
- Access, modify, or delete sensitive data.
- Cause service disruption and denial-of-service conditions.
- Pivot further into the internal network using the compromised application server.

Fixed Releases

Product	Fixed Version
Apache Roller	6.1.6 and later

Vendor Recommendation

- Immediately upgrade to Apache Roller 6.1.6 or later.
- If immediate patching is not possible:
  - Set enabledForExtensions=false in WEB-INF/web.xml.

- Or remove the /roller-services/xmlrpc servlet mapping.
- Restart the application after applying changes.
- Do not rely solely on disabling XML-RPC through the administration UI because vulnerable versions deserialize requests before checking that configuration setting.

Reference:

https://lists.apache.org/thread/lnz4s26tv6hdo03wngtdbpfj4hg4gtds

2.2 CVE-2026-114938: OpenJDK / Oracle Java SE Base64 Decoder Memory Corruption Vulnerability ("Java4Shell") Leading to Potential Remote Code Execution

Release Date: 17 November 2026

CVSS Score: 9.2 (Critical)

Affected Product:

Product	Affected Versions
Oracle Java SE	8u511b33-perf, 17.0.21.0.3, 21.0.13.0.3, 25.0.5.0.3, 27.0.1.0.3
Oracle GraalVM for JDK	17.0.21.0.3, 21.0.13.0.3
Oracle GraalVM Enterprise Edition	21.3.20.0.3

Summary

CVE-2026-114938, commonly referred to as **Java4Shell**, is a memory corruption vulnerability in the optimized Base64 decoder within the OpenJDK HotSpot JVM. A specially crafted Base64 string can trigger an out-of-bounds write, resulting in heap memory corruption. Under certain conditions, attackers can leverage the flaw to achieve unauthenticated remote code execution.

The vulnerability primarily impacts x86-64 systems using AVX-512 VBMI instructions and does not affect ARM64 systems.

Impact

- Achieve unauthenticated remote code execution (RCE).
- Take over affected Java applications and services.
- Read sensitive memory contents such as credentials, private keys, and session tokens.
- Cause application crashes and denial-of-service conditions

Fixed Releases

Product	Fixed Version
Oracle Java SE 8 Performance Build	8u513
Oracle Java SE / OpenJDK 17	17.0.21.1
Oracle Java SE / OpenJDK 21	21.0.13.1
Oracle Java SE / OpenJDK 25	25.0.5.1
Oracle Java SE / OpenJDK 27	27.0.1.1
Oracle GraalVM for JDK	Vendor-fixed releases available from Oracle

Vendor Recommendation

- Upgrade immediately to fixed Java/OpenJDK releases.
- Prioritize internet-facing Java applications, especially identity, CI/CD, and collaboration platforms.
- Restart all JVMs after applying updates.
- If patching is not immediately possible, disable the vulnerable optimization using:
  -XX:+UnlockDiagnosticVMOptions -XX:-UseBASE64Intrinsics.
- Alternatively, disable AVX-512 optimization with: -XX:UseAVX=2 (performance impact possible).

Reference:

Critical Patch Updates, Critical Security Patch Updates, Security Alerts and Bulletins

2.3 CVE-2026-123007: NGINX HTTP/2 Flow Control Window Overflow Leading to Heap Buffer Overflow and Potential Remote Code Execution

Release Date: 18 November 2026

CVSS Score: 10.0 (Critical)

Affected Product:

Product	Affected Versions
NGINX Open Source	Versions 1.9.5 through 1.31.8 (unpatched)
NGINX Open Source 1.30 branch	Versions earlier than 1.30.7
NGINX Open Source 1.31 branch	Versions earlier than 1.31.9
NGINX Plus	Builds prior to fixed releases (e.g., before 37.3.0.1 / 37.0.8.1 depending on release train)

Summary

A flaw exists in the HTTP/2 implementation of NGINX where specially crafted HTTP/2 traffic can cause the flow control window to exceed permitted limits. This condition results in a heap buffer overflow and memory corruption within the NGINX worker process.
The vulnerability is exploitable remotely without authentication against servers that process HTTP/2 traffic.

Impact

- Crash NGINX worker processes (Denial of Service).
- Corrupt process memory.
- Execute arbitrary code remotely under certain conditions, particularly where ASLR is disabled or can be bypassed.
- Potentially gain access to sensitive application traffic, credentials, session tokens, or TLS-related data handled by NGINX workers.

Fixed Releases

Product	Fixed Version
NGINX Open Source 1.30.x	1.30.7
NGINX Open Source 1.31.x	1.31.9
NGINX Plus	Fixed releases include 37.3.0.1 and 37.0.8.1 (depending on release branch)

Vendor Recommendation

- Immediately upgrade affected NGINX Open Source and NGINX Plus deployments to the latest fixed versions.
- Prioritize Internet-facing systems that accept HTTP/2 connections.
- If patching cannot be performed immediately, disable HTTP/2 support as a temporary mitigation measure.
- Review deployments for unsupported or End-of-Technical-Support (EoTS) versions and migrate to supported releases.

Reference:

NGINX ngx_http_v2_module vulnerability CVE-2026-123007

3. Attack Campaigns

3.1 Ipsos: Cybersecurity incident involving an internal information system

Description

Ipsos, a global market research and consulting firm, disclosed a cybersecurity incident affecting one of its internal information systems. The organization identified unauthorized activity within the affected system, promptly initiated its incident response procedures, engaged external cybersecurity specialists, and reported the incident to the relevant authorities. At the time of disclosure, the investigation remained ongoing to determine the full scope, root cause, and any potential impact on client, project, or business partner information. The company stated that the incident did not disrupt its business operations or client service delivery.

Attack Methodology

- Unauthorized Access to an Internal Information System: Threat actors successfully compromised an internal system within the Ipsos environment. While the exact intrusion vector has not been publicly disclosed, the incident involved unauthorized access to corporate infrastructure.
- Potential Access to Sensitive Corporate Information: As the forensic investigation remains ongoing, authorities and investigators are assessing whether information related to clients, projects, or business partners may have been accessed during the intrusion.
- Undetermined Initial Access Vector: No evidence has been publicly released regarding exploitation of a vulnerability, phishing activity, credential compromise, or malware deployment. Therefore, the initial access method remains unknown at this stage.

Key Takeaways

- Internal Systems Remain Attractive Targets: Even a single compromised internal system can expose sensitive corporate information and create potential risks for customers, partners, and ongoing business operations.
- Rapid Incident Response Reduces Business Impact: The prompt activation of containment procedures and engagement of external cybersecurity experts helped Ipsos manage the incident without reported disruption to client services or business operations. turn1search2
- Early Disclosure Supports Transparency: Notifying authorities and conducting a formal investigation demonstrates the importance of timely incident reporting and regulatory compliance when cybersecurity events occur. turn1search2
- Ongoing Monitoring Is Critical After Containment: Organizations must continue forensic analysis after an incident to determine whether sensitive data was accessed, modified, or exfiltrated before containment measures were implemented.

Mitigation Recommendations

- Implement Privileged Access Management (PAM): Deploy solutions such as CyberArk, Delinea, or Beyond Trust to control, monitor, and audit access to critical internal systems and administrator accounts.
- Enforce Multi-Factor Authentication (MFA): Require phishing-resistant MFA, such as FIDO2 security keys or Microsoft Authenticator, for all employee and privileged accounts accessing internal systems.
- Strengthen Continuous Monitoring and Threat Detection: Utilize SIEM and XDR platforms such as Microsoft Sentinel, Microsoft Defender XDR, CrowdStrike Falcon, or Google SecOps to identify suspicious activity and unauthorized access attempts in real time.
- Conduct Regular Security Assessments: Perform vulnerability assessments, penetration testing, and configuration audits to identify security weaknesses before they can be exploited by attackers.

- Enhance Incident Response Readiness: Maintain updated incident response playbooks, conduct tabletop exercises, and ensure forensic logging is enabled across critical infrastructure to accelerate investigation and containment efforts.
- Apply Network Segmentation and Least-Privilege Access: Restrict lateral movement opportunities by separating critical systems and limiting user access strictly to business requirements.

Reference:

https://www.ipsos.com/en/ipsos-announced-it-filed-complaint-regarding-breach-one-its-internal-systems

3.2 Osaki Electric: Ransomware disrupts manufacturing and shipment operations

Description

Osaki Electric Co., Ltd., a Japanese manufacturer known for smart meters and power-management solutions, disclosed that it suffered a ransomware attack that resulted in the encryption of internal servers and disruption of production-related systems. Following the discovery of the attack, the company disconnected affected systems from external networks, established an emergency response team, and suspended manufacturing and shipment operations for smart meters and other products at its Saitama R&D and Manufacturing Center and affiliated production sites. The company also launched a forensic investigation with external cybersecurity specialists and began assessing the possibility of data exfiltration.

Attack Methodology

- Unauthorized Access via VPN Infrastructure: Investigation revealed that the attackers gained access to the company's internal network through a VPN device used for remote connectivity. The threat actors successfully bypassed authentication controls and obtained access to internal systems.
- Exploitation of Accounts Without Multi-Factor Authentication (MFA): Osai Electric Co., Ltd. indicated that some VPN-connected accounts did not have MFA enabled. The attackers are believed to have conducted repeated password attempts against these accounts until successful authentication was achieved.
- Ransomware Deployment and Server Encryption: After gaining access to the network the attackers encrypted several virtual servers, disrupting critical production-related systems and forcing the shutdown of manufacturing operations.
- Potential Data Theft Prior to Encryption: During the investigation, the company became aware that information believed to originate from its internal systems had been posted on a website associated with the attackers, suggesting possible data exfiltration before ransomware deployment.

Key Takeaways

- VPN Services Remain High-Value Targets: Internet-facing VPN appliances continue to be a common entry point for ransomware operators, particularly when weak authentication controls or legacy accounts remain active.
- MFA Gaps Can Lead to Full Network Compromise: A single externally accessible account without MFA may provide attackers with a direct path into internal corporate environments, enabling lateral movement and ransomware deployment.
- Operational Technology and Manufacturing Environments Are Increasingly Targeted: Cyberattacks against production systems can result in significant business disruption, including halted manufacturing, shipment delays, and supply chain impacts.
- Data Extortion Often Accompanies Ransomware Attacks: Modern ransomware groups frequently steal information before encryption and use public leak sites as an additional pressure mechanism during extortion attempts.

Mitigation Recommendations

- Mandate MFA for All Remote Access Services**:** Enforce phishing-resistant MFA using solutions such as Microsoft Entra ID MFA, FIDO2 security keys, or Cisco Duo for all VPN, RDP, VDI, and privileged accounts.
- Harden VPN Infrastructure**:** Regularly review VPN accounts, remove dormant users, enforce strong password policies, restrict access through conditional access controls, and monitor for brute-force authentication attempts.
- Deploy Network Detection and Response (NDR)**:** Implement solutions such as Darktrace, Vectra AI, or Cisco Secure Network Analytics to identify anomalous VPN activity, lateral movement, and ransomware-related behaviours.
- Protect and Test Offline Backups**:** Maintain immutable backups using technologies such as Veeam Immutable Repositories, Rubrik, or Cohesity and routinely test restoration procedures to ensure business continuity.
- Segment Production and Corporate Networks**:** Separate manufacturing systems, OT environments, and critical production assets from corporate IT networks to reduce the impact of ransomware propagation.

- Enable Continuous Security Monitoring**:** Utilize SIEM and XDR platforms such as Microsoft Sentinel, Microsoft Defender XDR, CrowdStrike Falcon, or Google SecOps to detect credential attacks, privilege escalation, and suspicious file-encryption activity.

Reference:

https://www.osaki.co.jp/en/ir/news/auto_20261118582910/pdfFile.pdf

3.3 Equinor: Cyberattack against energy sector IT systems

Description

Equinor ASA, Norway's state-controlled energy company and one of Europe's largest natural gas suppliers, disclosed that it detected an ongoing cyberattack targeting certain internal IT systems. The incident disrupted several corporate IT services, including internal applications and email systems used by employees. Despite the intrusion, the company stated that oil and gas production, operational technology (OT) environments, and energy delivery operations remained unaffected. Equinor mobilized internal and external resources, coordinated with national security authorities, and launched containment and recovery efforts to restore affected systems. At the time of the company's updates, there was no indication that data had been stolen or altered.

Attack Methodology

- Attack Targeted Corporate IT Infrastructure: Threat actor conducted a cyberattack against specific internal IT systems within Equinor's enterprise environment. The affected systems included business applications and corporate services used by employees rather than operational technology responsible for energy production.
- Disruption of Internal Business Services: The attack resulted in disruptions to internal applications and administrative systems. Reports indicated that employees experienced difficulties accessing corporate resources, and the organization's internal email system was temporarily unavailable.
- Non-Virus-Based Intrusion: Equinor stated that the incident was not a virus attack and there was no risk of malware propagation to other systems. This suggests the attack involved a targeted compromise rather than self-spreading malware or ransomware.
- Containment and System Restoration Efforts: Following detection, the company engaged national security authorities and deployed resources to neutralize the threat, investigate affected systems, and restore full system integrity.

Key Takeaways

- Critical Infrastructure Organizations Remain Prime Targets: Energy companies continue to face persistent cyber threats due to their strategic importance and role in national and regional energy supply chains.
- Separation Between IT and OT Networks Limits Operational Impact: The attack disrupted corporate IT services but did not impact energy production, highlighting the value of network segmentation between business systems and operational technology environments.
- Business System Disruptions Can Affect Operations Without Production Outages: Even when industrial processes remain operational, the loss of email, internal applications, and administrative systems can significantly hinder business continuity and incident response activities.
- Rapid Coordination With National Cybersecurity Authorities Is Essential: Early engagement with organizations such as the Norwegian National Security Authority (NSM) enhances incident containment, forensic analysis, and recovery efforts during attacks on critical infrastructure operators.

Mitigation Recommendations

- Implement Strong IT-OT Network Segmentation: Deply industrial demilitarized zones (IDMZ), firewalls, and access controls between corporate IT networks and operational technology environments to prevent lateral movement into critical production systems.
- Adopt Zero Trust Access Controls: Utilize solutions such as Microsoft Entra ID, Palo Alto Prisma Access, or Zscaler Zero Trust Exchange to continuously verify user identities, device health, and access requests.
- Deploy Advanced Threat Detection Capabilities: Implement platforms such as Microsoft Defender XDR, CrowdStrike Falcon, or Google SecOps to identify anomalous activity, account misuse, and intrusion attempts across enterprise networks.

- Strengthen Email and Identity Security: Protect business-critical services through phishing-resistant MFA, conditional access policies, privileged access management (PAM), and continuous monitoring of authentication events.
- Conduct Regular Incident Response Exercises: Perform tabletop simulations involving IT, OT, legal, communications, and executive teams to validate cyber crisis response procedures and business continuity plans.
- Maintain Offline and Immutable Backups: Utilize platforms such as Rubrik, Cohesity, or Veeam Immutable Backup to support rapid recovery of critical business systems following cyber incidents.

Reference:

https://www.equinor.com/news/20261711-equinor-detected-cyber-attack

4. Security News

4.1 Optimizely: Malicious JavaScript injected into customer websites

Executive Summary

A significant supply chain attack targeting Optimizely's Web Experimentation platform resulted in malicious JavaScript being injected into customer website projects and distributed through Optimizely's trusted infrastructure. The compromise impacted at least 178 organizations across sectors including banking, technology, retail, media, and travel. The malicious code enabled cryptocurrency theft, payment card skimming, cookie theft, screenshot capture, and the delivery of iOS-focused exploit kits. Optimizely confirmed the incident, remediated the vulnerability, removed the injected code, and notified affected customers. The incident demonstrates the growing security risk associated with trusted third-party web services and client-side supply chain attacks.

Incident Summary

On 16 November 2026, identified malicious JavaScript embedded within customer projects hosted on Optimizely's Web Experimentation platform. The compromised code was found in 188 Optimizely scripts associated with 178 organizations, including major brands such as Zoom, BBC, CNN, Salesforce, GitLab, HSBC, and IKEA. Since the malicious content was delivered through Optimizely's legitimate content delivery network (CDN), website visitors unknowingly executed the payload while browsing affected sites. According to Optimizely, attackers exploited a vulnerability in the Experimentation account signup flow, allowing unauthorized modification of customer Project JavaScript configurations. The injected payload was designed to replace cryptocurrency wallet addresses with attacker-controlled addresses, harvest payment card information from payment forms, steal browser cookies, capture screenshots, and attempt delivery of the Coruna and DarkSword iOS exploit kits to mobile users. Researchers confirmed successful cryptocurrency theft, while the full extent of payment card and data theft remains unknown. Following discovery, Optimizely blocked the vulnerable pathway, removed the malicious code, revoked active sessions and tokens, reset affected accounts, and notified impacted customers.

Key Takeaways

- The incident represents a high-profile **client-side supply chain attack**, where trusted third-party JavaScript became the delivery mechanism for malicious code.
- Organizations were impacted without direct compromise of their own infrastructure, highlighting the security risks associated with third-party web dependencies.
- The malicious payload supported multiple objectives, including cryptocurrency theft, payment card skimming, session theft, screenshot collection, and potential malware delivery to iOS devices.
- Because the malicious JavaScript was delivered through legitimate Optimizely infrastructure and valid certificates, traditional trust mechanisms provided limited protection.
- The incident underscores the importance of third-party script governance, continuous monitoring of externally hosted JavaScript, Content Security Policy (CSP) enforcement, and vendor risk management processes.

Reference:

Optimizely Service Status

4.2 Contabo: Unauthorized access to hosting provider infrastructure

Executive Summary

Contabo, a Germany-based hosting provider offering VPS, VDS, and dedicated server services, disclosed a security incident involving unauthorized access to part of its internal infrastructure. The company detected the intrusion on 14 November 2026 and subsequently launched an investigation with external incident response and digital forensics specialists. As a precautionary measure, Contabo reset all customer VNC passwords, rotated internal credentials, blocked known access paths, and enhanced monitoring across its environment. While the company stated that there was no evidence of personal data exposure at the time of disclosure, the incident highlights the risks associated with infrastructure provider compromises and the potential impact on hosted customer environments.

Incident Summary

On 16 November 2026, Contabo publicly disclosed that it had detected unauthorized access to its systems and initiated a forensic investigation to determine the scope and impact of the incident. Subsequent investigation revealed that an unauthorized third party had access to a portion of the company's internal infrastructure between 13 November 2026 (15:29 CET) and 14 November 2026 (11:28 CET). The company stated that the unauthorized access was contained and that normal operations continued throughout the response effort. At the time of reporting, Contabo indicated that it had found no evidence of personal data leakage.

As part of its containment efforts, Contabo reset all customer VNC passwords, blocked identified access paths, rotated internal access credentials, and deployed additional monitoring and forensic controls. The company also engaged external cybersecurity specialists and notified relevant authorities in accordance with its legal and compliance obligations. Later updates indicated that a small number of instances were identified as having higher risk profiles, and affected customers were contacted directly. However, Contabo did not disclose the specific attack vector or provide evidence of direct compromise of customer servers.

Key Takeaways

- The incident involved unauthorized access to a portion of Contabo's internal infrastructure rather than a publicly confirmed compromise of customer servers.
- As a precautionary measure, Contabo reset all VNC passwords and rotated internal credentials, indicating concern that administrative access mechanisms could have been exposed during the incident.
- The company reported no confirmed evidence of personal data leakage during the investigation period.
- Customers were advised to review server activity, rotate credentials, change passwords, enable multi-factor authentication (MFA), and monitor for suspicious activity.
- The incident demonstrates how compromises affecting hosting providers can create downstream risks for organizations relying on third-party infrastructure services.

Reference:

https://help.contabo.com/en/support/solutions/articles/103000426255-potential-security-incident-of-14-november-2026

4.3 Reka: Cyberattack exposes customer travel data and triggers whatsapp fraud

Executive Summary

Reka (Swiss Travel Fund) disclosed a cyberattack that resulted in unauthorized access to customer personal information and travel booking data. The exposed information was subsequently used in highly targeted phishing campaigns conducted through WhatsApp, SMS, and email. Attackers leveraged legitimate booking details to impersonate Reka representatives and trick customers into visiting fraudulent websites designed to steal payment card information. Approximately 8,200 customers were affected. Reka has notified impacted individuals, launched a forensic investigation, strengthened security measures, and filed a criminal complaint while warning customers to remain vigilant against ongoing fraud attempts.

Incident Summary

In November 2026, Reka, a Swiss travel and holiday accommodation provider, suffered a cyberattack in which unknown threat actors gained access to customer personal information and travel reservation data. The incident came to light after numerous customers reported receiving fraudulent WhatsApp messages that referenced their actual holiday bookings. The messages contained legitimate customer details, including names, accommodation information, travel dates, and booking references, making the communications appear authentic. Investigations indicated that approximately 8,200 customers were impacted by the data exposure.

Following the breach, attackers used the stolen information to conduct highly targeted phishing campaigns. Victims received messages impersonating guest services from booked Reka holiday resorts and were instructed to verify or confirm their reservations through embedded links. These links directed users to fraudulent websites that displayed booking-related information and requested personal and payment card details under the guise of reservation validation. The attackers also applied time pressure by claiming reservations would be cancelled if confirmation was not completed within a limited timeframe. Reka stated that the method used to obtain the protected customer data remained under investigation and worked with cybersecurity specialists to determine the full scope of the attack.

Key Takeaways

- The cyberattack resulted in the exposure of customer personal information and travel booking details, affecting approximately 8,200 customers.
- Threat actors leveraged genuine booking information to conduct highly convincing phishing attacks via WhatsApp, SMS, and email.
- Fraudulent messages impersonated Reka guest services and directed victims to fake booking validation portals designed to harvest payment card information.
- The presence of accurate travel dates, accommodation details, and booking references significantly increased the credibility and effectiveness of the phishing campaign.
- Reka notified affected customers, strengthened security measures, initiated a forensic investigation, and warned users against sharing personal or financial information through unsolicited communications.

Reference:

https://reka.ch/en

Wave of WhatsApp scams affects over 8,000 Reka customers - SWI swissinfo.ch

Our Comprehensive Portfolio of Cyber Security Offerings

Service 1
SOC (Security Operation Center)

Deploying of SIEM, EDR, XDR, SOAR Technologies for Manage Detection and Response (MDR). 24x7 Incident Monitoring, Threat Intelligence & Threat Hunting, Incident Response

Service 7
Cloud Security Services

Cloud deployment, maturity assessments, migration, Securing Cloud by deploying the necessary controls



Service 6
Data Security

Data loss prevention, Data Discovery & Classification, Cyber Recovery Ransomware Strategy, Public Key Infrastructure, Data Encryption

Service 2
Enterprise Vulnerability Management

Vulnerability Management, Application Security, Penetration Testing, Red Teaming, DevSecOps

Service 5
Governance Risk and Compliance

Security Control effectiveness, identify solution to remediate risk through controls, frameworks, process and solutions, identify aplicable law and regulations and adopt industry framework & standards to meet compliance requirements

Service 3
IAM (Identity & Access Management)

Program setup & program governance, IAM strategy, architecture & roadmap, IAM maturity assessment, IAM product selection, consulting for role based access control/policy based access control strategy

Service 4
Network Security

Deploying perimeter devices like firewall, proxy, etc, implement zero trust strategy, Micro-Segmentation, Network security assessment

info.grc@crowe.ae
+971 52 373 4662
Level 21, The Prism, Business Bay, Dubai, UAE
Abu Dhabi | ADGM | DIFC | Sharjah
www.crowe.com/ae

Scan to Know more