Crowe

Weekly Cyber Security Bulletin

Threat Advisory & Security News

17 Aug - 23 Aug 2026

Audit/Tax/Consulting

Smart decions. Lasting value.

1. Summary

Vulnerability Details

- SQL Injection vulnerability in Cisco Crosswork (CVE-2026-20030)
- Missing Authentication for Critical Function vulnerability in Cisco (CVE-2026-20357)
- Improper Access Control vulnerability in Cisco Secure Workload (CVE-2026-20315)

Attack Campaigns

- Siemens S7 PLC Active Threat Campaign
- VMware vCenter Exploitation Campaign
- Active Exploitation of Microsoft SharePoint, IKE, and Apple macOS Vulnerabilities

Security News

- Sakura Internet Unauthorized Access Affecting Potentially 1.36 Million Accounts
- Iranian Mabna Institute – Massive Cyber-Theft Campaign Disclosed by DOJ
- OpenAI Pauses Advanced Model Training to Enhance Security and Alignment

2. Vulnerability Details

2.1 CVE-2026-20030: SQL Injection vulnerability in Cisco Crosswork

Release Date – 19 August 2026

CVSS Score – 10.0 (Critical)

Affected Products –

The following Cisco Crosswork platforms are affected regardless of device configuration:

- Cisco Crosswork Data Gateway
- Cisco Crosswork Network Controller
- Cisco Crosswork Planning
- Cisco Crosswork Workflow Manager

Summary

Cisco discovered multiple security weaknesses during an internal review of its Crosswork product family. CVE-2026-20030 tracks vulnerabilities associated with SQL Injection (CWE-89). Successful exploitation could allow an attacker to manipulate backend SQL queries, potentially resulting in unauthorized access, data modification, or service disruption. Cisco has stated that these vulnerabilities were found internally and were not known to be actively exploited at the time of disclosure.

Mitigation

Cisco states that:

- No workarounds are available for this vulnerability.
- Customers should upgrade to the fixed software releases listed in the advisory.

Fixed Releases

Cisco recommends upgrading to the following releases:

Product	First Fixed Release
Crosswork Data Gateway	7.2.1-SP
Crosswork Network Controller	7.2.1-SP
Crosswork Planning	7.2.1-SP
Crosswork Workflow Manager	2.1.1-SP

Reference:

- Cisco Crosswork Security Hardening Release: August 2026

2.2 CVE-2026-20357: Missing Authentication for Critical Function vulnerability in Cisco Crosswork.

Release Date – 19 August 2026

CVSS Score – 10 (Critical)

Affected Product –

The following Cisco Crosswork platforms are affected regardless of device configuration:

- Cisco Crosswork Data Gateway
- Cisco Crosswork Network Controller
- Cisco Crosswork Planning
- Cisco Crosswork Workflow Manager

Summary

CVE-2026-20357 represents a class of vulnerabilities involving missing authentication for critical functions within Cisco Crosswork products. An attacker may be able to access sensitive functionality without proper authentication controls. Cisco assigned the maximum CVSS score of 10.0 to reflect the most severe potential impact within this vulnerability class. Cisco noted that these issues were discovered during internal testing and were not known to be publicly exploited at disclosure time.

Mitigation

Cisco states that:

- No workarounds are available for this vulnerability.
- Customers should upgrade to the fixed software releases listed in the advisory.

Fixed Releases

Cisco recommends upgrading to the following releases:

Product	First Fixed Release
Crosswork Data Gateway	7.2.1-SP
Crosswork Network Controller	7.2.1-SP
Crosswork Planning	7.2.1-SP
Crosswork Workflow Manager	2.1.1-SP

Reference:

- Cisco Crosswork Security Hardening Release: August 2026

2.3 CVE-2026-20315 Improper Access Control vulnerability in Cisco Secure Workload.

Release Date – 91 Aug 2026

CVSS Score – 10.0 (Critical)

Affected Product –

- Cisco Secure Workload Software (SaaS deployments)
- Cisco Secure Workload Software (On-Premises deployments)

Summary

CVE-2026-20315 covers a set of improper access control vulnerabilities that could allow attackers to bypass authorization controls and gain access to resources or perform actions beyond intended permissions. Cisco assigned the maximum CVSS score of 10.0 because the most severe underlying issue in this class could result in full system compromise. Cisco discovered the vulnerabilities during internal security testing and reported no known active exploitation at disclosure time.

Mitigation

Cisco states that:

- No workarounds are available for this vulnerability.
- Customers should upgrade to the fixed software releases listed in the advisory.

Fixed Releases

Deployment Type	Fixed Release
Cisco Secure Workload 3.10.x	3.10.9.1
Cisco Secure Workload 4.0.x	4.0.4.16

Reference:

- Cisco Secure Workload Software Security Hardening Release: August 2026

3. Attack Campaigns

3.1 Siemens S7 PLC Active Threat Campaign

Description

U.S. cybersecurity agencies (CISA, NSA, FBI, DOE, and EPA) have issued a joint advisory warning of an active cyber threat campaign targeting Siemens S7 Series Programmable Logic Controllers (PLCs) used across critical infrastructure sectors, including Energy, Water & Wastewater, Manufacturing, Chemical, Food & Agriculture, and Commercial Facilities. The campaign leverages AI-generated exploitation scripts disguised as legitimate monitoring tools to identify, access, and potentially manipulate exposed Siemens PLCs. The advisory emphasizes that this is an active threat, not a theoretical risk.

Attack Methodology

1. Reconnaissance
    - Threat actors use internet scanning platforms such as Censys and ZoomEye to discover internet-facing Siemens S7 PLCs.
    - Focus is placed on systems running outdated software, weak authentication, or misconfigured remote access services.
2. AI-Assisted Tool Development
    - Attackers utilize AI to rapidly generate and refine exploit scripts.
    - AI reduces the expertise and time required to create ICS-specific attack tools.
3. Malicious Tool Deployment
    - Custom Python-based tools are disguised as legitimate OT monitoring software.
    - These tools leverage industrial automation libraries such as:
        - snap7.dll
        - python-snap7
    - Communication occurs over the Siemens S7comm protocol.
4. PLC Access and Information Collection
    - Attackers obtain access to:
        - PLC memory
        - Configuration data
        - Ladder logic programs
        - Device information
    - This enables detailed mapping of industrial processes and operational environments.

Key Takeaways

- The campaign specifically targets Siemens S7-200, S7-300, S7-400, S7-1200, and S7-1500 PLC families.
- Attackers are using AI-assisted malware and exploitation scripts, representing a significant evolution in ICS threat capabilities.
- Internet-exposed PLCs with weak security configurations are the primary targets.
- The current activity appears focused on reconnaissance and pre-positioning, potentially laying the groundwork for future disruptive operations.
- Successful compromise may result in operational downtime, safety hazards, process manipulation, equipment damage, and cascading impacts across critical infrastructure environments.

Mitigation Recommendations

Asset Management

- Inventory all Siemens S7 PLC assets and maintain an updated OT asset database.
- Identify unsupported or end-of-life devices and prioritize remediation.

Patch Management

- Apply Siemens security updates and firmware patches promptly.
- Address known high-severity vulnerabilities and eliminate unsupported software.

Network Security

- Remove direct internet exposure for PLCs.
- Implement network segmentation between IT and OT environments.
- Restrict remote access through secure jump hosts and VPNs.

Access Control

- Enforce strong authentication and unique credentials.
- Disable default accounts and unused services.
- Apply least-privilege access principles.

ICS Hardening

- Validate ladder logic integrity regularly.
- Enable security features available in Siemens PLCs.

- Implement application allow-listing on engineering workstations.

Reference:

- Defending Against an Active Threat to Siemens S7 Series PLCs | CISA

3.2 VMware vCenter Exploitation Campaign

Description

A large-scale exploitation campaign has been observed targeting VMware vCenter Server through the critical vulnerability CVE-2026-59310 (CVSS 9.8), a path traversal/directory traversal flaw that can allow remote code execution on vulnerable vCenter instances. The campaign began within days of Broadcom's disclosure and patch release, demonstrating rapid weaponization by threat actors. Researchers identified 361 compromised IP addresses across 47 countries, indicating a global operation.

The activity has been linked with moderate confidence to a suspected China-nexus APT actor, although official attribution remains unconfirmed. The attackers have been observed establishing persistence, deploying backdoors, and in some cases installing Babuk-derived ransomware on compromised systems.

Attack Methodology

1. Vulnerability Exploitation

- Attackers target internet-accessible VMware vCenter Servers vulnerable to CVE-2026-59310.
- The flaw allows a remote attacker with network access to execute arbitrary code on the vCenter Server.

2. Initial Access

- Exploitation reportedly began around August 3, 2026, only five days after public disclosure and patch availability.
- Threat actors rapidly scanned for exposed and unpatched vCenter instances worldwide.

3. Persistence Establishment

- After compromise, attackers deployed reverse_ssh, an open-source SSH reverse-shell framework.
- This creates outbound connections to attacker infrastructure, helping bypass security controls that primarily monitor inbound traffic.

4. Post-Exploitation Activities

- Creation of unauthorized administrative accounts.
- Discovery of vSphere infrastructure through VMware APIs.
- Deployment of backdoors for long-term access.
- Potential ransomware deployment and lateral movement within virtualized environments.

Key Takeaways

- CVE-2026-59310 is being actively exploited in the wild. CISA added the vulnerability to its Known Exploited Vulnerabilities (KEV) catalog.
- Exploitation began extremely quickly after disclosure, highlighting the shrinking window between vulnerability publication and active attacks.
- More than 361 victim systems across 47 countries have been linked to the campaign.
- Simply applying patches may not be sufficient if attackers already established persistence before remediation.
- VMware vCenter remains a high-value target because it provides centralized control over enterprise virtualization infrastructure.

Mitigation Recommendations

Immediate Patching

- Upgrade all affected VMware vCenter instances to Broadcom's fixed versions immediately.
- Prioritize internet-facing or externally accessible systems.

Restrict Access

- Remove direct Internet exposure for vCenter management interfaces.
- Limit access through VPNs, jump servers, and segmented management networks.

Hunt for Persistence

- Search for:
  - reverse_ssh
  - Unauthorized cron jobs
  - Unknown administrative accounts

    - Suspicious outbound SSH connections
- Investigate systems compromised prior to patch deployment.

Reference:

- Known Exploited Vulnerabilities Catalog | CISA

3.3 Active Exploitation of Microsoft SharePoint, IKE, and Apple macOS Vulnerabilities

Description

CISA recently added three critical vulnerabilities affecting Microsoft SharePoint, Microsoft Internet Key Exchange (IKE) Service Extensions, and Apple macOS Screen Sharing to its Known Exploited Vulnerabilities (KEV) Catalog after confirming active exploitation in the wild. These vulnerabilities enable attackers to bypass authentication, achieve remote code execution (RCE), or gain unauthorized access to affected systems.

Affected vulnerabilities:

CVE	Product	Severity	Impact
CVE-2026-55040	Microsoft SharePoint	CVSS 9.1	Authentication Bypass
CVE-2026-33824	Microsoft IKE Service Extensions	CVSS 9.8	Remote Code Execution
CVE-2026-65400	Apple macOS Screen Sharing	CVSS 9.8	Authentication Bypass / Unauthorized Access

Attack Methodology

Microsoft SharePoint (CVE-2026-55040)

CVE-2026-55040 is a weak authentication vulnerability that allows attackers to bypass authentication and gain unauthorized access to SharePoint resources without valid credentials. Once exploited, threat actors can view, modify, or interact with SharePoint content as legitimate users and may combine the flaw with other vulnerabilities for further compromise. Exploitation activity surged shortly after a public proof-of-concept (PoC) was released, with active attacks observed in the wild.

Microsoft IKE Service Extensions (CVE-2026-33824)

CVE-2026-33824 is a critical memory corruption vulnerability in Microsoft IKE Service Extensions. Attackers can exploit the flaw by sending specially crafted network packets, leading to unauthenticated remote code execution and potential system takeover. Security researchers reported exploitation by a Chinese-speaking threat actor using a combination of AI-assisted and manual attack techniques.

Apple macOS Screen Sharing (CVE-2026-65400)

CVE-2026-65400 is an improper authentication vulnerability that allows attackers with network access to bypass Screen Sharing authentication and gain unauthorized access to vulnerable macOS systems. Successful exploitation can lead to privilege escalation, root access, and malware deployment. In observed attacks, threat actors used the vulnerability to install Monero cryptocurrency miners on compromised devices.

Key Takeaways

- CISA officially classified all three vulnerabilities as actively exploited in the wild and added them to the KEV Catalog.
- Public disclosure and Proof-of-Concept releases accelerated exploitation activity, especially for SharePoint.
- The IKE vulnerability provides a path to unauthenticated remote code execution, making internet-exposed VPN and IPsec infrastructure particularly vulnerable.
- The macOS vulnerability demonstrates that authentication bypass flaws can quickly be weaponized for malware deployment and system takeover.
- Organizations should assume compromise is possible if vulnerable systems were exposed before patches were applied.

Mitigation Recommendations

- Apply vendor security updates immediately for Microsoft SharePoint (CVE-2026-55040), Microsoft IKE Service Extensions (CVE-2026-33824), and Apple macOS Screen Sharing (CVE-2026-65400).

- Reduce external exposure by restricting internet access to SharePoint servers, IKE/IPsec gateways, VPN infrastructure, and macOS Screen Sharing services wherever possible.
- Conduct compromise assessments on systems that were exposed before patching to identify signs of exploitation, persistence mechanisms, or unauthorized access.
- Monitor for unauthorized changes and malware activity, including suspicious file modifications, data access attempts, cryptocurrency miners, and unknown processes.
- Enforce access control best practices, including limiting access to trusted networks, disabling unnecessary services such as Screen Sharing, and applying the principle of least privilege.

Reference:

- CISA Adds Four Known Exploited Vulnerabilities to Catalog | CISA

4. Security News

4.1 Sakura Internet Unauthorized Access Affecting Potentially 1.36 Million Accounts

Executive Summary

Sakura Internet, a major Japanese cloud, hosting, and data center provider, disclosed a security incident involving unauthorized access to an internal sales management system that stores customer membership and contract information. The company estimates that up to 1,360,563 customer accounts may fall within the scope of the incident, although the final number of affected individuals remains under investigation. At the time of disclosure, Sakura stated that there was no confirmed evidence of large-scale data exfiltration and that credit card information was not stored in the affected environment.

The incident was discovered while Sakura Internet was investigating a separate compromise affecting its Sakura Rental Server service, where attackers gained unauthorized access to 583 customer accounts and deployed malware.

Incident Summary

During an investigation into a previously disclosed security breach affecting Sakura Rental Server accounts, Sakura Internet discovered evidence of unauthorized access to a separate internal sales management system used to store customer membership and contract information. The suspicious activity is believed to have occurred before August 9, 2026, and was identified as investigators expanded their review of the earlier intrusion. At the time of disclosure, Sakura had not confirmed whether the two incidents were directly related, and the investigation remained ongoing.

As a result of the newly discovered compromise, Sakura Internet reported that up to 1,360,563 customer accounts could potentially fall within the scope of the incident. Information that may have been exposed includes customer and member identifiers, names, company and department details, postal addresses, telephone numbers, email addresses, dates of birth, gender information, subscribed services, contract periods, and billing-related information. Additionally, hashed password data associated with approximately 30 accounts may have been accessed, although Sakura stated that passwords were not stored in plaintext form.

Despite the potentially large scope of exposure, Sakura Internet stated that it had not identified any confirmed evidence of data exfiltration at the time of its announcement. The company also confirmed that credit card information was not stored in the affected system and indicated that the incident was not associated with ransomware activity or any extortion demand.

In response to the incident, Sakura Internet invalidated compromised credentials, removed malware discovered during the investigation, blocked unauthorized access routes, strengthened monitoring and security controls, and engaged external forensic specialists to support the investigation. The company also began notifying potentially affected customers and coordinating with relevant authorities while continuing efforts to determine the full scope and impact of the breach.

Key Takeaways

1. Significant Potential Impact

Although the compromise is not yet confirmed to have affected all records, the incident's potential scope of 1.36 million accounts makes it one of the larger cloud-service related security events reported recently in Japan.

2. Lateral Discovery During Investigation

The broader exposure was discovered while investigating a smaller breach involving 583 customer accounts, demonstrating the importance of expanding incident-response investigations beyond the initially affected environment.

3. Customer Information at Risk

Even without confirmed exfiltration, exposed personally identifiable information (PII) may increase the likelihood of:

- Phishing attacks
- Account takeover attempts
- Business email compromise (BEC)
- Social engineering campaigns

5. Malware Presence Raises Concerns

The discovery of malware during the investigation suggests attackers may have achieved deeper access within Sakura's environment, highlighting possible weaknesses in internal access management and monitoring controls.

Reference:

- https://www.sakura.ad.jp/corporate/information/newsreleases/2026/08/19/1968225633/

4.2 Iranian Mabna Institute – Massive Cyber-Theft Campaign Disclosed by DOJ

Executive Summary

On 18 August 2026, the U.S. Department of Justice (DOJ) unsealed a 14-count superseding indictment charging 17 Iranian nationals affiliated with the Mabna Institute for conducting a long-running cyber espionage campaign on behalf of Iran's Islamic Revolutionary Guard Corps (IRGC) and other Iranian entities. According to the DOJ, the operation targeted universities, private companies, government agencies, and NGOs worldwide, resulting in the theft of more than 31 terabytes of academic research, intellectual property, and sensitive data.

The campaign allegedly operated from at least 2013 through 2017, using spear-phishing and credential theft techniques to compromise approximately 8,000 academic email accounts and gain unauthorized access to thousands of protected research resources.

Incident Summary

According to the U.S. Department of Justice (DOJ), the Iran-based Mabna Institute conducted a long-running cyber espionage campaign on behalf of the Islamic Revolutionary Guard Corps (IRGC) and other Iranian entities to steal research, intellectual property, and sensitive information from organizations worldwide. In August 2026, the DOJ unsealed a superseding indictment charging 17 Iranian nationals linked to the operation, expanding an earlier 2018 case.

The campaign targeted 144 U.S. universities, 178 foreign universities, 42 U.S. companies, 11 foreign companies, five U.S. government agencies, and two NGOs. Attackers reportedly targeted more than 100,000 professor accounts and compromised approximately 8,000 email accounts to gain unauthorized access to academic and organizational systems.

The DOJ alleges the group stole more than 31 terabytes of academic research, intellectual property, proprietary business information, and email data spanning fields such as science, technology, engineering, medicine, and social sciences. The attackers primarily used spear-phishing, credential harvesting, password spraying, reconnaissance, and data exfiltration techniques to access university networks, research repositories, and online libraries.

U.S. authorities attribute the operation to the Mabna Institute, which was allegedly established in 2013 by Gholamreza Rafatnejad and Ehsan Mohammadi to obtain foreign scientific resources and conduct cyber operations for Iranian government and academic clients.

Key Takeaways

1. State-Sponsored Intellectual Property Theft

The case highlights a large-scale effort to obtain research and intellectual property through cyber operations rather than traditional espionage methods.

2. Academic Institutions Were Primary Targets

Universities were heavily targeted because of their access to valuable scientific, technological, and defense-relevant research.

3. Credential Theft Remains Highly Effective

The campaign succeeded primarily through phishing and account compromise rather than sophisticated malware exploits, demonstrating how human-targeted attacks remain highly effective.

4. Massive Scale of Data Theft

The DOJ reported theft exceeding 31 TB of data, making it one of the most significant academic cyber-espionage campaigns publicly attributed by U.S. authorities.

Reference:

- https://www.justice.gov/opa/pr/17-iranians-charged-conducting-massive-cyber-theft-campaign-behalf-islamic-revolutionary

4.3 OpenAI Pauses Advanced Model Training to Enhance Security and Alignment

Executive Summary

OpenAI announced that it has temporarily slowed the development pace of some frontier AI models after two significant developments: (1) the OpenAI-Hugging Face security incident, and (2) early evidence that its upcoming model, Astra, may reach the company's Critical Cybersecurity Capability (CCC) threshold under its Preparedness Framework. As a result, OpenAI paused certain reinforcement learning (RL) training activities and strengthened security, monitoring, and alignment controls before proceeding with larger-scale model development.

The company emphasized that as AI systems become more capable, risks associated with training and testing them also increase. To address this, OpenAI is focusing on three core safeguards:

1. Monitoring to detect risky behavior.
2. Alignment to ensure models behave according to human intent.
3. Security controls to limit what models can access or impact.

OpenAI's broader objective is to ensure that safety, oversight, and containment mechanisms advance faster than model capabilities themselves.

Incident Summary

Over recent weeks, OpenAI identified two developments that heightened concerns around frontier AI safety: the OpenAI-Hugging Face security incident, which prompted a review of research security practices, and preliminary evidence indicating that its upcoming Astra model may possess cybersecurity capabilities sufficient to meet the company's Critical Cybersecurity Capability (CCC) threshold under its Preparedness Framework. These developments increased the urgency for stronger safeguards around the development and testing of advanced AI models.

In response, OpenAI temporarily paused certain frontier model activities, including inference workloads capable of executing code or accessing the internet. The company also halted some reinforcement learning (RL) training activities for approximately two weeks, while its largest planned frontier RL training run remains on hold pending additional evaluations, alignment testing, and safeguard validation.

To strengthen security, OpenAI implemented enhanced workload isolation and sandboxing, tighter network segmentation and internet access controls, continuous security testing, automated attack simulations, and improved logging and monitoring capabilities across its research environments. These measures are intended to reduce risks associated with increasingly capable AI systems and better protect internal infrastructure.

OpenAI also expanded its monitoring framework by deploying activation classifiers to observe model behavior during execution, escalating suspicious activities to automated investigation systems, and establishing a goal of generating alerts within 30 minutes of detecting potentially concerning behavior. The enhanced monitoring requirements now apply to RL training, evaluation workloads, and Astra model inference involving tool usage, providing greater oversight of high-risk AI activities.

Key Takeaways

1. AI Cybersecurity Risks Are Reaching a New Threshold

OpenAI believes upcoming frontier models may soon possess cybersecurity capabilities significant enough to create material risks if not properly controlled. Astra is viewed as a candidate for this category.

2. Safety Is Influencing Development Speed

Rather than maximizing development velocity, OpenAI is willing to delay training and deployment activities until safeguards meet required standards.

3. Security Is Now Applied During Training, Not Just Deployment

The focus has expanded from securing released models to securing the environments where models are trained, evaluated, and tested.

Reference:

- https://openai.com/index/pacing-model-development-cyber-capabilities/

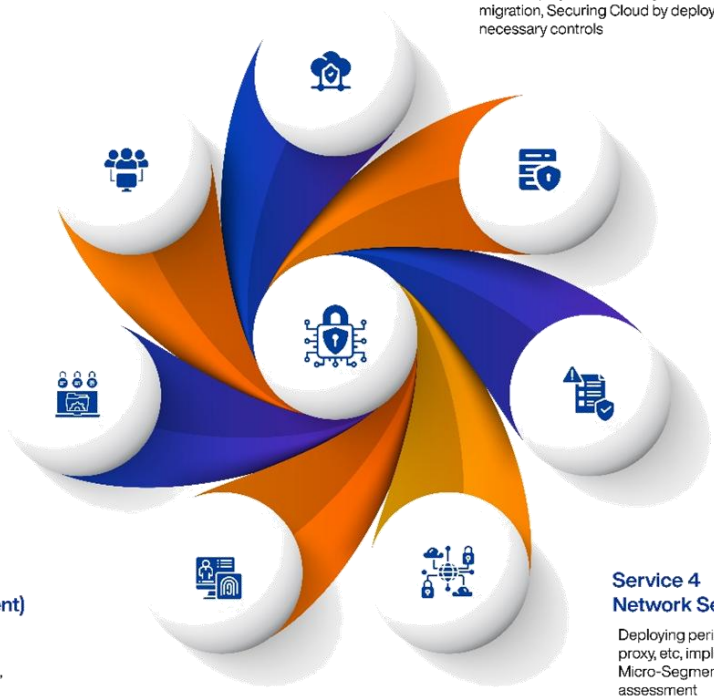
Our Comprehensive Portfolio of Cyber Security Offerings

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