XVCTEM

Continuous Threat Exposure Management (CTEM) is a proactive, five-stage framework designed to reduce the risk of cyber attacks. By systematically identifying vulnerabilities, correlating them with potential attack paths, and prioritising them based on their risk to critical assets, XVCTEM enables businesses to efficiently address exposures and enhance their security posture.

FIFTEEN

HOW DOES XVCTEM WORK?

XVCTEM conducts simulations using a lightweight software sensor that securely gathers information without affecting the host or network. This sensor creates a 'digital twin' in our database, allowing attack scenarios to be run without impacting the customer's infrastructure.

The sensors operate continuously, capturing and replicating any changes in the environment within the digital twin. Simulations involve checking conditions on all devices and performing calculations in the database. If the calculations confirm a vulnerability, we demonstrate that an attack is possible, considering user activity, misconfigurations, and vulnerabilities.

XVCTEM FEATURES

IDENTIFY ENVIRONMENTAL WEAKNESSES

Detect potential vulnerabilities in the environment that could put critical assets at risk

EXPOSE ATTACK VECTORS AND PATHS

Uncover possible attack routes towards critical assets, including lateral movement. This includes how adversaries might exploit these vulnerabilities and how automated malware, such as ransomware, could propagate through the network.

IDENTIFY PIVOT POINTS

Detect crucial hubs within the network through which most attack paths traverse

HIGHLIGHT ATTACK VECTORS

Focus on areas related to:

- Risky user activity.
- Software vulnerabilities.
- Misconfigurations or inadequate IT hygiene.

SHARED CREDENTIAL RISKS

Identify risks associated with shared or cached user credentials and passwords (both local and domain users) that could jeopardise multiple assets if leaked.

ENSURE NO INTERRUPTION OF IT OPERATIONS

Maintain seamless IT operations without impacting endpoints, performance, network, or safety.

- **Endpoints:** No user interactions, pop-ups, or warnings.
- **Performance:** No negative impact on deployed entities or performance issues.
- **Network:** Non-disruptive network transportation.
- Safety: Ensure XM Cyber operations do not adversely impact systems.

3RD PARTY INTERGRATIONS

Support for AWS, Azure-based infrastructure, as well as EDR, SIEM, and SOAR solutions.

XVCTEM Service Inclusions

INITIAL SCOPING SESSIONS

Identify critical assets and define risk scenarios.

CRITICAL ATTACK SCENARIOS

Notification and remediation steps for identified threats.

CUSTOMISED ATTACK SCENARIOS

Tailored from any starting point to any target asset.

DETAILED VISUALISATION

Comprehensive display of attacker paths to critical assets.

COMPREHENSIVE CYBERSECURITY REPORTS

Assess and report on the organization's cybersecurity status and posture.

ENVIRONMENT SETUP

Based on initial scoping.

5-DAY HYPERCARE PERIOD:

Access to consultative services to review initial outcomes and modify scenarios as needed. Includes:

- Modifying existing scenarios.
- Adding up to three new scenarios per month.

REGULAR EXECUTIVE AND TECHNICAL REPORTS

Highlight key assessments, remediation steps, and next steps.

REGULAR CUSTOMER SERVICE MANAGER (CSM) REVIEWS

Include :

- Report presentation.
- Incident identification and posture changes.
- Review of current configuration and options for change.
- Review of current functionality and additional products to enhance security posture.
- Review of last period MACs.
- Discussion of relevant upcoming customer events.
- Cadence based on customer size:
  - 25–50 sensors: every 6 months.
  - 50–150 sensors: quarterly.
  - 150–500+ sensors: monthly.

REAL-TIME EVENT NOTIFICATIONS

Immediate alerts for detected events such as password compromises, data loss detection, and malware, or any actions violating policy.

Why **XVCTEM** for CTEM?

Enhance your cybersecurity strategy with the XVCTEM team's professional services. We partner with you to deploy and customise solutions tailored to your customers' needs, defining and assessing critical attack profiles.

Working alongside you and your customers, the XVCTEM team delivers in-depth analysis and actionable recommendations to elevate your customers' cybersecurity posture.

Our XVCTEM service includes ongoing monitoring to continuously evaluate and report on cybersecurity status. Available on a monthly or per-annum basis, this service provides a comprehensive view of the cybersecurity environment, along with expert support to address any issues. Upgrade to continuous monitoring for enhanced protection.

Choose XVCTEM for continuous monitoring and benefit from regular reviews by our team, ensuring the best possible outcomes for your customers' environments. Monthly reporting and periodic assessments are standard features of the XVCTEM service, offering you peace of mind and proactive cybersecurity management.

FIFTEEN