visium ANALYTICS

Visium Technologies, Inc.

Empower Your Security Analysts and Executives with TruContext and Tru-AI

CONTACT:
We Source It 4 U Ltd
84B Roberts Street, Port of Spain
1 (868) 686-9447
wesourceit4ultd@gmail.com
wesourceit4u.com

Revolutionizing Cybersecurity with AI-Powered Insights

- In today's fast-paced digital world, security analysts are overwhelmed by vast amounts of data, while C-suite executives struggle to gain meaningful insights into cybersecurity risks.

- TruContext from Visium Technologies bridges this gap by providing an AI-driven, real-time cybersecurity platform that empowers both technical teams and business leaders with actionable intelligence.

visium ANALYTICS

For Security Analysts:

Simplify Threat Detection & Response

- **All Your Data, One Comprehensive View:** TruContext integrates **any and all data sources** into a single, intuitive dashboard. No more siloed information—just clear, real-time visibility.
- **AI-Powered Analysis:** Detect and respond to threats faster with AI-driven correlation and anomaly detection.
- **Automated Response:** Reduce manual workload with intelligent automation that prioritizes and mitigates threats instantly.
- **Real-Time Insights**: Gain a contextualized, 360-degree view of security incidents to **act immediately** and minimize damage.

visium ANALYTICS

For C-Suite Executives:

Clarity & Control Over Cyber Risks

- **Business-Centric Cybersecurity Insights:** Easily understand security risks with high-level dashboards tailored for executive decision-making.
- **Compliance & Risk Management:** Stay ahead of regulatory requirements with comprehensive reporting and risk assessment tools.
- **Reduced Operational Costs:** Improve security efficiency, reduce false positives, and lower costs through AI-driven automation.
- **Proactive Security Posture:** Move beyond reactive defense and **adopt a proactive cybersecurity strategy** that protects business continuity.

visium ANALYTICS

Tru-Context Verticals:

Financial Institutions: Banks, investment firms, and insurance companies require robust cybersecurity measures to protect sensitive financial data and prevent fraud.	**Telecommunications Companies:** Providers of communication services need to secure their networks against intrusions and data breaches.
Healthcare Organizations: Hospitals, clinics, and healthcare networks need to safeguard patient information and comply with regulations like HIPAA.	**Retail Corporations:** Large retail chains process significant customer data and payment information, necessitating strong cybersecurity measures.
Critical Infrastructure Operators: Companies managing utilities, energy grids, and transportation systems must protect their networks from cyber attacks that could disrupt services.	**Manufacturing Firms:** Companies in this sector are increasingly adopting IoT technologies, making them vulnerable to cyber attacks on their operational technologies.
Government Agencies: Federal, state, and local government bodies are prime targets for cyber threats and can benefit from enhanced situational awareness.	**Law Enforcement Agencies:** Police departments and investigative bodies require tools to analyze and visualize data for criminal investigations.
Educational Institutions: Universities and research centers handle vast amounts of sensitive data and require advanced cybersecurity solutions.	**Supply Chain and Logistics Companies:** Organizations managing complex supply chains need to protect their data and ensure the integrity of their operations.

visium ANALYTICS

Why Choose TruContext?

✅ **XDR & SIEM Integration:** Unify extended detection & response (XDR) with security information & event management (SIEM) for unparalleled network security.
✅ **AI-Powered Decision Making:** Let machine learning handle complex analysis, so your team can focus on strategic tasks.
✅ **Scalability & Flexibility:** Whether you're a small business or an enterprise, TruContext adapts to your needs.
✅ **Fast, Efficient, and Reliable:** Less effort, more impact—TruContext makes cybersecurity simpler and more effective.

Take Action Today

- 🔷 **Request a Demo** and see how TruContext can transform your cybersecurity strategy.
- 🔷 **Talk to Our Experts** to learn how TruContext fits your organization's needs.
- 🔷 **Stay Ahead of Threats**—Don't wait for a cyber incident to take action. Secure your enterprise now!

🚀 **TruContext: The AI-Driven Cybersecurity Platform That Works for You!**

visium ANALYTICS

Identity and Access Management:

When applied to **Identity and Access Management (IAM)**, TruContext can significantly improve an organization's ability to monitor, analyze, and enforce security policies by leveraging advanced data correlation, visualization, and threat detection capabi

- **Key Applications of TruContext in IAM:**

1. **Context-Aware Access Controls:**
    1. TruContext can **ingest and analyze identity-related data** from multiple sources (Active Directory, SSO logs, authentication logs, etc.) and correlate it with network activity to determine **risk-based access policies**.
    2. It enables **adaptive authentication**, where access rights adjust dynamically based on **user behavior, location, and device context**.
2. **Anomalous Behavior Detection & Threat Prevention:**
    1. By continuously monitoring **user access patterns** and comparing them to baselines, TruContext can detect **anomalies** (e.g., logins from unusual locations, excessive access requests, privilege escalations).
    2. Suspicious activities trigger **real-time alerts** or automated remediation, such as **multi-factor authentication enforcement** or session termination.
3. **Privilege Access Monitoring & Least Privilege Enforcement:**
    1. TruContext helps enforce **least privilege access** by visualizing and analyzing **privileged user activities** across an organization.
    2. It identifies **unnecessary or risky permissions**, helping security teams **right-size access levels** and prevent privilege creep.
4. **Insider Threat Detection & Risk Scoring:**
    1. By mapping out **user behaviors, asset interactions, and security events**, TruContext assigns **risk scores** to identities based on their activity.
    2. High-risk users (e.g., those accessing sensitive data irregularly) can be flagged for **enhanced monitoring or additional security controls**.
5. **Regulatory Compliance & Audit Readiness:**
    1. IAM compliance with regulations like **NIST, GDPR, CMMC, and SOC 2** is simplified through TruContext's ability to provide **audit trails and automated reporting**.
    2. Security teams can **quickly investigate access violations** and produce **clear visual reports** for auditors.
6. **Zero Trust Architecture Enablement:**
    1. TruContext supports **Zero Trust Security** by ensuring continuous **verification of identities, devices, and behaviors** before granting access.
    2. Integrating with IAM solutions, it ensures that **no implicit trust** is given based on static credentials alone.

Risk, Vulnerability, and Patch Management:

- TruContext enhances Risk, Vulnerability, and Patch Management by providing **context-driven intelligence, real-time threat correlation, and automated risk prioritization**. By **visualizing attack paths, integrating threat intelligence, and streamlining patching efforts**, TruContext **reduces exposure, improves security operations efficiency, and ensures compliance** with evolving cybersecurity standards.
- **1. Comprehensive Risk Analysis & Prioritization**
- **Contextual Risk Scoring:** TruContext correlates vulnerability data with **asset criticality, threat intelligence, and real-world exploitability** to provide **risk-based prioritization** of security issues.
- **Attack Surface Visualization:** By mapping vulnerabilities to **network architecture, user behaviors, and threat actor tactics**, TruContext helps security teams **identify high-risk attack paths** before they can be exploited.
- **2. Advanced Vulnerability Detection & Correlation**
- **Cross-Domain Vulnerability Insights:** TruContext aggregates data from **vulnerability scanners, endpoint security, cloud services, and network logs** to provide a **unified view** of an organization's security posture.
- **Threat Intelligence Integration:** By correlating vulnerabilities with **real-world attack patterns** (MITRE ATT&CK, CVE databases, SIEM alerts), TruContext identifies **actively exploited weaknesses** that need urgent remediation.
- **Zero-Day Threat Monitoring:** Machine learning models detect **abnormal system behaviors** and **suspicious activity patterns**, helping uncover potential **zero-day vulnerabilities** before an official patch is available.

visium ANALYTICS

Risk, Vulnerability, and Patch Management continued:

- **3. Patch Management Optimization & Automation**
- **Patch Prioritization Based on Real-World Threats:** TruContext helps organizations **determine which patches are most critical** by assessing the **likelihood of exploitation, asset importance, and operational impact**.
- **Automated Patch Impact Analysis:** Before deploying patches, TruContext **simulates potential system disruptions**, helping IT teams avoid **unexpected downtime** or conflicts.
- **Continuous Patch Validation:** The platform monitors **patched systems for anomalies**, ensuring successful remediation and **detecting potential rollback scenarios** caused by improper updates.
- **4. Compliance & Regulatory Alignment**
- **Real-Time Compliance Monitoring:** TruContext helps organizations maintain compliance with **NIST, CISA, ISO 27001, HIPAA, and other security frameworks** by **tracking patch status, vulnerability remediation, and risk levels**.
- **Automated Audit Reporting:** By providing **visual evidence of risk mitigation efforts**, TruContext simplifies **audit preparation** and reduces the time required for compliance assessments.
- **5. Threat Hunting & Proactive Risk Mitigation**
- **Predictive Threat Analysis:** TruContext uses AI-driven models to predict **which vulnerabilities are likely to be exploited** based on **emerging threat intelligence**.
- **Proactive Incident Response:** If a vulnerability is detected in a **critical system**, TruContext enables **automated containment actions** (e.g., isolating affected endpoints or enforcing stricter access controls) before an attack can spread.

visium ANALYTICS

Data and Software Security

Data Security: Protecting Sensitive Information

◆ Data Classification & Contextual Protection

- TruContext analyzes **data flows, access patterns, and usage behavior** to identify and classify **sensitive data** (e.g., PII, intellectual property, financial records).
- It enforces **context-driven security controls**, ensuring **only authorized users and systems** access critical data.

◆ Anomalous Data Access & Insider Threat Detection

- By **monitoring file movements, access logs, and data transfers**, TruContext detects **unauthorized or suspicious activities**, such as **data exfiltration attempts**.
- AI-driven **behavioral analytics** can flag **insider threats** (e.g., employees accessing sensitive files outside of normal behavior patterns).

◆ Data Loss Prevention (DLP) & Compliance Alignment

- TruContext integrates with **DLP tools and cloud storage** to **prevent accidental or malicious data leakage**.
- Helps ensure **GDPR, CMMC, HIPAA, and NIST compliance** by providing **real-time monitoring and automated audit reports** for data protection policies.

visium ANALYTICS

Data and Software Security, continued

Software Security: Secure Development & Application Protection

Software Supply Chain Security & Code Integrity

- TruContext **correlates software dependencies, build environments, and third-party libraries** to identify **vulnerabilities, malware injections, or compromised components.**
- It ensures **secure software development** by **tracing code integrity** across repositories and deployment pipelines.

Vulnerability Detection & Exploit Prevention

- By **mapping software vulnerabilities (CVEs) to real-time threat intelligence**, TruContext **prioritizes critical fixes** for applications, reducing exposure.
- It helps security teams **identify zero-day risks** by detecting **suspicious software behaviors, privilege escalations, or unexpected API calls.**

DevSecOps & CI/CD Security Integration

- TruContext integrates with **CI/CD pipelines, scanning code repositories and containerized environments** to **enforce secure coding practices.**
- It enables **real-time security monitoring in software development**, ensuring **vulnerabilities are caught before deployment.**

Runtime Application Security & API Monitoring

- TruContext monitors **live applications, APIs, and microservices** for **anomalous behavior, unauthorized access, or injected threats.**
- Helps prevent **API abuse, unauthorized data requests, and application-layer attacks** in real time.

visium ANALYTICS

Data and Software Security, continued

- **Threat Hunting & Incident Response for Data & Software Security**
- **🔷 Proactive Threat Intelligence & Attack Path Visualization**
- **TruContext maps out cyber threats** using frameworks like **MITRE ATT&CK** to **visualize potential attack paths** targeting data and software.
- By correlating **network telemetry, application logs, and identity data**, it detects **emerging threats before they escalate**.
- **🔷 Automated Incident Response & Remediation**
- If a security breach is detected, TruContext can **automate response actions** such as:
  - ✅ **Blocking malicious traffic**
  - ✅ **Isolating compromised applications**
  - ✅ **Forcing re-authentication for suspicious users**
- Reduces response time and mitigates **data theft or software exploits** before damage occurs.

TruContext enhances **Data and Software Security** by providing **real-time threat correlation, automated risk prioritization, and deep contextual visibility** across **sensitive data, applications, and development environments**. By integrating with **DevSecOps, SIEMs, and identity management systems**, it **fortifies an organization's digital ecosystem against evolving cyber threats**.

visium ANALYTICS

Threat Detection and Response

- Visium Technologies' **TruContext** platform enhances **Threat Detection and Response (TDR)** by leveraging **real-time analytics, AI-driven correlation, and advanced threat visualization** to provide **deep security insights, rapid detection, and automated remediation**.
- 🔹 **Real-Time Threat Intelligence Correlation**
- TruContext **ingests and correlates data** from SIEMs, firewalls, EDRs, identity systems, and cloud platforms.
- It maps **security events to frameworks like MITRE ATT&CK**, identifying known **attack techniques, tactics, and procedures (TTPs)**.
- 🔹 **Behavioral Analytics & Anomaly Detection**
- AI-driven analytics establish **baselines of normal behavior** across **users, devices, applications, and networks**.
- Detects **anomalous activities** (e.g., **lateral movement, unusual logins, privilege escalations**) indicative of an attack.
- 🔹 **Threat Prioritization with Context-Aware Insights**
- Security alerts are enriched with **contextual intelligence**—correlating indicators of compromise (IOCs) with real-world attack patterns.
- **Risk-based scoring** helps security teams **focus on the most critical threats** instead of drowning in alert fatigue.

visium ANALYTICS

Threat Detection and Response , continued

- **Proactive Threat Hunting & Incident Investigation**
- 🔷 **Attack Path Visualization & Threat Mapping**
- TruContext **creates dynamic attack path visualizations**, allowing security teams to **see how an attack is unfolding**.
- By **mapping vulnerabilities, compromised assets, and threat actor movements**, it enables **proactive containment** before escalation.
- 🔷 **Threat Hunting with AI-Powered Contextualization**
- Security teams can perform **hypothesis-driven threat hunting**, querying security logs and forensic data using **natural language-based searches**.
- TruContext **automates data correlation**, identifying **hidden patterns or stealthy attacks** that traditional rule-based security tools miss.
- 🔷 **Insider Threat Detection & Credential Abuse Prevention**
- By monitoring **identity behaviors**, TruContext flags **unusual access patterns**, such as:
  - ✅ **A user suddenly accessing high-value assets**
  - ✅ **Repeated failed logins from a critical account**
  - ✅ **Access attempts from risky geolocations or new devices**

visium ANALYTICS

Threat Detection and Response , continued

- **Rapid Threat Response & Automated Remediation**
- **🔷 Automated Incident Response Playbooks**
- TruContext integrates with **SOAR platforms** to trigger **automated response actions** based on risk level, such as:
  - ✅ **Isolating compromised endpoints**
  - ✅ **Blocking malicious IPs in firewalls**
  - ✅ **Forcing multi-factor authentication for suspicious accounts**
- **🔷 Adaptive Security Controls & Zero Trust Enforcement**
- Enforces **real-time policy changes** based on threat intelligence (e.g., **restricting access to critical systems when a risk threshold is exceeded**).
- Supports **Zero Trust Security** by continuously verifying **identity, device health, and behavioral context** before granting access.
- **🔷 Incident Forensics & Root Cause Analysis**
- TruContext provides **visual timeline reconstructions** of incidents, showing:
  - ✅ **Where the attack originated**
  - ✅ **How it spread**
  - ✅ **What data or systems were impacted**
- This accelerates root cause analysis and prevents repeat attacks.

visium ANALYTICS

Threat Detection and Response, continued

- Compliance & Regulatory Alignment
- 🔷 Automated Compliance Monitoring & Reporting
- TruContext helps organizations stay compliant with **NIST, CMMC, GDPR, and SOC 2** by ensuring:

  ✅ **Threat monitoring and logging**
  ✅ **Audit trails of security events**
  ✅ **Proactive security policy enforcement**

TruContext enhances **Threat Detection and Response** by **correlating security data, visualizing attack paths, automating response actions, and providing deep forensic insights**. Its **AI-driven analytics and real-time threat intelligence** empower security teams to **detect, investigate, and neutralize cyber threats faster** than ever before.

visium ANALYTICS

TruContext and SOAR

TruContext is a **real-time cybersecurity analytics and visualization platform** that enhances **SOAR (Security Orchestration, Automation, and Response)** by providing **deep contextual intelligence, advanced threat correlation, and *automated incident response capabilities***.

- When integrated with a **SOAR solution**, TruContext empowers security teams by:

✅ **Enhancing threat intelligence correlation**
✅ **Automating incident response with enriched data**
✅ **Reducing false positives through contextual analysis**
✅ **Providing clear attack path visualization for rapid decision-making**

visium ANALYTICS

TruContext and SOAR , continued

Enhancing Threat Intelligence & Correlation

Aggregating & Contextualizing Security Data

- TruContext **ingests security telemetry** from multiple sources (SIEM, firewalls, EDR, cloud security logs, IAM systems, etc.).
- It **correlates disparate alerts**, identifying relationships between security events and **providing a holistic threat picture.**

Real-Time Threat Mapping & Prioritization

- By integrating with **MITRE ATT&CK** and threat intelligence feeds, TruContext assigns **risk scores** to incidents based on real-world attack techniques.

- Helps SOAR systems **focus on high-priority threats**, reducing alert fatigue.

visium ANALYTICS

TruContext and SOAR , continued

Automating Incident Response & Threat Mitigation

Triggering Automated Playbooks

- When TruContext detects a high-risk anomaly, it **triggers predefined SOAR workflows** for:
  - ✅ **Blocking malicious IPs and domains**
  - ✅ **Isolating compromised devices**
  - ✅ **Enforcing multi-factor authentication (MFA) for suspicious logins**
  - ✅ **Revoking privileged access for compromised accounts**

Dynamic Security Policy Adjustments

- TruContext enables **adaptive security controls** by automatically **modifying firewall rules, access policies, and endpoint security settings** based on real-time threat intelligence.

- Supports **Zero Trust enforcement**, ensuring **continuous authentication and access monitoring**.

visium ANALYTICS

TruContext and SOAR , continued

Threat Hunting & Forensic Investigations

🔷 Attack Path Visualization & Root Cause Analysis

- TruContext provides **interactive attack path visualization**, allowing analysts to **trace how an attack evolved** across the network.
- Helps SOAR playbooks **contain threats faster** by identifying:
  - ✅ **Initial entry points**
  - ✅ **Lateral movement tactics**
  - ✅ **Compromised assets & data exfiltration attempts**

🔷 Automated Threat Hunting & IOC Matching

- Security teams can **automate threat-hunting queries** using TruContext's **context-aware analysis** to detect:
  - ✅ **Unusual credential use**
  - ✅ **Suspicious privilege escalations**
  - ✅ **Potential insider threats**

visium ANALYTICS

TruContext and SOAR , continued

Compliance & Reporting Automation

◆ Automated Compliance Reporting

- TruContext integrates with SOAR platforms to generate **real-time compliance reports** aligned with **NIST, CMMC, GDPR, and SOC 2** requirements.
- Ensures organizations maintain **continuous security monitoring and documentation** for audits.

◆ Incident Documentation & Post-Mortem Analysis

After a security event, TruContext provides **visual reconstructions** of incidents, **helping SOC teams refine their response strategies**.

When paired with a **SOAR platform**, TruContext **enhances automation, reduces response times, and improves situational awareness** through its **context-driven threat intelligence and attack path visualization**.

visium ANALYTICS