WHY USE CCS INTSIGHTS DARK MARKET SCANNING (DMS)?

The growing threat landscape means more tasks cybersecurity teams must attend to in order to maintain protection for their organizations. IntSights simplifies phishing detection, brand protection, dark web monitoring and more.

PHISHING DETECTION - IT'S SIMPLE AND IT WORKS

Phishing is popular among attackers because it's simple and it works. There are, however, proactive measures organizations can take to cut off these attacks before they can cause damage.

WHY CHOOSE US?

IntSights' automatically scans the surface, deep and dark web to uncover signs of targeted phishing attacks in the making. Continuous alerting and intelligence about fake domains with names similar to your brands and companies.

DOMAIN IDENTIFICATION - Continuous alerting and intelligence about fake domains with names similar to your brands and companies.

TAKEDOWN - External threat takedown capabilities let you quickly dispatch the fake site to eliminate the risk.

VULNERABILITY PRIORITIZATION - PATCH WITH A PURPOSE

Given how fast the threat landscape grows and changes, manually correlating threat and exploit data to vulnerabilities is no longer a viable strategy.

WHY CHOOSE US?

IntSights collects vulnerability data from a range of sources and analyses it in real-time to deliver contextual, tailored threat intelligence.

AUTOMATED, REAL-TIME ASSESSMENTS - IntSights identifies the risk, urgency, and potential impact of exploits to your organization's specific vulnerabilities.

PRIORITIZED PATCHING - By automating inefficient manual processes, IntSights brings new clarity, accuracy and effectiveness to vulnerability prioritization.

DARK WEB MONITORING - PROACTIVE DEFENSE

Attackers often tip their hands by doing things on the surface and dark web like scouting targets, using suspicious tools, and collaborating with other hackers.

Attackers often tip their hands by doing things on the surface and dark web like scouting targets, using suspicious tools, and collaborating with other hackers.

WHY CHOOSE US?

IntSights watches for signs of pending attacks against our customers' organizations.

AUTOMATED RECONNAISSANCE - Continuous scanning and sophisticated data mining and machine learning techniques aggregate and analyse a wide range of information gained from forums, advertisements, and paste bins.

TAILORED INTELLIGENCE & DEFENSE - Actionable information about validated threats that pose risk to your assets drives automated updates of perimeter devices, triggers notifications to employees and customers, and informs vulnerability patching.

BRAND PROTECTION - SECURE THE NAME

It takes lots of time, effort, and money to create a brand and build brand equity. That's what makes it so valuable – and so popular as targets for hackers.

WHY CHOOSE US?

CONTINUOUS MONITORING - Real-time scanning of external sources detect tampering that could negatively affect your organization's reputation. This includes your organization's domains, IP addresses, mobile applications, and social media pages.

OPERATIONAL AWARENESS - Share continuous risk alerts with other departments including compliance, IT, public affairs, legal, R&D, fraud and HR to manage and eliminate risks to partners, employees, customers and brand.

THREAT INVESTIGATION & RESPONSE

In any adversarial situation, it's critical to study and know your enemy.

FRAUD DETECTION - MITIGATE RISK

Most organizations have a range of IT security tools in place, such as firewalls, gateways, IDS/IPS, and malware detection systems. With these tougher defense-in-depth measures to beat, many hackers now use fraud instead.

WHY CHOOSE US?

IntSights delivers a unique approach to fraud detection.

CREDENTIAL LEAKAGE IDENTIFICATION - Find data stolen in fraud schemes and criminal attempts to sell those items on the black market such as social security numbers, credit card or bank account numbers of your employees and customers.

REAL-TIME ALERTING - Quickly notify employees and customers, update accounts, and build better fraud prevention into internal systems and processes.

ROGUE & FAKE MOBILE APP DETECTION - APPLICATION SECURITY

With users handling more and more of their daily activities via their smartphones and tablets, devices have become prime targets of hackers, and rogue mobile applications are becoming a preferred attack strategy.

WHY CHOOSE US?

IntSights' rigorous scanning of the deep and dark web uncovers malicious impersonation of our customers' brands and business, and can quickly detect when rogue or fake mobile apps are made available in major app stores.

AUTOMATED DETECTION - Surface, deep and dark web scanning capabilities identify suspicious applications, provide detailed forensic data, and enable rapid investigation and analysis.

TAKEDOWN - Eliminate malicious and rogue applications quickly via IntSights' partnerships with app stores to mitigate risks to application users and their sensitive data.

VIP PROTECTION - EXECUTIVE SECURITY

Organizations need to worry about cybersecurity for other senior people associated with their businesses, including investors, board members, and advisors.

WHY CHOOSE US?

IntSights helps protect the digital personas of our customers senior executives, board members and other VIPs.

CUSTOMIZED MONITORING - Continuous, customized scanning of a wide range of online sources, including email and social media sites, ensures real-time notification of criminal attempts to spoof executive personas.

PRIORITIZED REMEDIATION - Automated and human-driven mitigation capabilities quickly and effectively mitigate threats to executive online identities.

EXTERNAL THREAT MITIGATION - TAKEDOWN FAKE DOMAINS AND APPS

Enterprise organizations need a more efficient way to monitor the online places where these attacks are formulated, as well as more targeted and decisive ways to take down external threats once they've been identified.

WHY CHOOSE US?

IntSights continuously scans the surface, deep and dark web to identify malicious attempts to scam customers, employees and partners using illegitimate social media campaigns, app stores and spoofed websites.

OPERATIONAL AWARENESS - Visibility of fraudulent domains, fake mobile apps or social media pages, or any number of other illicit online activities.

RAPID RESPONSE - Detailed attack development timelines provide the required evidence to confirm malicious activities and engage with domain registrars, app stores, and search engines.

TAKEDOWN - Automated and analyst-driven threat takedown capabilities let organizations quickly dispatch the external threat to eliminate the risk.

INTERNAL RISK REMEDIATION - INTEGRATED PROTECTION

The challenge for security teams is the time it takes to update their existing security devices to protect employees from hackers targeted attempts to exploit them.

WHY CHOOSE US?

IntSights delivers intelligence and automation that mitigates risk and streamlines security processes.

TAILORED INTELLIGENCE - Continuous, tailored surface, deep and dark web monitoring drives real-time alerting to the presence of employee target lists, suspicious domains, phishing campaigns, and leaked credentials.

SECURITY AUTOMATION - Pre-built connectors and API-level integration with a wide range of security devices enables automation of the time-consuming and mundane task required to update in-place security devices.

RESOURCE EFFICIENCY - With updates automated, cybersecurity professionals gain the time they need to focus on more strategic security concerns.

IOC PRIORITIZATION - FOCUS ON RELEVANT THREATS

While data and threat feeds can certainly contain valuable security intelligence, these feeds create major challenges for cybersecurity professionals. There's certainly no shortage of threat information available today – data and threat feeds of all kinds from all types of sources many of which are low- or no-cost. While they can contain valuable security intelligence, these feeds require deeper analysis and processing.

WHY CHOOSE US?

IntSights changes this dynamic to deliver prioritized, tailored and actionable intelligence.

AGGREGATION - Tailored intelligence, generic third-party feeds, and data supplied from existing security devices is gathered and organized.

ENRICHMENT - Customized threat profiles and filters are added to identify valuable elements and provide context for generic threat intelligence feeds.

PRIORITIZATION - Threats are categorized and ranked based on relevance and severity to guide focused response, investigation, and mitigation.

CREDENTIAL LEAKAGE - MONITOR PROTECTED ACCESS

The easiest and most effective way for any criminal to succeed is with direct, credentialed access. Stolen credentials may be used in order to infiltrate a company's systems. The easiest and most effective way for any criminal to succeed is with direct, credentialed access to protected systems. Stolen emails and passwords are some of the most valued information on the dark web, and unfortunately social-engineering campaigns and gaps in security processes leave them exposed and easily attainable.

WHY CHOOSE US?

IntSights shines a light on data leaks and provides near real-time notification of credential leakage incidents.

TAILORED INTELLIGENCE - Continuous surface, deep and dark web monitoring of applications types, keywords, domains, IPs, and employee names.

REAL-TIME ALERTING - Automate employee and security team notification of compromised credentials with instructions for immediate password change.

ACTIVE DIRECTORY INTEGRATION - Direct integration with Active Directory can be configured to force credential updates upon new log-in attempts to ensure threat mediation and employee protection.

IN SUMMARY

Dark Market Scanning Cyber Security Maturity Benefits

Our DMS provides benefits across the organisation in terms of leadership and governance, people, information risk management, business continuity and crisis management, operations and technology, legal and compliance.

Specifically, our DMS provides the following benefits …

Leadership & Governance

- Reduce risk across the broader operating environment
- Improve operations across the Client environment
- Enhanced governance
- Reduced Project risk
- Migration towards a proactive state of readiness

People

- Removal or remediation of threats against the Client workforce
- Removal or remediation of threats against the Client Executive and Board
- Improved education programs
- More aware and cybersafe workforce
- Safer “work from home” practices leading to a more flexible workforce model
- Enhanced 3rd Party Risk Assurance
- Reduction of 3rd Party Risk

Information Risk Management

- Early identification of threats
- Proactive and more immediate remediation
- Protection of the Client brand
- Harm minimisation
- Risk reduction
- Enhanced state of readiness and response
- Reduction of breach costs
- Assist procurement in acquisition of safer equipment
- Improved business decision making
- Enhanced influence across the business

Business Continuity & Crisis Management

- Improved Incident Response
- Reduction of harm
- Reduction of business interruption
- Faster breach response time
- Enhanced business continuity
- Enhanced executive engagement
- Enhanced executive awareness
- Regular risk briefings to executive & board

Operations and Technology

- Advanced warning of vulnerabilities
- Advanced warning of possible or impending attacks
- Enhanced maturity level of operations

Legal and Compliance

- Compliant state
- Reduction of risk for the Client Brand
- Improved response processes
- Argument for cyber insurance policy cost reduction

CCS – Cultural Cyber Security Pty Ltd
www.cultural cybersecurity.com
James Carlopio – 0488 028 054
jcarlopio@culturalcybersecurity.com