TRAPX SECURITY

Threatscape

SOLUTION DATASHEET

DeceptionGrid™ 6.3

DeceptionGrid - A Powerful Defense for Advanced Threats.

In today's environment, the question isn't whether or not attackers will penetrate your cloud, data-center or user networks, but when and how often. Attackers are using increasingly sophisticated techniques to penetrate the most complex perimeter and endpoint defenses. Lack of effective detection causes dwell time which creates serious damage to your organization. **"Today, the average amount of time required to identify a data breach is 197 days. Companies that are able to contain a breach in less than 30 days can save more than one million dollars compared to those that take more than 30 days."**[1]

How can you get visibility and identify breaches quickly? How can you know what the attacker's intentions are? What are their tactics and techniques? How quickly can you stop an attack and return to normal operations? TrapX DeceptionGrid addresses these important questions with powerful technology to help you deceive, detect and defeat even the most sophisticated cyber attackers.

DeceptionGrid dynamically baits, engages, and traps attackers across all areas of the network.

DeceptionGrid Traps appear identical in every way to your real operational IT assets and your connected Internet of Things (IoT) devices. When cyber attackers penetrate an enterprise network, they perform reconnaissance to enumerate network assets and then move laterally to compromise these high-value targets. DeceptionGrid dynamically deceives, detects and defeats attackers across all areas of the network and at every stage of their attack. Just one touch of the DeceptionGrid by the attacker sets off a high-confidence alert. DeceptionGrid integrates with key elements of the network and security ecosystem to contain attacks and enable a return to normal operations.

DeceptionGrid 6.3 brings powerful automation and ease-of-use suitable for even the largest enterprise. DeceptionGrid is able to quickly discover the network and build Traps (decoys) that exactly match your user, data-center and even IoT assets. Our automation then orchestrates the deployment of Tokens (lures), medium and high-interaction Traps throughout your networks.

1 Global study based on 500 interviews conducted by The Ponemon Institute on behalf of IBM.

The New Features In DeceptionGrid 6.3

Artificial Users

Traps (decoys) are now smarter than ever; they can now mimic user activities, while acting like real exploited users. This gives attackers a false sense of a successful attack – when in reality they're only interacting with an artificial user inside a sophisticated cyber trap. This new cyber trap ultimately exposes hackers and their latest tactics in a safe environment while keeping the organization's real users and network fully secure.

Hacker Tracker

Hackers can no longer remain hidden with DeceptionGrid's Hacker Tracker capabilities. DeceptionGrid is now able to track hackers back to their command and control locations by tracking deceptive files accessed from outside the network.

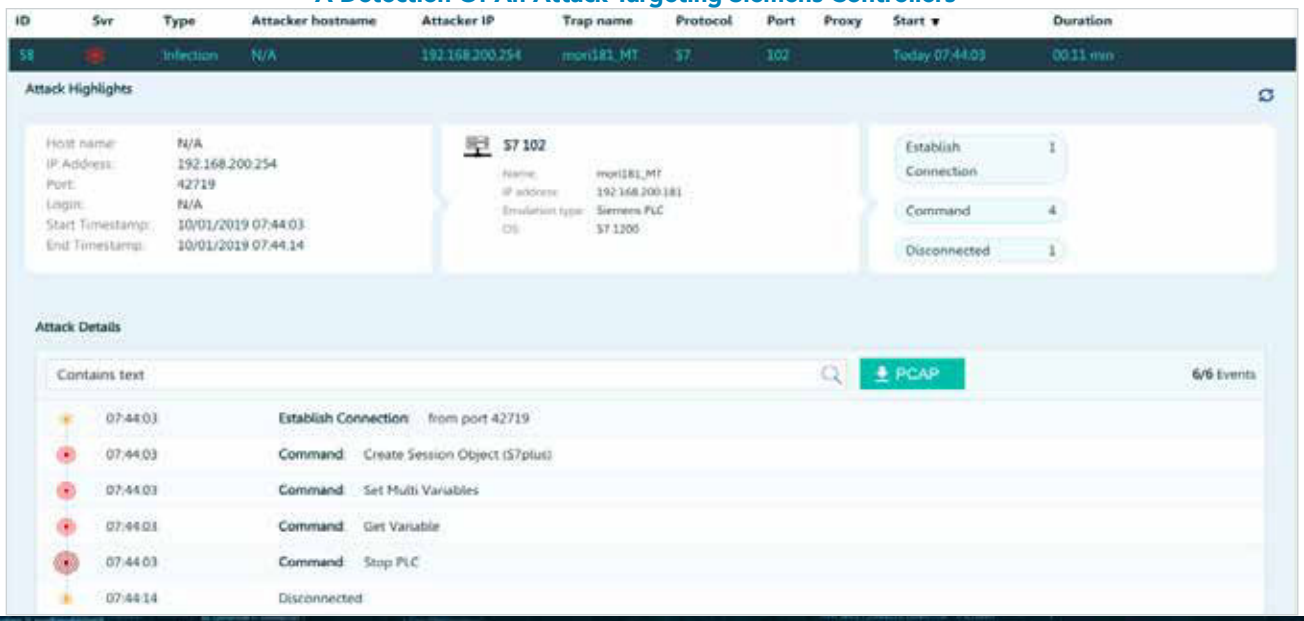
Build Your Own Trap

This powerful feature enables users to create any tailor-made attack surfaces to be identical to the users' native environment. In addition to this, a new point and click feature allows users to create additional fake instances of sensitive web applications. A broader range of IoT devices are now available to be emulated.

Improved Protection for Rockwell / SIEMENS SCADA Controllers

TrapX Security is in a close partnership with some of the world's leading manufacturing companies and is constantly creating new generations of cyber traps that can perfectly mimic operational technology devices such as Rockwell and Siemens industrials controllers. Attackers cannot tell if they're in a trap or if they're in a real system since the design and functionality of these controllers are identical.

A Detection Of An Attack Targeting Siemens Controllers



DeceptionGrid Core Components

DeceptionGrid Core Functionality – DeceptionGrid scans your existing network and provisions hundreds-to-thousands deception components. Deception Tokens (lures), which appear as ordinary files and databases are embedded within real IT assets. Traps (decoys) that emulate servers, workstations, network switches, etc.—can be deployed rapidly, as can special Traps that emulate medical devices, ATMs, retail point-of-sale terminals, components of the SWIFT™ financial network, and more. In addition, users can now create Traps that are customized to their environment by simply pointing to an asset and having the system learn its attributes.

Full Automated Forensics – Real-time automation allows attacker tools and malware to be isolated and forwarded wherever necessary for advanced analysis. TrapX provides malware analysis services based on our ecosystem integration, and we also offer a cloud-based option. We combine the additional intelligence gained from our analysis with Trap activity to deliver a comprehensive assessment to your security operations center team.

Deploy in the Cloud or On-Premise

DeceptionGrid is designed to be rapidly deployed on large enterprise networks. Automation allows IT teams to complete full deployment in just a few hours. We can also deploy DeceptionGrid through a managed security service provider (MSSP). DeceptionGrid's security operations console provides support to MSSPs to monitor the status of large numbers of customers.

Automation Delivers Enterprise Scale

DeceptionGrid was developed to overcome the limitations of conventional perimeter defenses, signature-based tools, intrusion-detection methods and honeypots. Our multi-tier Deception in Depth architecture includes the powerful automation for scalability that is required to support large enterprise and government systems without the high cost of manually configuring individual deception nodes.

Partner Ecosystem

The TrapX partner integrations create end-to-end workflows from detection to remediation and increase value from existing ecosystem investments.

Comprehensive Service and Support

The TrapX Service and Support Programs are designed to help you stay several steps ahead of attackers. Our proactive services for deploying our advanced deception technology can help you identify and eliminate threats that often go unnoticed by other cybersecurity solutions, ensuring the highest level of protection for your key assets.

DeceptionGrid takes a different approach.

Unlike firewalls and endpoint security methods, which generate alerts based upon probability, DeceptionGrid alerts are binary.

Attackers either attempt to engage our Traps or they don't.

If they do touch a Trap, we know with nearly 100% probability that it's an attack.

Differentiation

- Fast, real-time detection of cyber attacker movement anywhere in your local network and cloud environments.
- Artificial Users can mimic user activities, while acting like real exploited users. This gives attackers a false sense of a successful attack – when in reality they're inside a sophisticated cyber trap.
- Hacker Tracker enables DeceptionGrid to to track hackers back to their command and control locations by tracking deceptive files accessed from outside the network.
- Build Your Own Trap (BYOT) enables users to create their own fake attack surfaces & webapps to be tailor-made to their environments and devices.
- Dynamic Deception enables traps (decoys) to shift continuously to create a moving minefield that no attacker can avoid.
- No more alert-fatigue. A TrapX alert is more than 99% accurate and immediately actionable.
- Complete automated forensic analysis of capture malware and attacker tools.
- Automated deployment of thousands of DeceptionGrid Traps with minimal resources.
- Provides everything needed for security operations centers to act rapidly in response to a threat.
- Powerful emulation technology enables camouflaging Traps as industry-specific devices, including medical devices, ATMs, point-of-sale terminals, Internet of things (IoT) devices, and much more.
- Deception in Depth architecture integrates the benefits of Tokens, emulated Traps, FullOS Traps, and our Active Networks feature in one integrated multi-tier architecture for more rapid detection, deep attacker engagement, and comprehensive threat containment.

Key Benefits of DeceptionGrid

- **Targets the new breed of cyber attackers.** Deception technology finds sophisticated attackers that may already be inside your network that other cybersecurity solutions cannot detect.
- **DeceptionNet community.** Allows users to share defensive counter-measures and two-way sharing of Traps developed by community members.
- **Reduces or eliminates economic losses.** Accurate and rapid detection reduces the risk of economic loss due to destruction of enterprise assets, theft of data, and overall impact to business operations.
- **Reduces time to breach detection.** Advanced real-time forensics and analytics, coupled with high accuracy and high fidelity alerts that uniquely empower your security operations center to take immediate action to disrupt all attacks within the network perimeter.
- **Comprehensive visibility and coverage.** Defense in Depth provides comprehensive visibility into internal networks, revealing attacker activity and intentions, and terminating the attack.
- **Improves compliance.** To meet PCI and HIPAA data breach laws, along with other regulatory requirements in various countries.
- **Lowest cost of implementation.** Deception in Depth provides the greatest breadth and depth of deception technology at the lowest cost to your enterprise.
- **Compatible with existing investments.** Deception technology can integrate with your existing operations and defense-in-depth vendor solutions.

About TrapX Security

TrapX Security is the pioneer and global leader in cyber deception technology. Their DeceptionGrid solution rapidly detects, deceives, and defeats advanced cyber attacks and human attacker in real-time. DeceptionGrid also provides automated, highly accurate insight into malicious activity unseen by other types of cyber defences.

Want to Learn More?

To learn more, get in touch with the Threatscape team via info@threatscape.com or on 0203 653 0000 (UK) or 01 901 7000 (Ireland)