K@K IT
SECURITY SOLUTIONS

Services

Infosec Services That We Offer

ABOUT US

Centralized Monitoring of LOGS

Services

- SHIPS
  (Shared Host Integrated Password System)

Solutions

- Internal VAPT
- External VAPT

NAC (Network Access Control)

DNS Firewall

Black Box Testing

DLP (Data Loss Prevention)

Internal Security Audit

Infosec Services That We Offer

Internal Security Audit

– Not at all a stressful or an expensive solution to assess your security compliance

- Improve security of your Organization.
- Prove to be effective in scoring the security of their organization.
- Find your weakness and fix them appropriately.
- Penetration testing is very important.
- Proper solutions is very important to be implemented.

Internal Security Audit

Infosec Services That We Offer

Create a Baseline

– Measure your enchantment's for future audits

Audits need to be done frequently.

Gathering and sorting relevant data is simplified because it isn't being distributed to a third party.

Internal security audits cause less disruption to the workflow of employees.

Why we always mention in our caption (Red Team) is because doing a Red Team Audit gives us a clear picture about your complete network as well as your other assets.

Internal Security Audit

Infosec Services That We Offer

Comprehensive Report

– A full comprehensive report for management as well as the technical staff

We will be sending you a complete comprehensive report about your assets and Vulnerabilities found on the Network.

We will include checks for RANSOMEWARE Attacks.

We will check for your confidential data whether it can be leaked to the outside world.

Data can be leaked Intentionally or Unintentionally but protecting it is very important

Provide you with solutions and fixes.

External Security Audit

Infosec Services That We Offer

Red Team Assignment

- Red teaming helps a business remain competitive while securing its business interests by leveraging social engineering and physical, application and network penetration testing to find ways to shore up your defenses.

- During a red team engagement, highly trained security consultants enact attack scenarios to reveal potential physical, hardware, software and human vulnerabilities.Red team engagements also identify opportunities for bad actors and malicious insiders to compromise company systems and networks or enable data breaches.

External Security Audit

Infosec Services That We Offer

Who Needs It

If you are a small to midsize businesses, you might think red teaming is not for you. “I’m too small to be a target,” you might theorize. However, in fact, this is exactly the line of thinking that puts an organization at risk. If you were a bad actor, wouldn’t you want to go after the person who would never expect it?

While you might think no one would care enough to hack into your company, businesses of all sizes – and individuals – are regularly victimized.

Why?

In addition, it is not just about sensitive information. Bad actors are also trying to take over the technologies that power our lives. For instance, they might be looking to access your network to better hide their activities while taking over another system or network somewhere else in the world. Your data does not matter. It is your computers they want to infect with malicious software so that they add your system to a botnet group.

External Security Audit

Infosec Services That We Offer

Red Team Assignment

Black Box – Application Testing

Infosec Services That We Offer

CONCEPTUAL DIFFERNCES AMONG THREE TYPES OF TESTING

APPLICATION SECURITY

Routinely using black box testing techniques for application security testing presents challenges for many development teams. Managing black box testing requires a great deal of time and resources, which can be a hindrance for adhering to aggressive development timelines.

FLAWS

Blackbox testing techniques look for vulnerabilities and flaws from the outside of the application, imitating methods and tools that attackers might use to penetrate security.
Black box testing techniques can be highly effective at finding certain kinds of flaws, from server configuration mistakes or errors to input/output validation problems and other issues specific applications.

TECHNIQUES

Black box testing techniques are an essential part of any application security testing program. In contrast to white box testing where source code is available for testing and review, black box testing techniques are employed without access to code and with no information about the application structure.

Grey Box and White Box Testing

Infosec Services That We Offer

WHITE BOX SECURITY AUDIT

White Box Testing approach our team would have as much information as possible about the target environment, such as an actual employee would possess.
This approach is designed to prepare for a worst-case-scenario where an attacker has in-depth information about your infrastructure.

GREY BOX SECURITY AUDIT

Our team would be given partial information about the target environment, such that could be identified by a motivated attacker.
Documents provided could include policy documents, network diagrams and other valuable information.

Application Security Audit

Infosec Services That We Offer

Application Security Audit

AN APPLICATION SECURITY AUDIT IS AN ASSESSMENT OF THE SECURITY RISKS THAT ARE ASSOCIATED WITH YOUR WEB APPLICATIONS AND CLIENT SERVER APPLICATIONS; BOTH THOSE THAT HAVE EXTERNAL EXPOSURE VIA THE INTERNET (SUCH AS WEB SHOPS AND CUSTOMER PORTALS), AND THOSE THAT ARE PART OF THE INTERNAL WORKING OF YOUR ORGANIZATION (SUCH AS YOUR FINANCE SYSTEM OR CUSTOMER RELATIONSHIP MANAGEMENT SOFTWARE). AS PART OF AN APPLICATION SECURITY AUDIT, K@K IT SECURITY WILL CARRY OUT A SECURITY ASSESSMENT OF:

- THE DESIGN OF EACH COMPONENT
- WEB SITE COMMUNICATIONS
- APPLICATION LAYER
- WEB SERVICES
- INTERFACES
- DATABASE

Firewall Security Audit

Infosec Services That We Offer

Understand Where the Firewall sits in the Network Topology

Extract Configured Security and Threat Policies and Translate Into Plain English

Identify Policy Overlaps, Duplicates, Artifacts and Orphans

Audit the Device Security Configurations Against an Accepted Best Practices Baseline

Perform a Health Capacity Assessment of System Resources

Identify Recently Logged Anomalies, Incidents and Errors

Shared Host Integrated Password System (SHIPS)

Infosec Services That We Offer

- The ships is an open-source solution created by trustedsec to provide Unique and rotated local super user or administrator passwords for Environments where it is not possible or not appropriate to disable These local accounts.
- Clients for Windows and Linux may be configured To rotate passwords automatically.
- Stored passwords can be retrieved by desktop support personnel as required, or updated when a password has to be manually changed in the course of system maintenance.

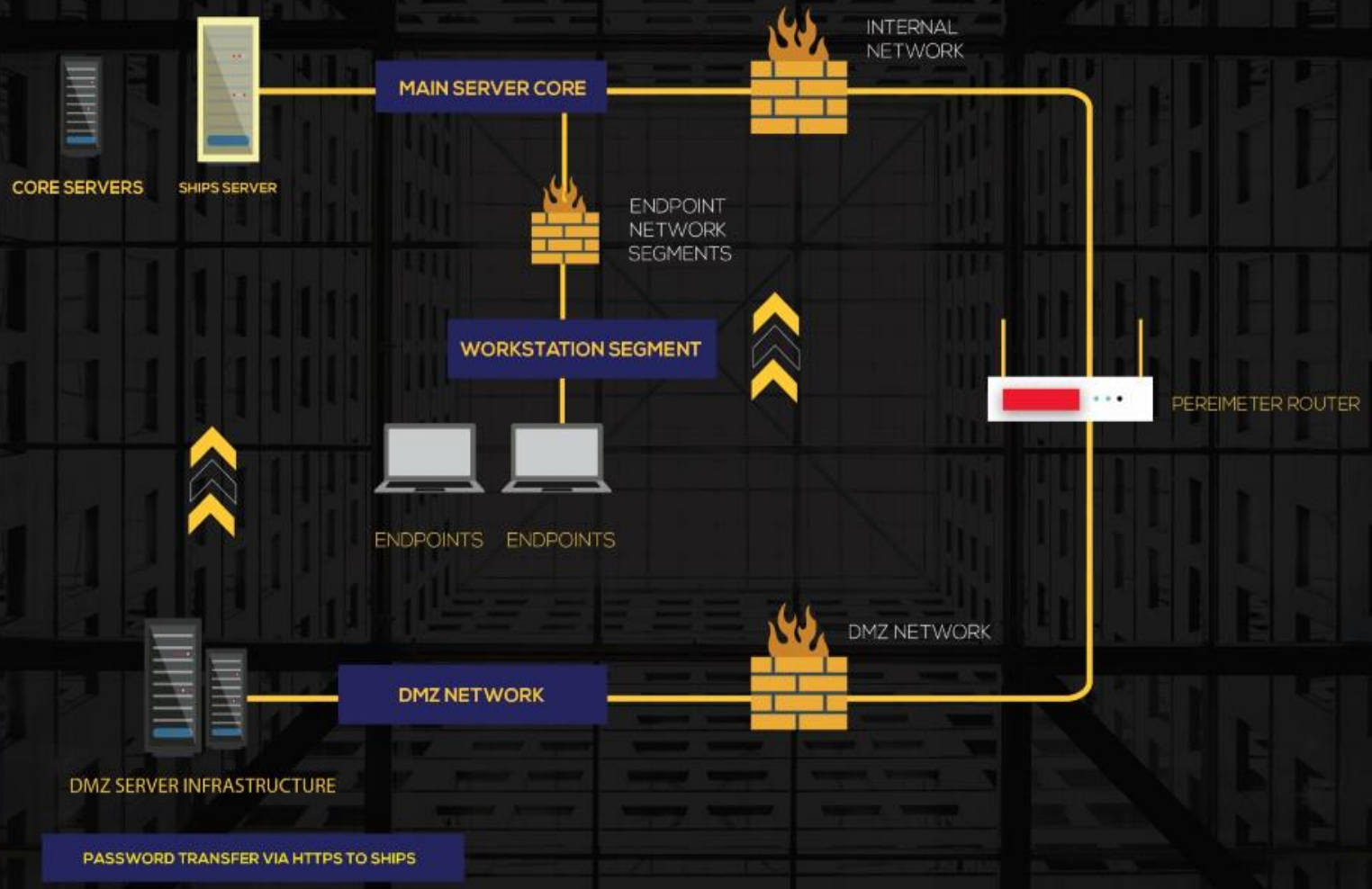
Shared Host Integrated Password System (SHIPS)

Infosec Services That We Offer

- By having unique passwords on each machine and logging of password retrievals, security can be improved by making networks ore resistant to lateral movement by attackers and enhancing he ability to attribute actions to individual persons.
- SHIPS is designed to make post-exploitation more difficult and minimize what systems attackers gain access to.
- Once SHIPS is set up, there isn't much else that is needed and it's simple to integrate into existing business processes.

Shared Host Integrated Password System (SHIPS)

Infosec Services That We Offer



DLP (Data Leak Prevention)

Infosec Services That We Offer

- Data loss prevention (DLP) is a set of tools and processes used to ensure that sensitive data is not lost, misused, or accessed by unauthorized users.
- DLP software classifies regulated, confidential and business critical data and identifies violations of policies defined by organizations or within a predefined policy pack, typically driven by regulatory compliance such as HIPAA, PCI-DSS, or GDPR. Once those violations are identified.
- DLP enforces remediation with alerts, encryption, and other protective actions to prevent end users from accidentally or maliciously sharing data that could put the organization at risk.
- Data loss prevention software and tools monitor and control endpoint activities, filter data streams on corporate networks, and monitor data in the cloud to protect data at rest, in motion, and in use.
- DLP also provides reporting to meet compliance and auditing requirements and identify areas of weakness and anomalies for forensics and incident response.

DLP – Key Features

Infosec Services That We Offer

Key Features

- On demand Workstation discovery MyDLP API.
- Document Hashes.
- SMTP Gateway Integration
- Simple Reporting
- Text matching details mail recipient details policy Revisioning Keywords
- Predefined Dictionaries
- Distance (Partial Context
- Grouping) Predefined Policies
- Mail BCC protection, Custom Content definition Block and Log Actions.
- Quarantine and Archive Actions
- Native SYSLOG Integration, Exporting to Microsoft Excel or mail archive
- Regular Expression
- Partial (Approximate) Document Matching
- IRM Actions MICROSOFT ACTIVE
- Active Directory Integration
- Database Integration (SQL/ JDBC)
- Remote Storage Integration (CIFS,SMB NFS,FTP And more ..)
- ICAP Integration
- Customizable Dashboard
- Full-Text Search with SOLR Integration Removable Storage
- Inbound Archive

DNS Firewall

Infosec Services That We Offer

- Now a days Bring Your Own Device (BYOD) is gaining popularity.
- Mobile devices from inside and outside your Network are continuously crossing mixed physical and cloud infrastructure whose security may not always be under your control. As a result, your network is being persistently exposed to malware threats.
- And DNS is their main pathway. More than 90 percent of malware uses DNS to speak with C2C (command and control servers), steal data, or redirect traffic to malicious sites.
- Existing security pedals and perimeter defenses are not designed to prevent, isolate, and remediate DNS-based malware threats.

THREAT INSIGHT	THREAT INTELLIGENCE FEED
AVOID DATA EXFILTRATION WITH DNS-BASED ANALYTICS	REPORTING AND ANALYTICS
DNS RESPONSE POLICY ZONES (RPZS)	SECURITY PORTAL

Centralized Log Management OSSEC

Infosec Services That We Offer

- Enforcing retention policies on your logs so they are available for a specific time period
- CLM Centralized Log Management
  granting login access to particular users without granting serverroot access
- Storing log data from multiple sources in a central location Easily searching inside the logs for important information Generating alerts based on metrics you defined on the logs
  Low costs and increased storage and backup for historical data setting up security alerts.

OSSEC + Logstash, Elasticsearch and Kibana

Infosec Services That We Offer

- OSSEC is an Open Source HIDS solution with file integrity checking capabilities.
  Elastic Stack is the combination of three popular Open Source projects for log management, known as Elasticsearch, Logstash, and Kibana.

- Elasticsearch is a highly scalable full-text search and analytics engine. Logstash is a tool to collect logs, parse them, and store them for later use. Kibana is a flexible and intuitive visualization dashboard.

- OSSEC HIDS integration with Elastic Stack provides a real-time alerts management console, as well as a scalable and flexible way to store data for as long as needed.

- Detailed Information on https://kakitsecurity.com/centralized-log-management.php

NAC (Network Access Control)

Infosec Services That We Offer

N

A

C

Network Access Control aims to do exactly what the name implies—control access to a network with policies, including pre-admission endpoint security policy checks and post-admission controls over where users and devices can go on a network and what they can do.

Network Access Control (NAC) is a computer networking solution that uses a set of protocols to define and implement a policy that describes how to secure access to network nodes by devices when they initially attempt to access the network.

A network access control system allows organizations to restrict access to resources on their network.
Choosing to implement NAC can drastically improve an organization's network security posture by allowing for greater control over what devices are accessing the network, and what they are granted access to.

Reverse Proxy & Load Balancing

Infosec Services That We Offer

REVERSE PROXY

A reverse proxy is a server that sits in front of web servers and forwards client (e.g. web browser) requests to those web servers.

Reverse proxies are typically implemented to help increase security, performance.

LOAD BALANCING

Load balancing is a technique used to distribute workloads uniformly across servers or other compute resources to optimize network efficiency, reliability and capacity.

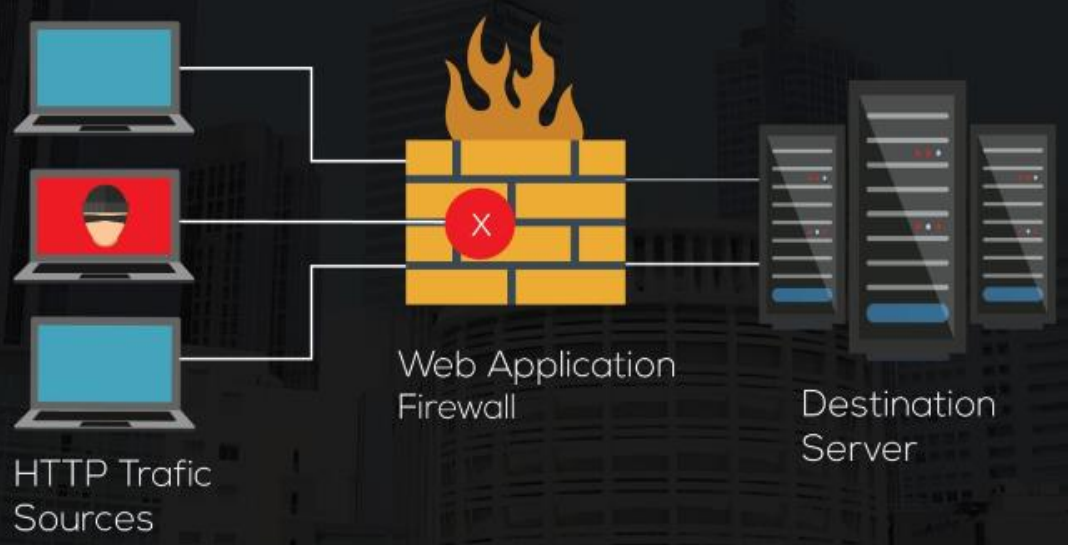
Load balancing is performed by an appliance -- either physical or virtual -- that identifies in real time which server in a pool can best meet a given client request, while ensuring heavy network traffic doesn't unduly overwhelm a single server.

WAF (Web Application Firewall)

Infosec Services That We Offer

Application Security Audit

- A WAF or Web Application Firewall helps protect web applications by filtering and monitoring HTTP traffic between a web application and the Internet.
- It typically protects web applications from attacks such as cross-site forgery, cross-site-scripting (XSS), file inclusion, and SQL injection, among others.



Deception Technology

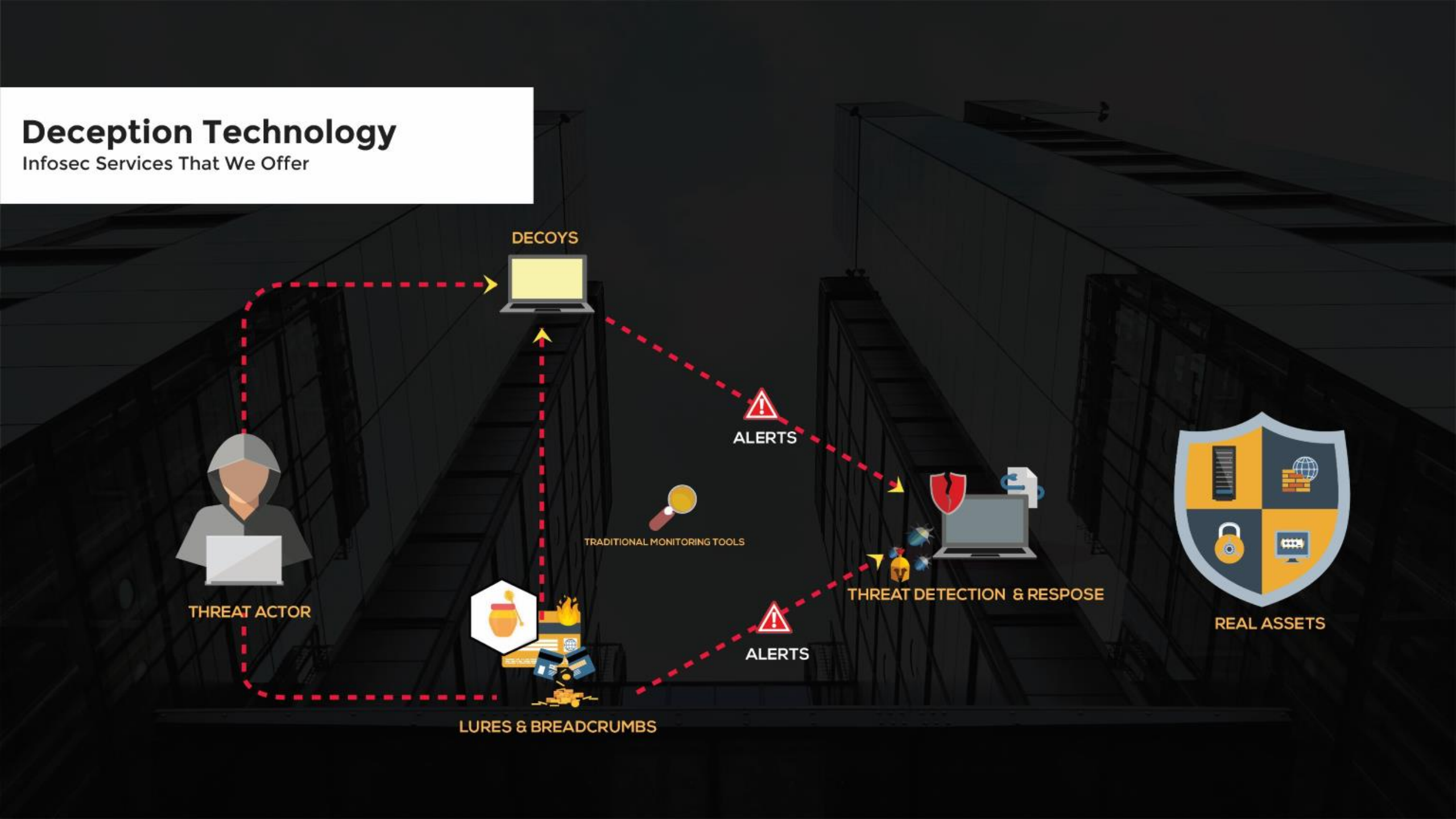
Infosec Services That We Offer

Definition

- The aim of deception technology is to prevent a cybercriminal that has managed to infiltrate a network from doing any significant damage.
- The technology works by generating traps or deception decoys that mimic legitimate technology assets throughout the infrastructure. These decoys can run in a virtual or real operating system environment and are designed to trick the cybercriminal into thinking they have discovered a way to escalate privileges and steal credentials.
- Once a trap is triggered, notifications are broadcast to a centralized deception server that records the affected decoy and the attack vectors that were used by the cybercriminal.

Deception Technology

Infosec Services That We Offer



Server Hardening (CIS Benchmark)

Infosec Services That We Offer

- Security Best Practice advocates the minimizing of your IT systems' 'Attack Surface'. By using CIS Benchmark secure configuration guidance we can harden systems against attack. Known vulnerabilities can be removed and defenses strengthened by applying an expert-derived configuration policy.

- The Center for Internet Security also recommends hardening services configurations, cutting back functionality to reduce further the opportunities to compromise a system. However, the demands of each organization, their IT services and their environment are all different, making it impossible to accurately prescribe a hardened services policy for every situation.