invisible
bits

2018

World Trade Center
Edif. Este 5ª planta 08039
Barcelona
España

vSOC Platfom & Delfos SIEM

Correlation for CyberSecurity needs

Tabla de contenido

Managed Security Multi Service Approach

Today's Security incidents have very diverse nature. Malware use variety of penetration techniques. So, threat detection is based on different use cases which appear and evolve every day: Unauthorized access to corporate networks, credentials theft, valuable data leakage, vulnerable mobile apps, ransomware, phishing, crypto currency injections, malicious bots, DDos and many more …

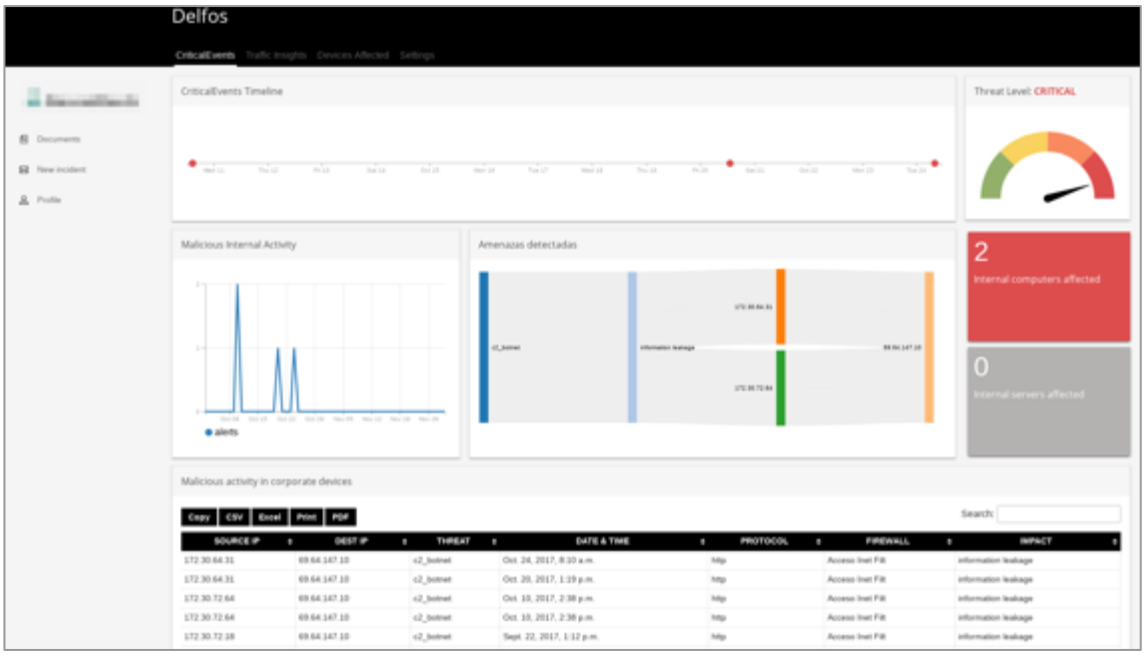
How to predict, avoid, detect and respond?? It becomes a big challenge for the modern protection systems! How to provide an enterprise with a holistic tool to stand against such different vectors of attack!

From the very beginning Invisible Bits vSOC ® and Invisible Bits Cyber Security Portal Delfos ® was developed having these factors in mind. From the very beginning we have seen that majority of compromises are provoked by the grey area between known use cases.

Invisible Bits Delfos ® is a modular front-end Macro Correlation Platform

Centralized Unique Console for Incident Management

Invisible Bits Cyber-Security Portal is designed as an all in one front end for Incident Monitoring and Management. Web-portal is easy to use tool with different views, functionality and integration with 3rd Party security solutions. Many sources of information from Security Devices or SIEM as well as embedded Threat Intelligence Sources permit Security Specialists of Organizations of MSSPs access all critical



security information.

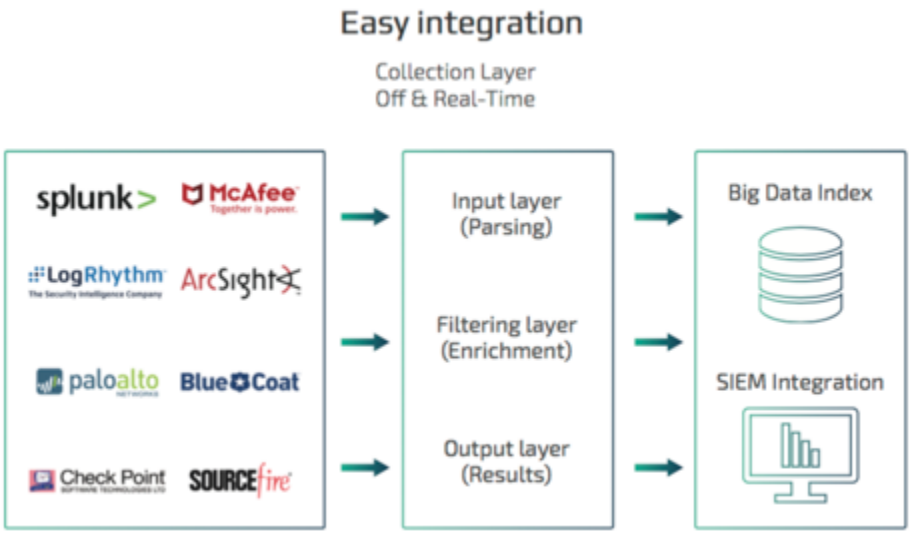
Platform Key capabilities:

- Incident management full life cycle
- Drill down to threat source
- Variety of Threat Modules (Use Cases)
- Easy integration with 3rd Party Security Solutions
- Imbedded Threat Intelligence
- Automation and Orchestration

Integration Options

Varity of security solutions, different consoles, portals and incident sources making the work of Cyber Security teams really difficult and not efficient. It's easy to lose focus and follow the procedures in complicated environment. The efficiency of Invisible Bits Cyber Security Platform Delfos ® is designed as an open and easy to integrate system. As a correlator Delfos can insource directly the Row logs or threat events after correlation on external SIEM. APIs and integration with own agents and threat feeds making the system really attractive to integrate all security incidents management. Following integration sources are available:

- Row logs through proper collectors and Syslog protocol
- Correlated Threat Events form majority of SIEM solutions
- Through API with cloud and on-premise security solutions for incident insourcing
- Indicators of compromise (IOCs) and Threat Intelligence Feeds
- Orchestrator and Security Devices Change Management with the most of Security solutions



Visualization and reporting

Security leaders of organizations as well as operational managers will find corresponding level of security incidents information. Full threat management cycle is covered by with possibility to drill down to more details or have a general view of threat situation.

Reporting is one of the most prominent features of the service. Today's customer needs to be informed and up to date about critical incidents, suspicious activities and all security incidents statistics. Threat Visibility and Return on Investments are key in communicating and informing customers about their Security Incidents and Cyber Threats.

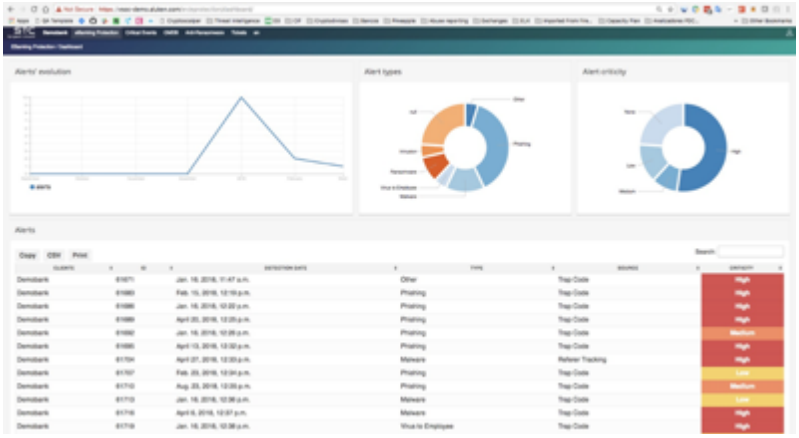


Image: Example of Realtime Phishing Attacks Report (Dashboard)

Types of Report

Security leaders of organizations as well as operational managers will find corresponding level of security incidents information. Full threat management cycle

is covered by SOC Portal with possibility to drill down to more details or have a general view of threat situation.

Delfos Threat Modules Available from the Portal

CyberWatch is a set of Use Cases for specific types of enterprise security Incidents. All modules are based on the correlation of events coming from different devices or services or proper agents. Processes permit users rely on following Modules:

- **CyberWatch E-Channel Protection**: set of specific Use Cases for different Industries. Module permits detection & mitigation of threats against different channels:
- **Anti-phishing** Monitoring and detection of phishing attacks targeting specific corporate valuable information and credentials or employees or general phishing attacks
- **Cyber – Squatting:** Malicious URLs, fake domains will be blocked, notified.
- **Rogue mobile apps:** Malicious Mobile Applications misuse of brand name is a real threat to any organization. Delfos constantly monitors and notify in case of detection
- **Trap Code**: proactive detection of attacks on online channels: it detects phishing before it occurs, and clients avoids any exposure to risk. The technology behind is unique approach which tracks marked code peace
- **IdentiView**: · Detection of anomalies in executive accounts, suspicious activity and unauthorized access to corporate networks and enterprise systems
- **SecurityView:** centralized view of the vulnerabilities of the corporate park. It integrates with Qualys and generates additional dashboards.
- **CertiView:** detection of security problems in the SSL / TLS certificates of the company and control of when they expire, both internal and external.
- **Anti-Ransomware:** ransomware detection in corporate environments. Detection by behavior that up to date detects 100% of the families with which it has been tested. Complements the antivirus to ensure that even if they do not have the signatures, the endpoint will not be affected. It relies on an agent that is installed on the computers.
- **INTACT Mail:** protection against threats that arrive via email (spear phishing, ransomware, malware, infected documents, etc.) with a new concept of corporate email isolation technology. It relies on the installation of agents in the form of plugins for mail clients (e.g. Outlook).
- **Code review:** detection of OWASP vulnerabilities in source code, only for web applications (no mobile apps, no desktop applications).
- **Critical Events:** detection of critical events inside of corporate environments:

those that have skipped all security layers deployed. Use case detects connections of infected devices.

Delfos Threat Intelligence

Threat Intelligence is a key element of Invisible Bits approach. To Monitor, Investigate and React nowadays is not possible without having real time relevant context rich threat intelligence tools.

Delfos Threat Intelligence feeds provides near-to-real-time actionable Indicators of Compromise of 0day daily advanced cyber threats.

Feeds can be directly fed to SIEMs, web proxies, firewalls and any IT security devices. If required connector is still not available, Invisible bits will create and provide it without extra charge.

Delfos Threat Intelligence
Actionable Quality Feeds

Product	Code	Description
Phishing feed	PSF	Feed of phishing attacks against financial entities, ecommerce sites and cloud services as email and cloud storage, created to steal credentials from final users and employees.
Cybersquatting and Brand Abuse	CBF	Feed of suspicious and malicious domains aiming to impersonate targeted brands by email, false or offending websites.
Credit Card Theft	CCF	Feed of stolen credit cards related to specific financial institutions, detected in real time when they are subtracted from victims. Allows to prevent economical fraud, integrate with risk scoring systems and take early countermeasures before malicious transactions are executed.
Internet infected devices	IIF	Feed of IP address of infected devices with information stealer trojans, detected as part of malicious infrastructures and sending confidential information to a botnet. Useful to detect compromised customers, employees and corporative hacked servers.
Botnets Crime Servers	BCF	Feed of CrimeServers collectors where infected devices are sending stolen information and publishing Remote Access Tools for allowing attackers to acceding corporate resources. Allows to detect corporate compromised devices in internal networks infected with advanced threats. DGA and RAT 0day malware included.
0day Ransomware	RWF	Feed of new daily new ransomware campaigns. Usefull for avoid information & devices hijacking by 0day ransomware attacks as WannaCry, Petya, Cryptolcker, Locky, Cerber, etc.