Building intelligence-driven Security Operations Center

Mariusz Stawowski, Ph.D.
CISSP, CCISO

25 years | CLICO

Agenda

- How to build Security Operations Center?
- GDPR and NISD - new UE law for data, networks and IT systems protection
- How to protect and audit PII?
- How to efficiently manage the incidents?

Security Operations Center (SOC) - centralized unit that deals with security issues on an organizational (business) and technical level

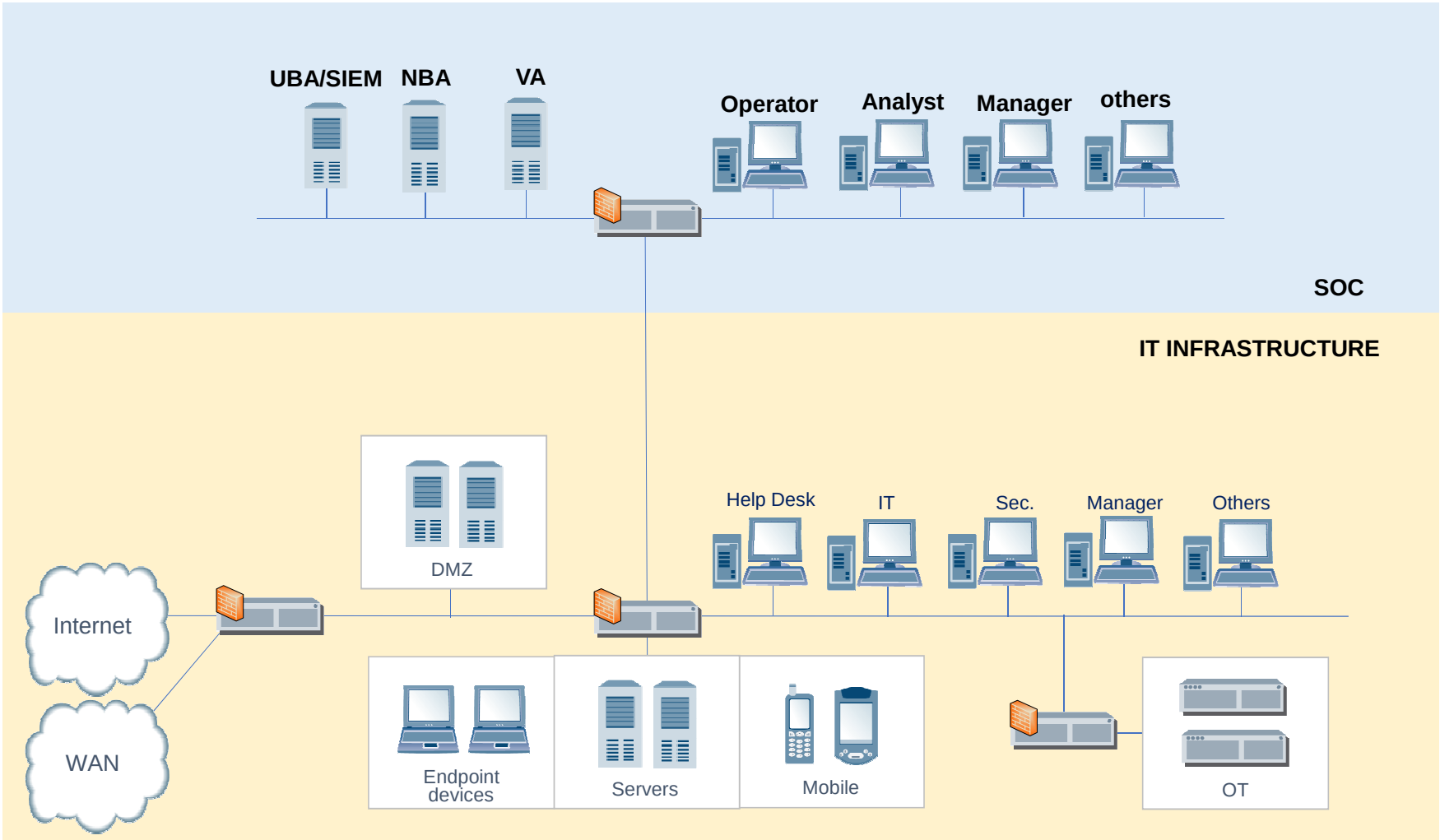
More information: „Building a World-Class Security Operations Center: A Roadmap", SANS Institute 2015

other names: Information Security Operations Center (ISOC), CyberSecurity Operations Center (CSOC), Security Defense Center (SDC), Security Analytics Center (SAC), Network Security Operations Center (NSOC), Security Intelligence Center (SIC), Cyber Security Center (CSC), Threat Defense Center (TDC), Security Intelligence and Operations Center (SIOC), Infrastructure Protection Centre (IPC)

SOC vs CERT, CSIRT

SOC types: Corporate SOC, Outsourced SOC, Cloud SOC

SOC infrastructure

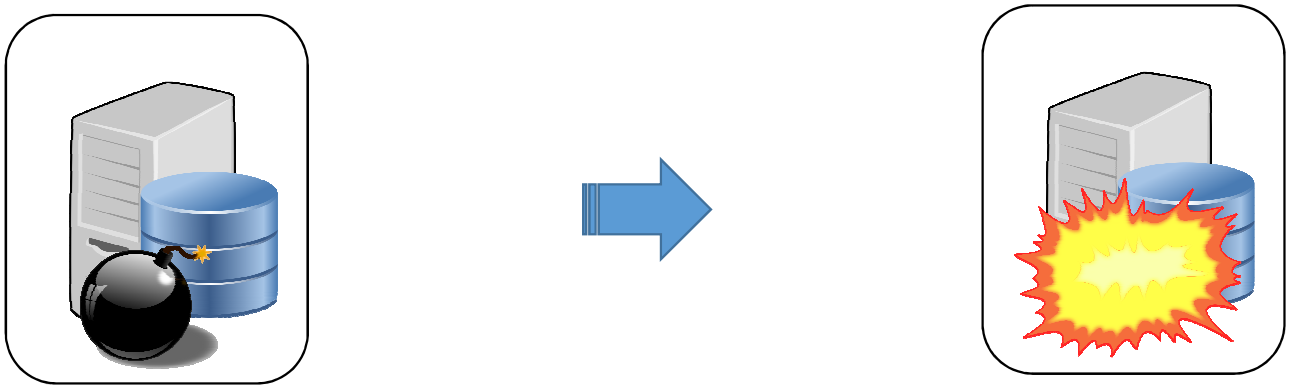


Why we need SOC?

- **Late detection of incidents** leads to serious security breaches
- Security management requires building **large team of security experts**
- Employee rotation is **risk of knowledge loss** by the organization
- IT documentation and other IT related **important data dispersed in many places**
- Difficulties in **understanding technical events in business context**
- Security **breach reporting requirements** of new UE law (eg GDPR, NISD)

25 years | CLICO

Example of late incident detection – energy sector, Ukraine 2015



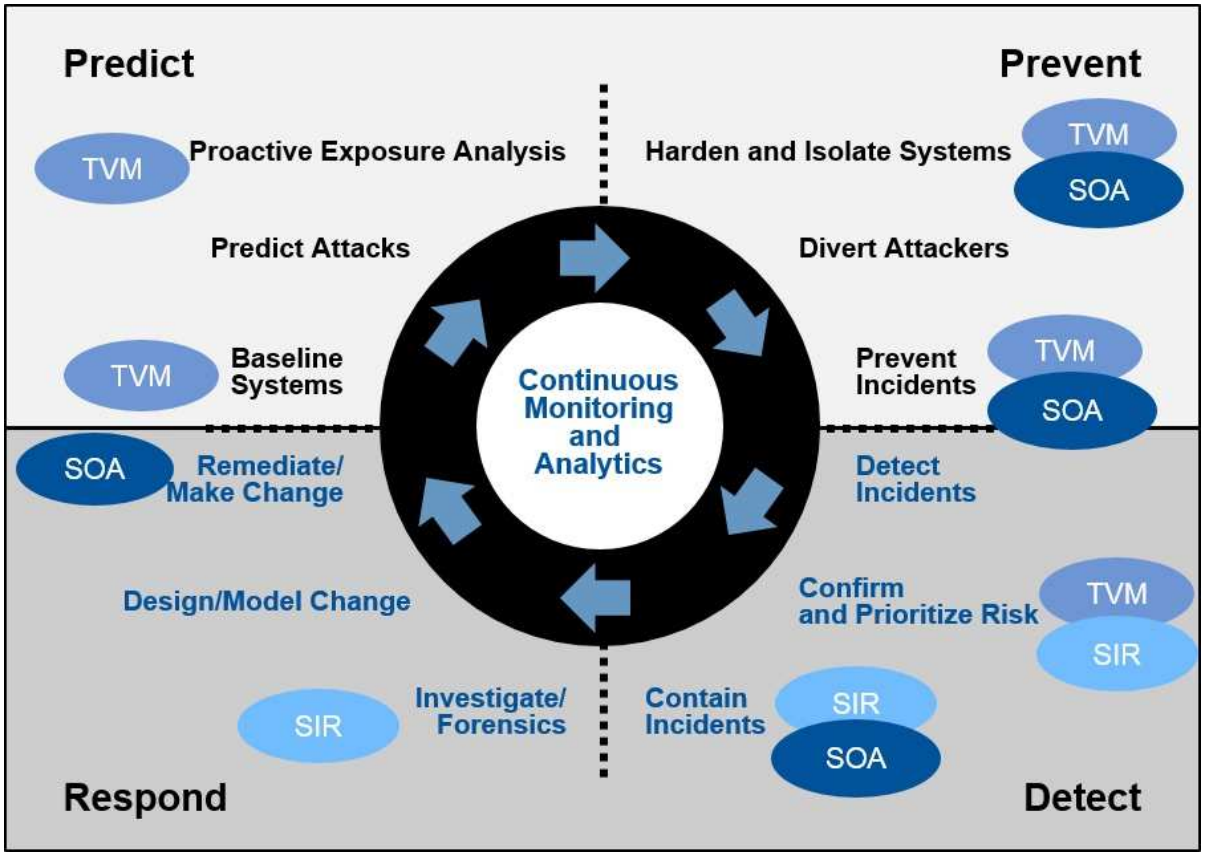
- Social engineering attack (email Phishing)
- The attached in email MS Office doc. installs BlackEnergy 3 malware
- **C&C access and recognition of IT environment (+6 months)**
- Obtaining data for remote access to ICS systems
- Remote access to ICS systems
- Installation of KillDisk malware
- DoS attack at Call Center

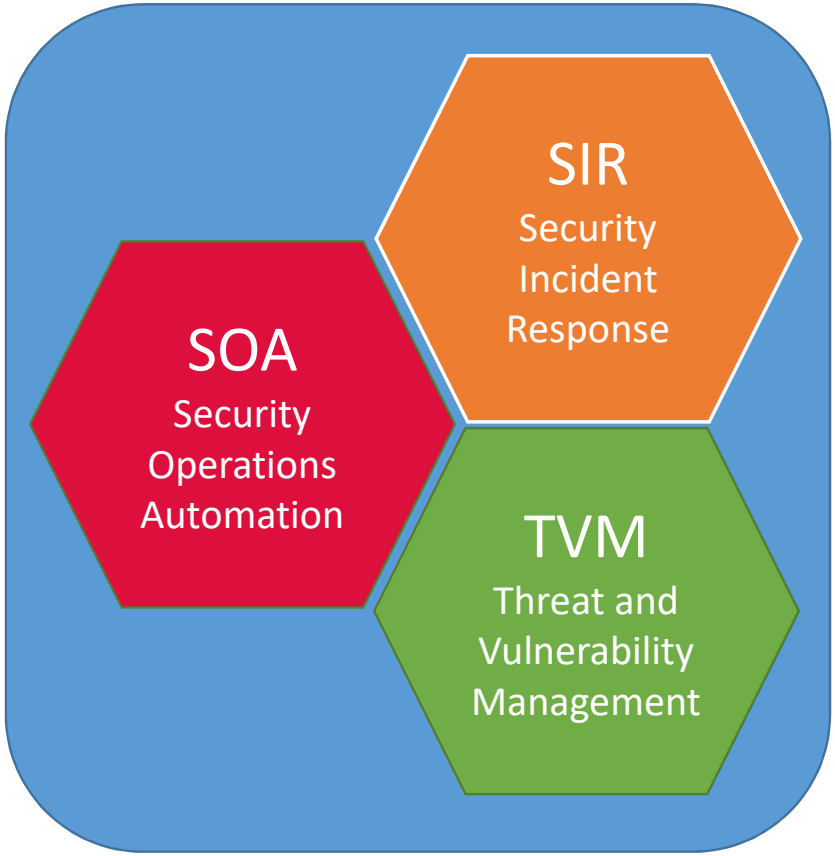
- The attack at the power distribution system (attack by HMI SCADA, resulting in a lack of energy at 225,000 customers)
- False ICS firmware makes difficult the systems recovery
- Turning off the systems backup power supply (UPS)
- Removing the traces of the attack (the removal of logs, destruction / locking systems, etc.)

More information: Analysis of the Cyber Attack on the Ukrainian Power Grid, Defense Use Case, Electricity Information Sharing and Analysis Center, SANS-ICS, March 18, 2016

25 years | CLICO

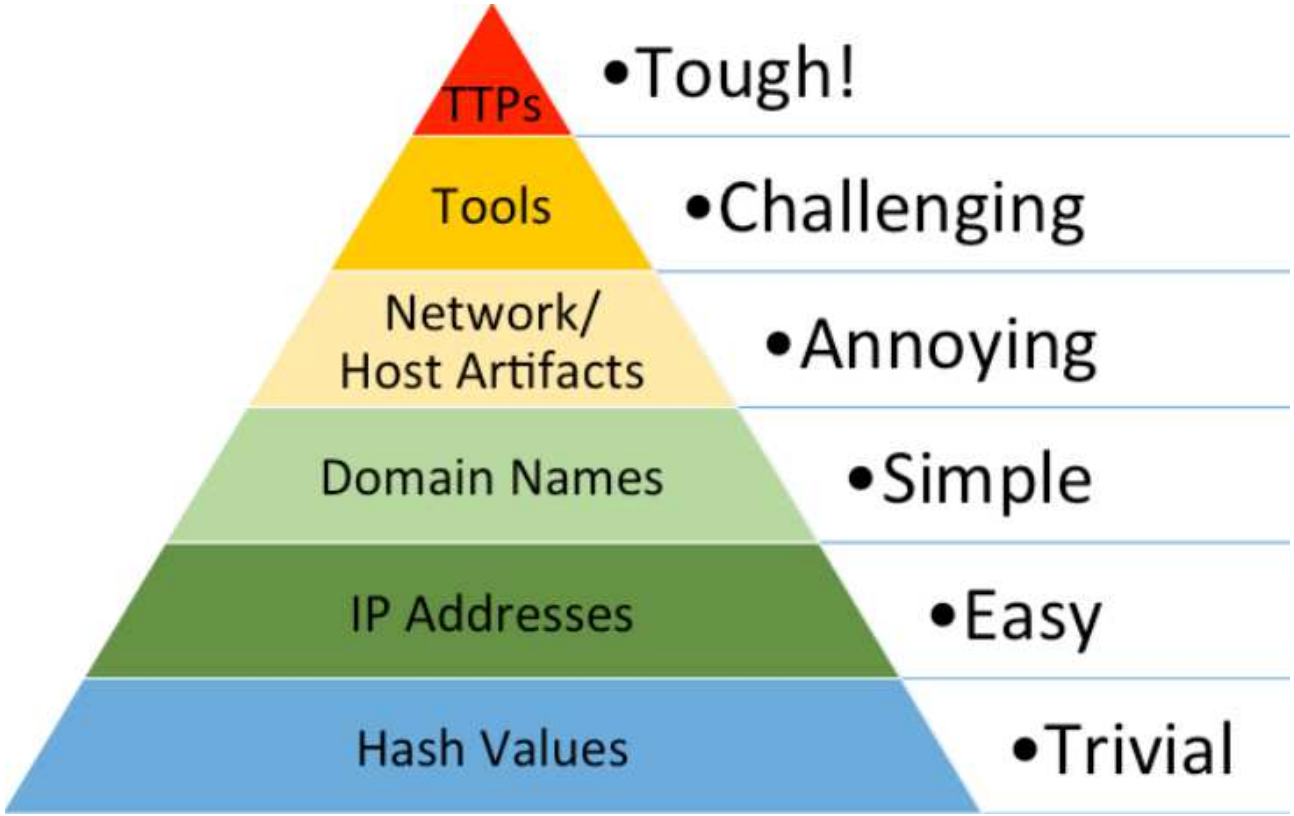
Intelligence-Driven SOC





More information: The Five Characteristics of an Intelligence-Driven Security Operations Center, Gartner 2015

Threat Intelligence in SOC

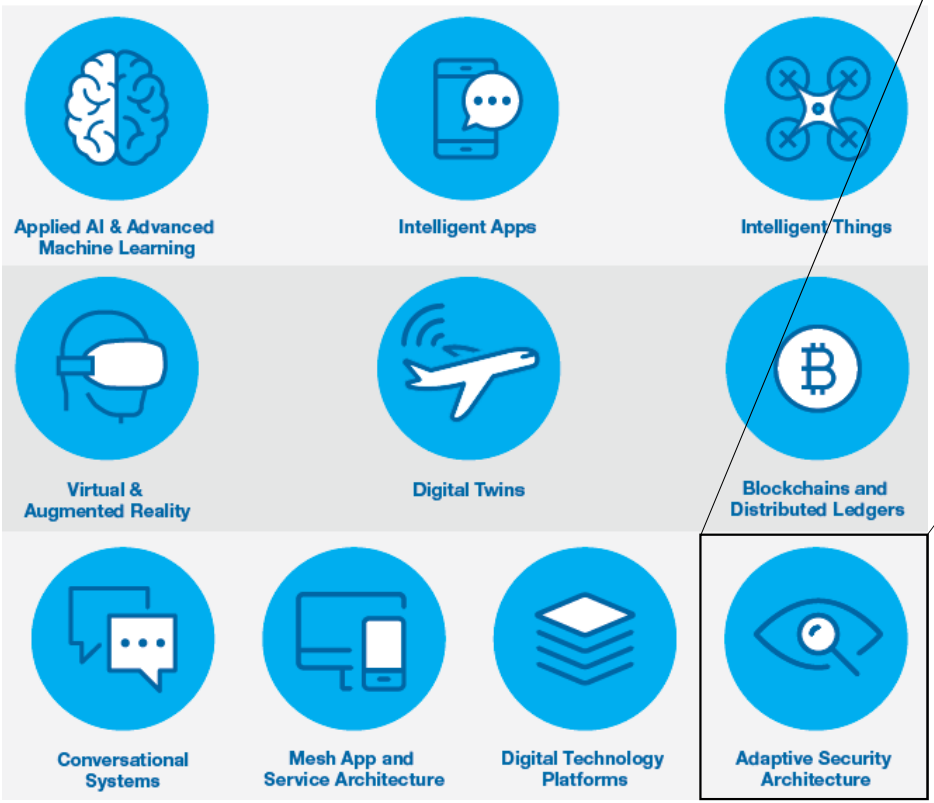


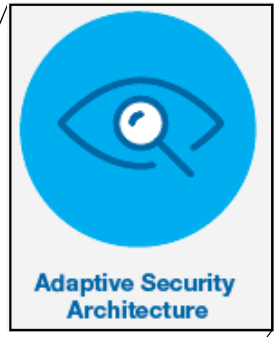
More information: "The Pyramid of Pain" - David Bianco

25 years | CLICO

Gartner's Top 10 Strategic Technology Trends for 2017

Artificial intelligence, machine learning, and smart things promise an intelligent future.





(...) **Multilayered security and use of user and entity behavior analytics will become a requirement for virtually every enterprise.**

More information: http://www.gartner.com/smarterwithgartner/ gartners-top-10-technology-trends-2017/

25 years | CLICO

Why EU cybersecurity law was tightened?

- GDPR: *designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens data privacy and to reshape the way organizations across the region approach data privacy*
- NISD: *bring cybersecurity capabilities at the same level of development in all the EU Member States and ensure that exchanges of information and cooperation are efficient, including at cross-border level*
- **Other reasons:**
  - **Cybercrime is recognized risk for the economy**
  - **„Security is a cost" approach = no real safety**
  - **„Security checklist" approach = no real safety**

25 years | CLICO

New UE law for data and IT systems protection

December 2015, EU Commission reached an agreement on new law for data and IT systems protection law:

- **General Data Protection Regulation (GDPR)**

  GDPR will give EU citizens stronger rights, empowering them with better control of their data and ensuring that their privacy remains protected.

- **Network and Information Security Directive (NISD)**

  NISD is complementary to the GDPR, aimed at the protection of IT systems of operators of essential services and the providers of critical digital services.

25 years | CLICO

New UE law for data and IT systems protection

Regulation	GDPR	NISD
Primary Goals	• Directive on **protecting personal data** processed for prevention, detection, investigation or prosecution of criminal offenses …	• Improve Member States' **cooperation on cyber security**. • Directive concerning measures to **ensure a standard high level of network and information security** across the EU.
Organizations Impacted	• Data controllers and data processors. • Essentially **any organization with personal data**.	• **Operators of essential services** in the energy, transport, banking and healthcare sectors. • **Providers of critical digital services** like search engines and cloud computing.

New UE law for data and IT systems protection

Regulation	GDPR	NISD
Effective Date	**May 2018**	**May 2018** - Transposition into national law **November 2018** - Member States to identify operators of essential services

New UE law for data and IT systems protection

Regulation	GDPR
Security technology requirements	• Data protection by design and by default (Article 25). • Security of processing (Article 32). • Breach notification (Article 33). • Data protection impact assessment (Article 35).

Privacy by Design

'The controller shall..**implement appropriate technical and organisational measures..in an effective way**.. in order to meet the requirements of this Regulation and protect the rights of data subjects'. Article 23 calls for controllers to hold and process only the data absolutely necessary for the completion of its duties (data minimisation), as well as limiting the access to personal data to those needing to act out the processing.

ISO/IEC standards relevant for PII protection

ISO/IEC 29100:2011	Privacy framework
ISO/IEC 29101: 2013	Privacy architecture framework
ISO/IEC 29115:2013	Entity authentication assurance framework
ISO/IEC 29134	Privacy Impact Assessment - Methodology
ISO/IEC 29151	Code of practice for PII protection
ISO/IEC 29190:2015	Privacy capability assessment model
ISO/IEC 27018:2014	Code of practice for PII protection in public clouds acting as PII processors
ISO/IEC TS 19608	Guidance for developing security and privacy functional requirements based on ISO/IEC 15408 (Expected date of publication: 2017)

New UE law for data and IT systems protection

Regulation	GDPR	NISD
Security breaches reporting	• Data breaches must be reported as soon as possible and, where feasible, **no later than 72 hours after discovery of a breach** • Regulation will apply to companies headquartered outside of Europe as long as they have operations in Europe • Data Transfers to third countries and international organizations may only be carried out in full compliance with this Regulation • Requires Data Protection Officer	• Requires operators of essential services in the energy, transport, banking and healthcare sectors, and providers of critical digital services like search engines and cloud computing, to **take appropriate security measures and report incidents to the national authorities** • Member States will also be required to **designate a national competent authority** for the implementation and enforcement of the Directive, as well as **Computer Security Incident Response Teams (CSIRTs)** responsible for handling incidents and risks

New UE law for data and IT systems protection

Regulation	GDPR

Penalties	• GDPR states that all penalties must be effective, proportionate to the offense, and dissuasive, i.e.:
	  • Fine: **10,000,000 Euros or 2% Global Turnover**, for offenses related to:
	  o Child consent;
	  o Transparency of information and communication;
	  o Data processing, security, storage, breach, breach notification; and
	  o Transfers related to appropriate safeguards and binding corporate rules.
	  • Fine: **20,000,000 Euros or 4% of Global Turnover**, for offenses related to:
	  o Data processing;
	  o Consent;
	  o Data subject rights;
	  o Non-compliance with DPR order; and
	  o Transfer of data to third party.
	• The penalty will be whichever number is greater, either the flat fine or the percentage of global turnover.
	• Global turnover applies to all sales of a company, net of taxes. GDPR authorizes penalties in the event of both material and non-material damages.

ISSA: Practical Steps for Compliance with New EU Data Privacy Regulations

1. Locate the data
2. Define access
3. Identify and manage security risks

Avoid the "checklist" approach to security

More information: ISSA Journal February 2017, Patrick Looney, "Practical Steps for Compliance with New EU Data Privacy Regulations".

25 years | CLICO

Practical Steps for Compliance with New EU Data Privacy Regulations

1. Locate the data	It is important to understand the data within the organization by knowing the range of data formats that contain personal information (e.g., databases, file storages, backups, multimedia files, metadata associated with image files, etc.).

Practical Steps for Compliance with New EU Data Privacy Regulations

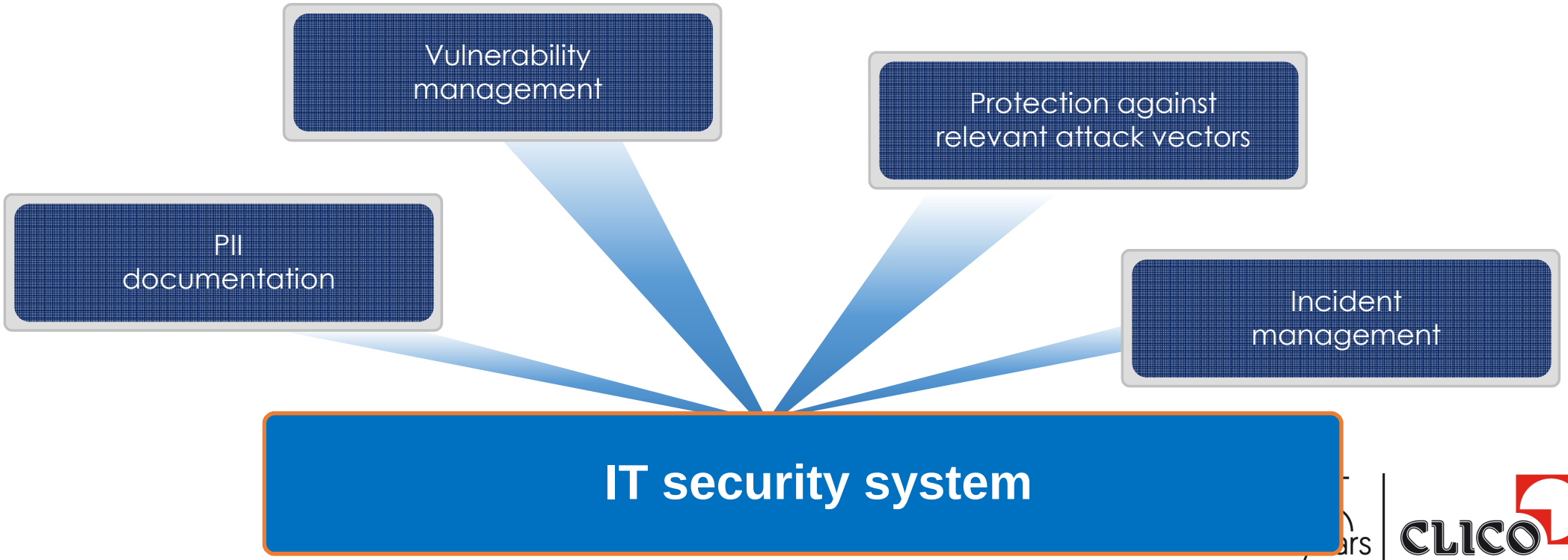
2. Define access	"High standard of protection" for personal data and this standard to be maintained across the enterprise, which includes third parties and operations in other countries.

Practical Steps for Compliance with New EU Data Privacy Regulations

3. Identify and manage security risks	The companies need to understand the security risks and the threats associated with these risks versus how their controls and measures are performing; the combination of these two factors gives the ability to quantify risk and identify areas for improvement and investment.

How to protect PII?

Defense-in-Depth



Quick GDPR audit

1.	Intentional or accidental leakage of personal data due to **employees' fault**	**Security Awareness** **Next-Gen Firewall** **DLP**
2.	Leakage of personal data due to **malware infection on employees' computers**	**Next-Gen Firewall** **Anti-Virus** **Sandboxing** **Endpoint security** **Data Encryption** **…**

25 years | CLICO

Quick GDPR audit

3.	Leakage of personal data as a result of **hacking into Web application**	**WAF - Web Application Firewall**
4.	Leakage of personal data as a result of **hacking into database**	**DBFW - Database Firewall** **DB Encryption**
5.	Leakage of personal data as a result of **hacking into file server**	**File Firewall** **File Encryption**

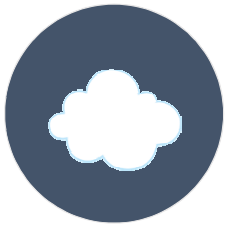
Quick GDPR audit

6.	Leakage of personal data as a result of **hacking into mobile device**	**MDM - Mobile Device Management**
7.	Leakage of personal data as a result of **hacking into privileged user account**	**PAS - Privileged Account Security**
8.	Leakage of personal data as a result of **unauthorized VPN/RAS access**	**Strong User Authentication**
9.	Leakage of personal data as a result of **hacking or unauthorized use of cloud applications**	**CASB - Cloud Access Security Broker**

Encryption as recommended PII protection

- Comprehensive Data Protection
  - VM Instance (ProtectV)
  - File, Directory, Partition (ProtectFile)
  - Database (ProtectDB)
  - Application (ProtectApp)
  - Network (High Speed Encryptor)
- Centralized Key Management (KeySecure)
- Secure Key Storage (Luna Hardware Security Module)

gemalto
security to be free



Run workloads securely in a multi-tenant environment

Safe decommission of data

Separation of duties between cloud service provider, storage, security and other administrators

Meet compliance and regulatory mandates

25 years | CLICO

Encryption as recommended PII protection

Vormetric Data Security Manager (DSM)

Many deployment forms:

- **Virtual Appliance**
- **Physical Appliance (FIPS 140-2 Level 2 Certified)**
- **Physical Appliance with HSM (FIPS 140-2 Level 3 Certified)**

- **Manage Key's**
- **Manage Policy's**
- **Audit Access**
- **Encryption**
- **Strong (AES 256)**
- **Transparent**
  (MetaClear™, US Pat)

THALES

Common Criteria

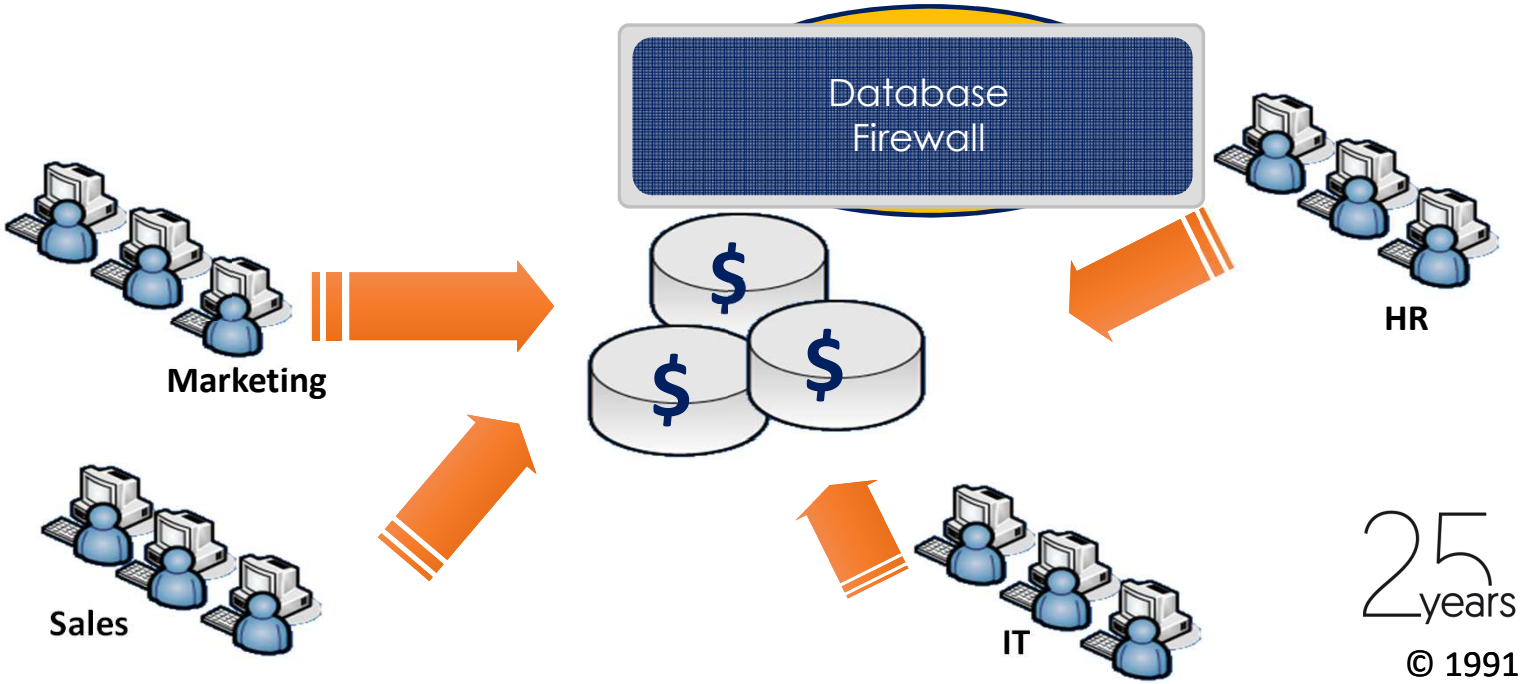
FIPS VALIDATED 140-2

25 years | CLICO

PII protection in databases

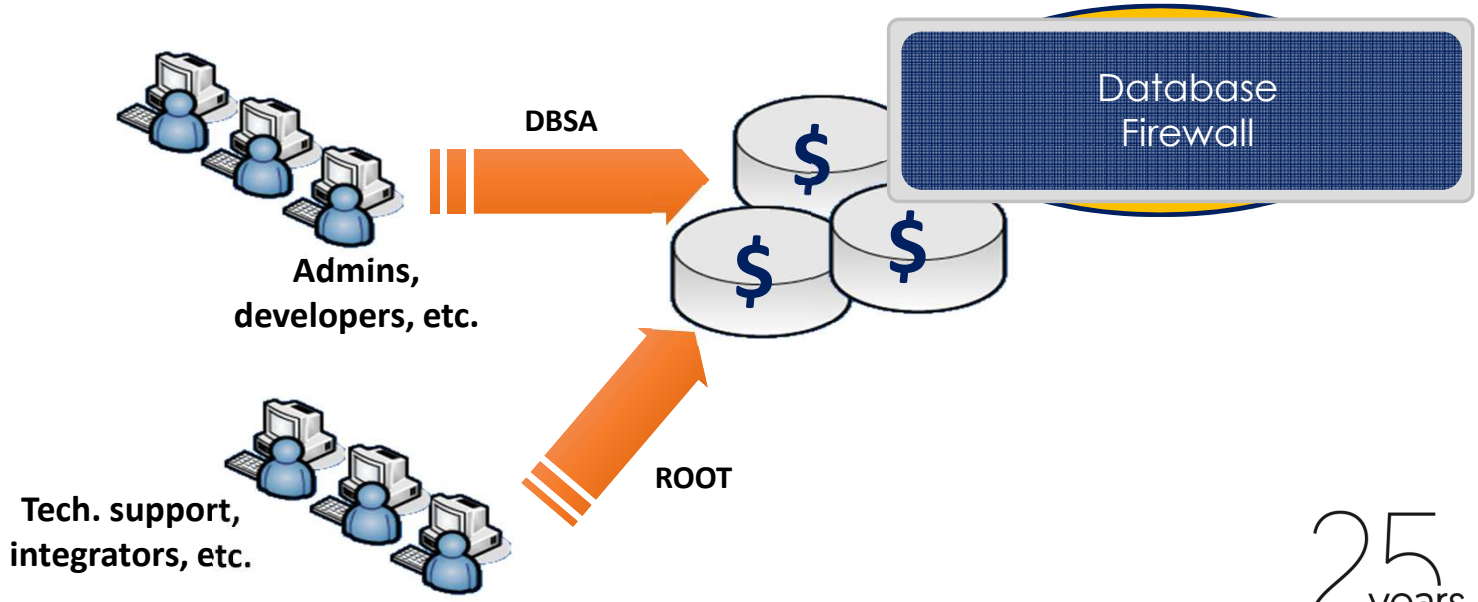
"Need to Know" principle difficult to execute for the users in databases

- Often, multiple databases in the organization, developed independently
- Often, the user accounts in the applications different then in the databases
- Often, the access rights are defined in many places (e.g. in different apps and databases)



PII protection in databases

Privileged users (e.g. system administrators, database administrators, application administrators, application developers, technical support, auditors) often have unlimited access (and practically uncontrolled) to PII and other sensitive data.

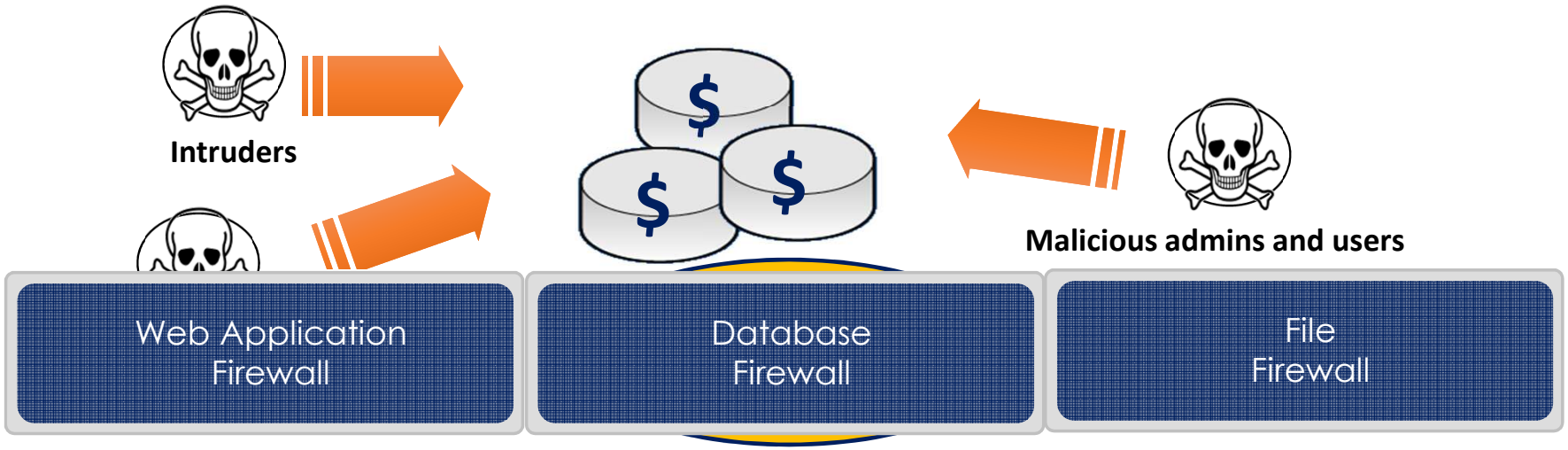


25 years | CLICO

PII protection in databases

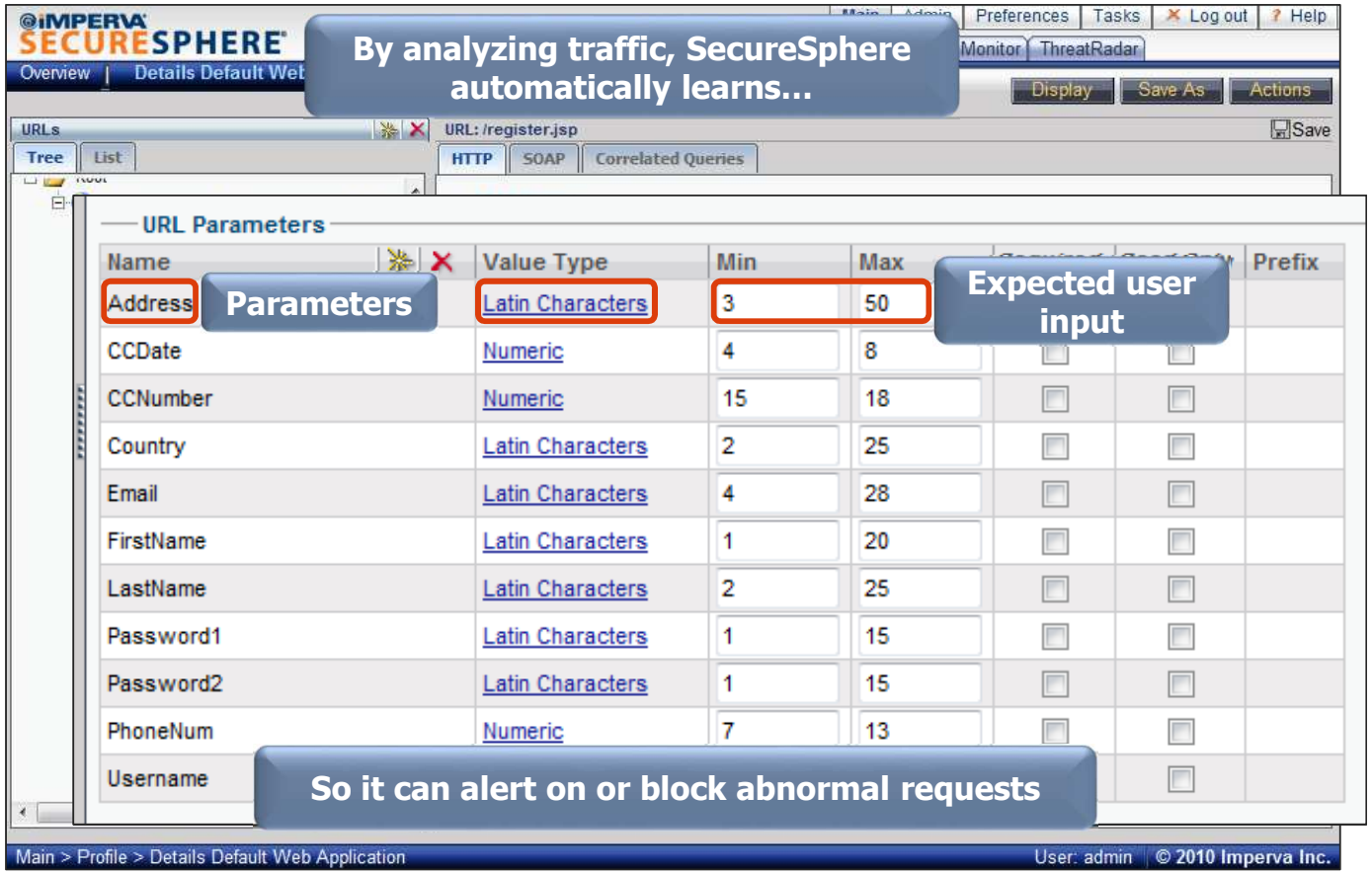
Maintaining the database security is difficult

- Many attack vectors (exploit, SQL-I, privilege misuse, etc.)



- Problems installing security patches in production databases

Imperva Web Security



- Conventional protections like FW/UTM and IPS are not able to protect against specific Web attacks (eg SQL-I)
- **The only effective Web security solution is Web Application Firewall (WAF)**

IMPERVA

25 years | CLICO

Imperva Database Security

IMPERVA®

- **SecureSphere Database Activity Monitoring**

  + Full auditing and visibility into database data usage

- **SecureSphere Database Firewall**

  + Activity monitoring and real-time protection for critical databases

- **SecureSphere Discovery and Assessment Server**

  + Vulnerability assessment, configuration management, database discovery and classification

- **User Rights Management for Databases**

  + Review and manage user access rights to sensitive databases

- **ADC Insights for SAP, Oracle EBS and PeopleSoft**

  + Pre-packaged reports and rules for SAP, Oracle EBS and PeopleSoft compliance and security

SAP ORACLE e-businesssuite ORACLE PEOPLESOFT ENTERPRISE

Detailed Audit Trail

IMPERVA®

SecureSphere automates the creation of a continuous audit process

Complete Audit Trail

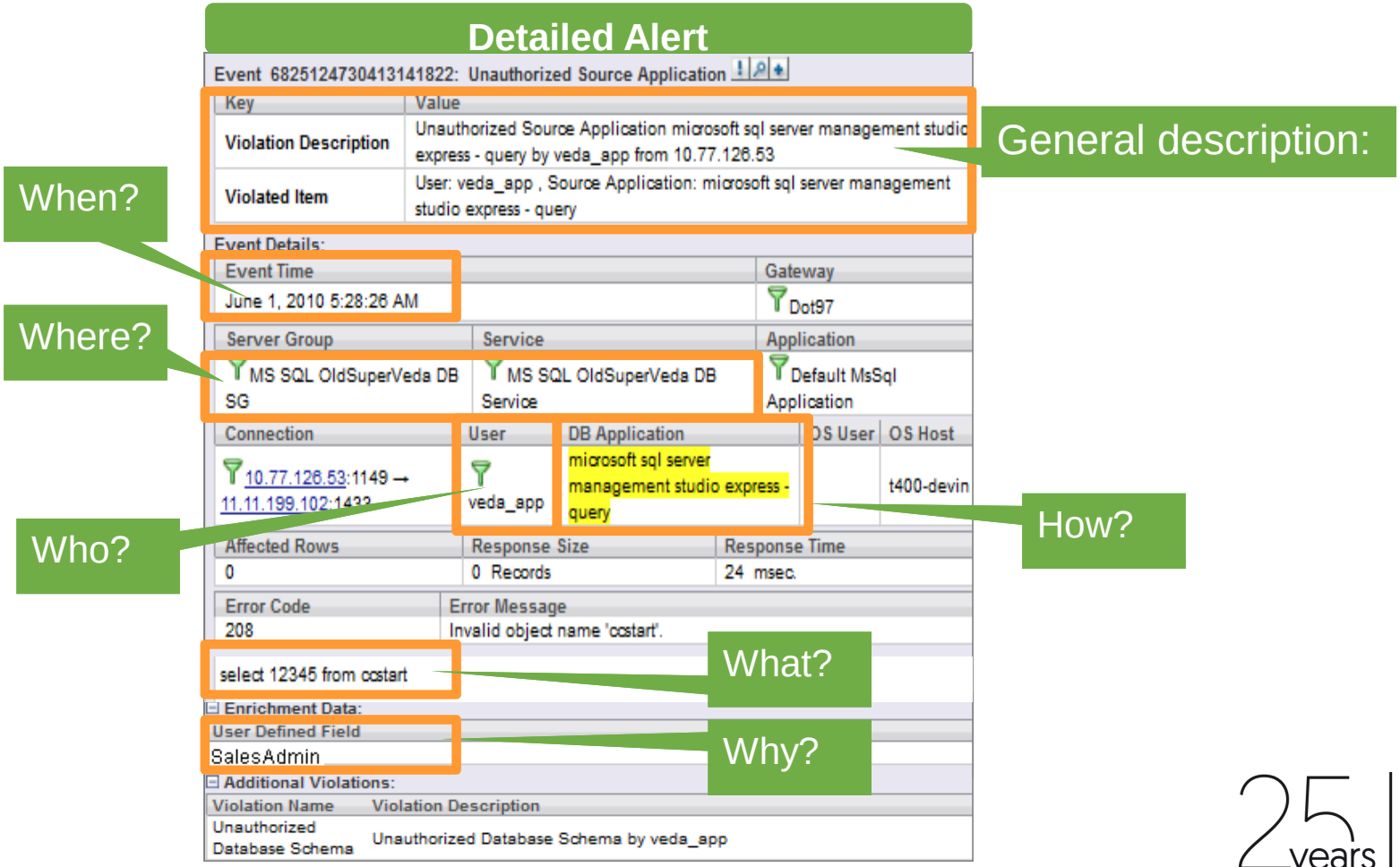
Event Date and Time	Source IP	User	Destination IP	Service	Source Application	Query
User: erez (7)						
June 10, 2010 5:09:54 PM	192.168.0.110	erez	11.11.199.122	Solaris Oracle Service	sqlplusw.exe	CREATE OR REPLACE FUNCTION MYFUNC
June 10, 2010 5:09:01 PM	192.168.0.110	erez	11.11.199.122	Solaris Oracle Service	sqlplusw.exe	select * from table_users
June 10, 2010 5:08:51 PM	192.168.0.110	erez	11.11.199.122	Solaris Oracle Service	sqlplusw.exe	SELECT ATTRIBUTE,SCOPE,NUMERIC_VAL
June 10, 2010 5:08:51 PM	192.168.0.110	erez	11.11.199.122	Solaris Oracle Service	sqlplusw.exe	SELECT CHAR_VALUE FROM SYSTEM.PRO
June 10, 2010 5:07:22 PM	192.168.0.110	erez	11.11.199.122	Solaris Oracle Service	sqlplusw.exe	SELECT ATTRIBUTE,SCOPE,NUMERIC_VAL
June 10, 2010 5:07:22 PM	192.168.0.110	erez	11.11.199.122	Solaris Oracle Service	sqlplusw.exe	SELECT CHAR_VALUE FROM SYSTEM.PRO
June 10, 2010 4:58:55 PM	192.168.0.110	erez	11.11.199.122	Solaris Oracle Service	sqlplusw.exe	SELECT "SPW_LANGUAGE","SPW_WORD",""
User: foo (18)						
March 31, 2010 10:44:49 PM	10.77.126.93	foo	11.11.199.122	Solaris Oracle Service	sqlplusw.exe	drop table testpriv
March 31, 2010 10:44:41 PM	10.77.126.93	foo	11.11.199.122	Solaris Oracle Service	sqlplusw.exe	truncate table testpriv

When? **Who?** **Where?** **How?** **What?**

25 years | CLICO

Real–Time, Detailed Alerts

IMPERVA

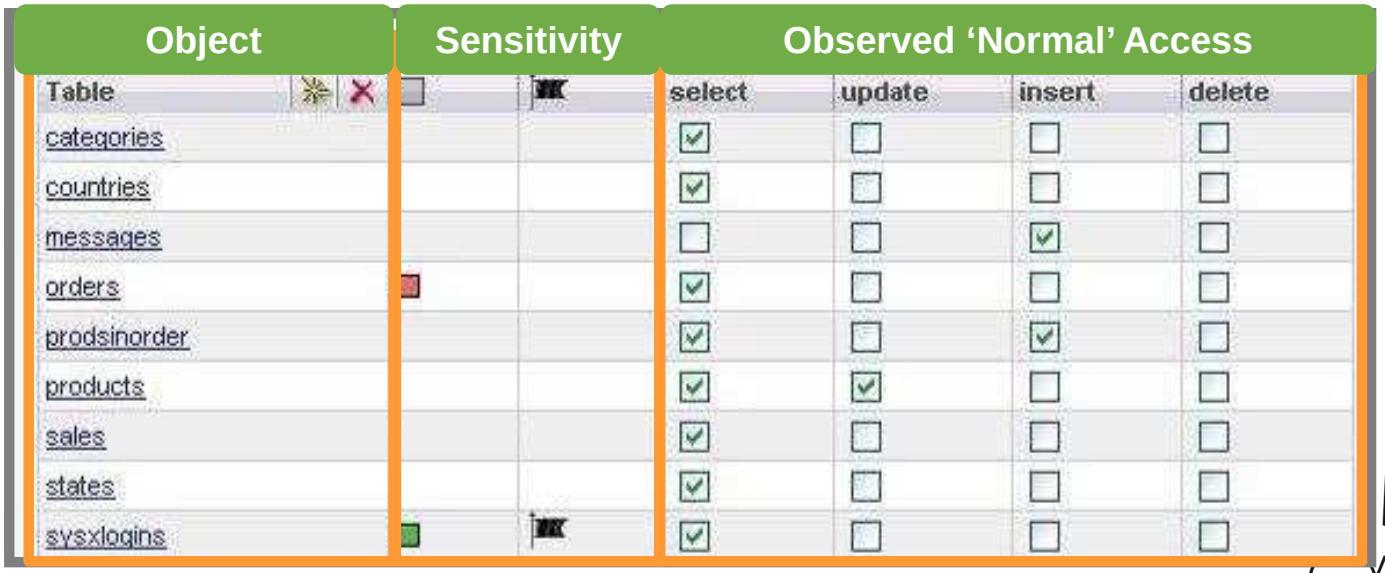


25 years | CLICO

Identifying Abnormal Behaviors

IMPERVA

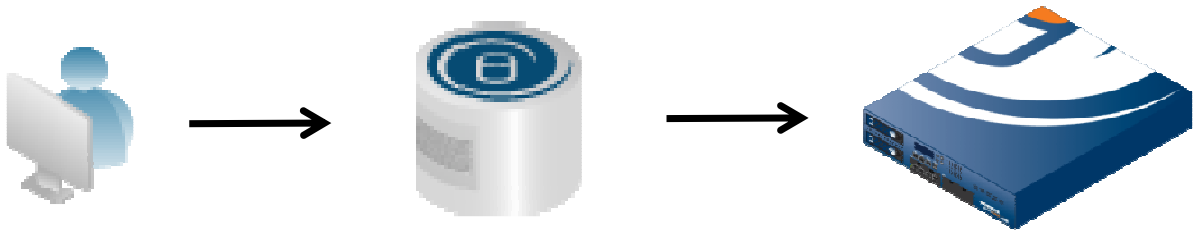
- Usage profile built for each user to represent 'normal behaviour'
- Continuously updates –> significantly reduces manual updates
- Profile deviations create an alert and can be blocked



Auditing Local Privileged Activity

IMPERVA

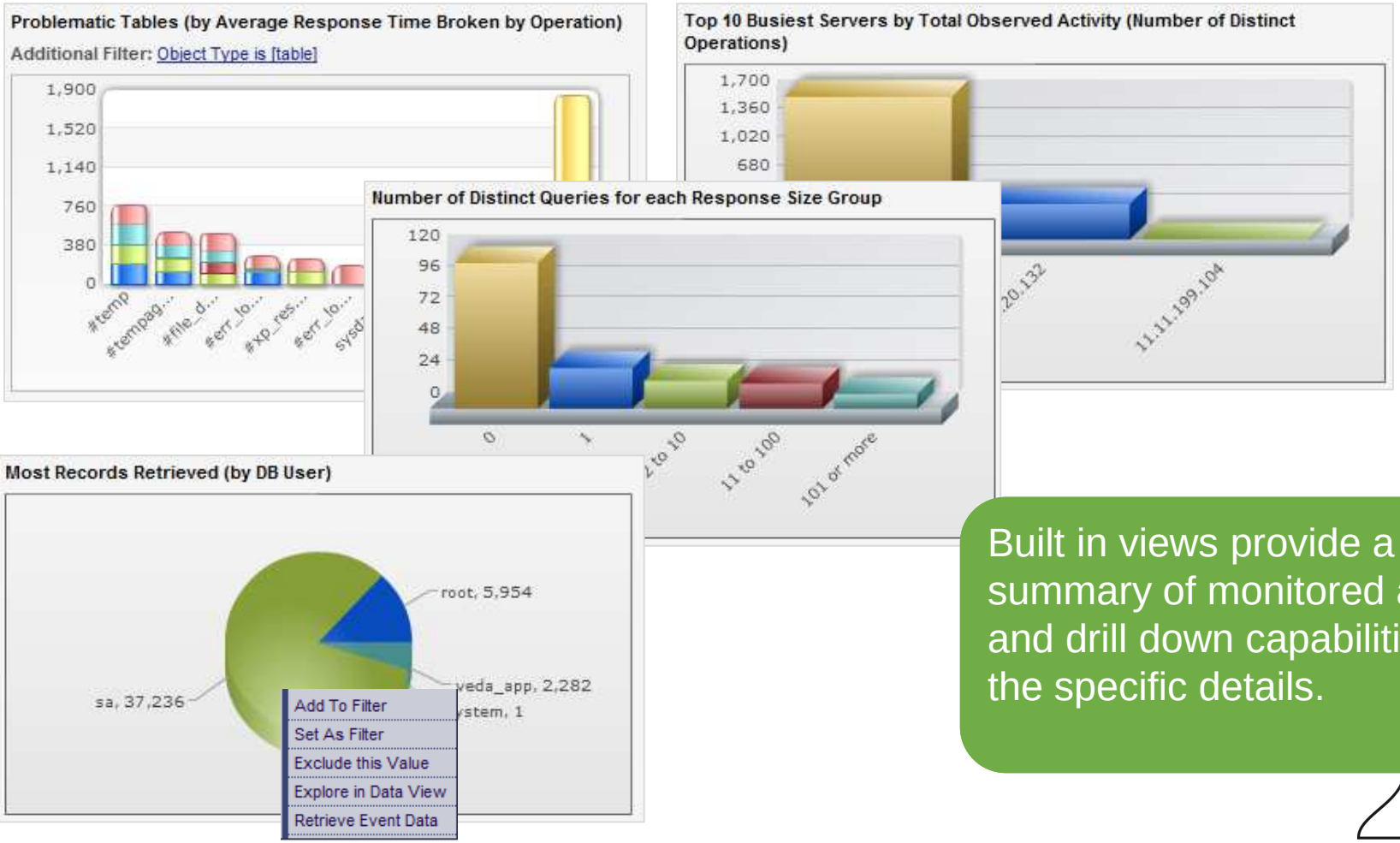
- SecureSphere utilizes lightweight agents to monitor database activity performed locally on the database server
- The agents eliminate blind spots by monitoring internal network communications
- The agents send the data to the appliance where it is parsed analyzed and stored in the audit trail
- The agent is completely independent of the RDBMS



25 years | CLICO

Performance Management

IMPERVA



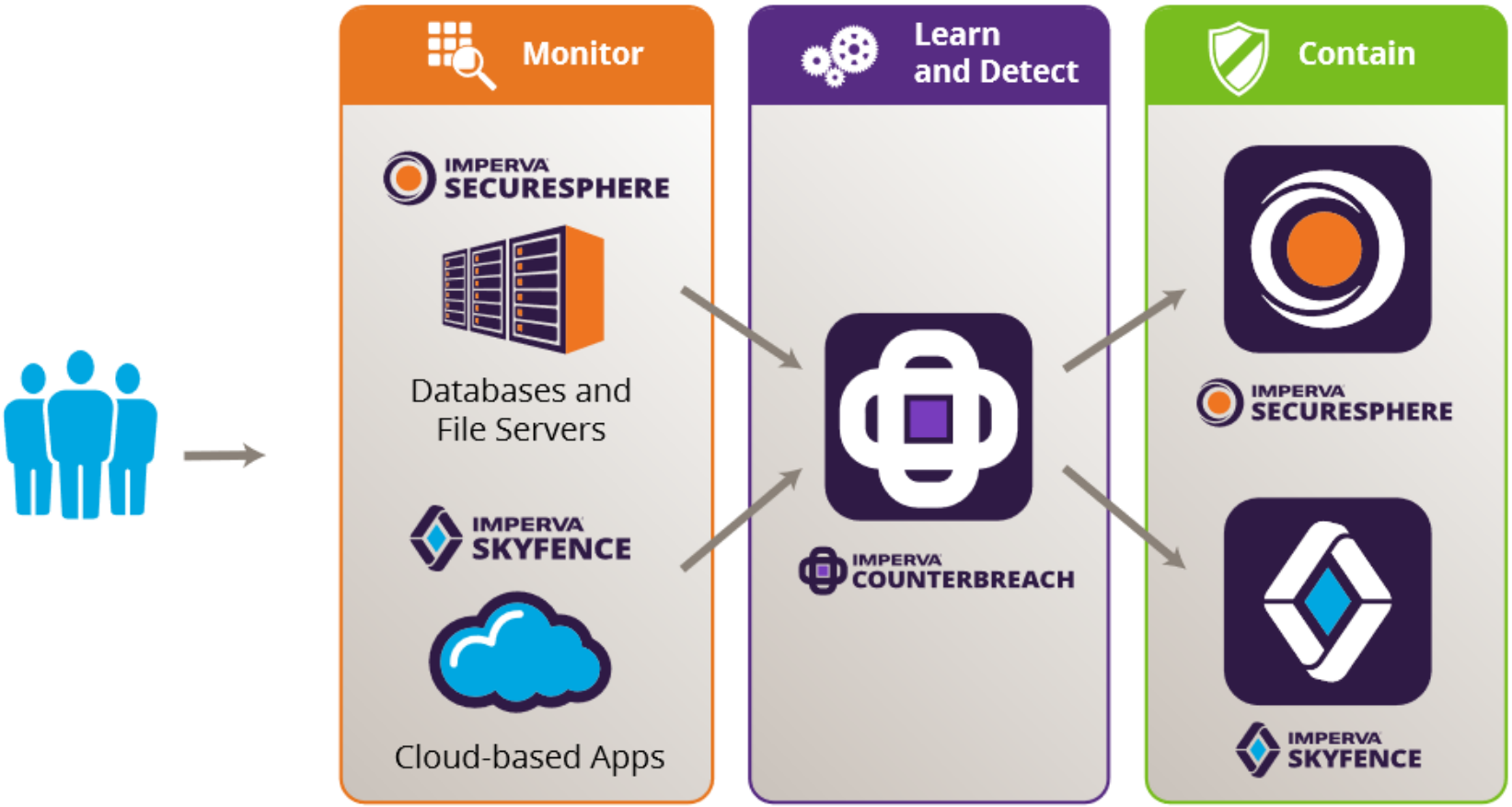
Built in views provide a summary of monitored activities and drill down capabilities into the specific details.

25 years | CLICO

Imperva CounterBreach

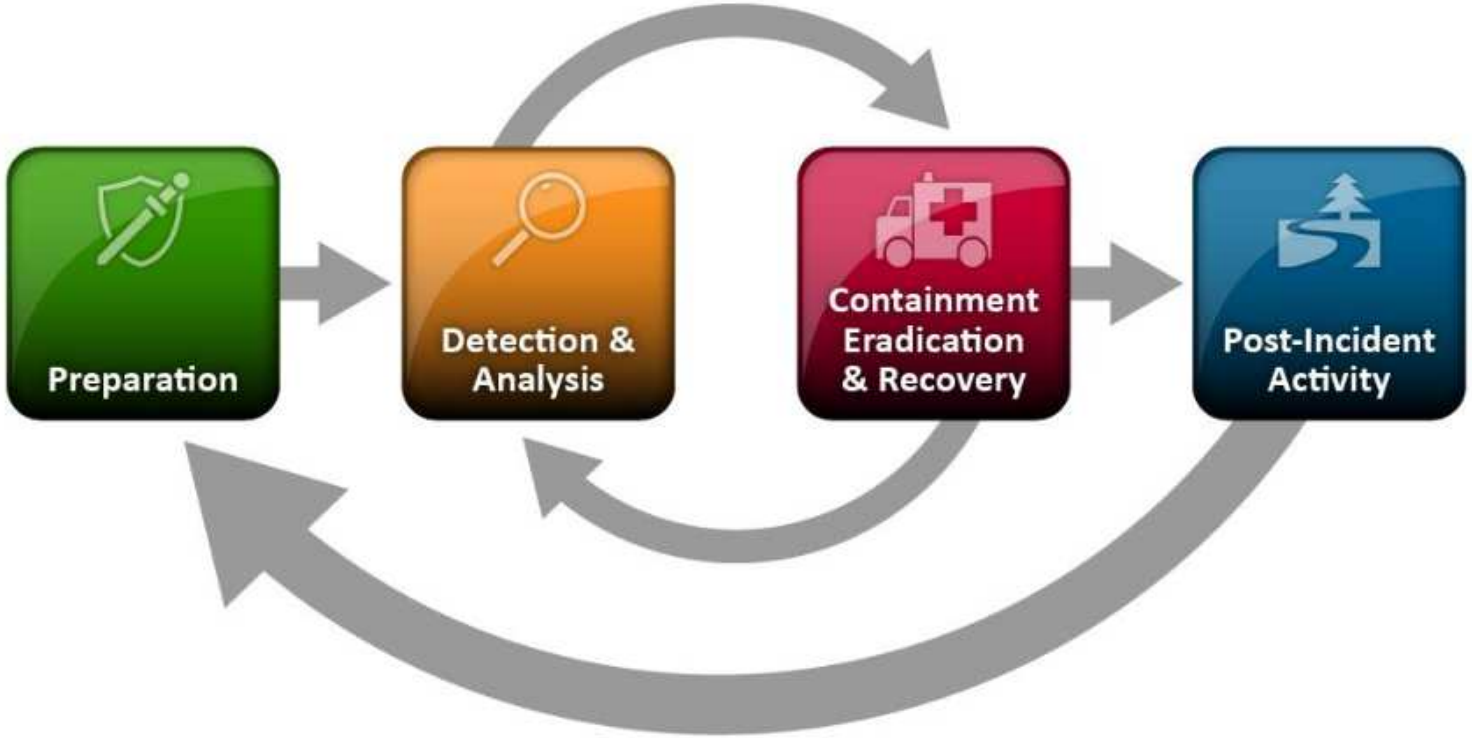
User Behavior Analytics in databases and cloud

IMPERVA



25 years | CLICO

How to manage the incidents?



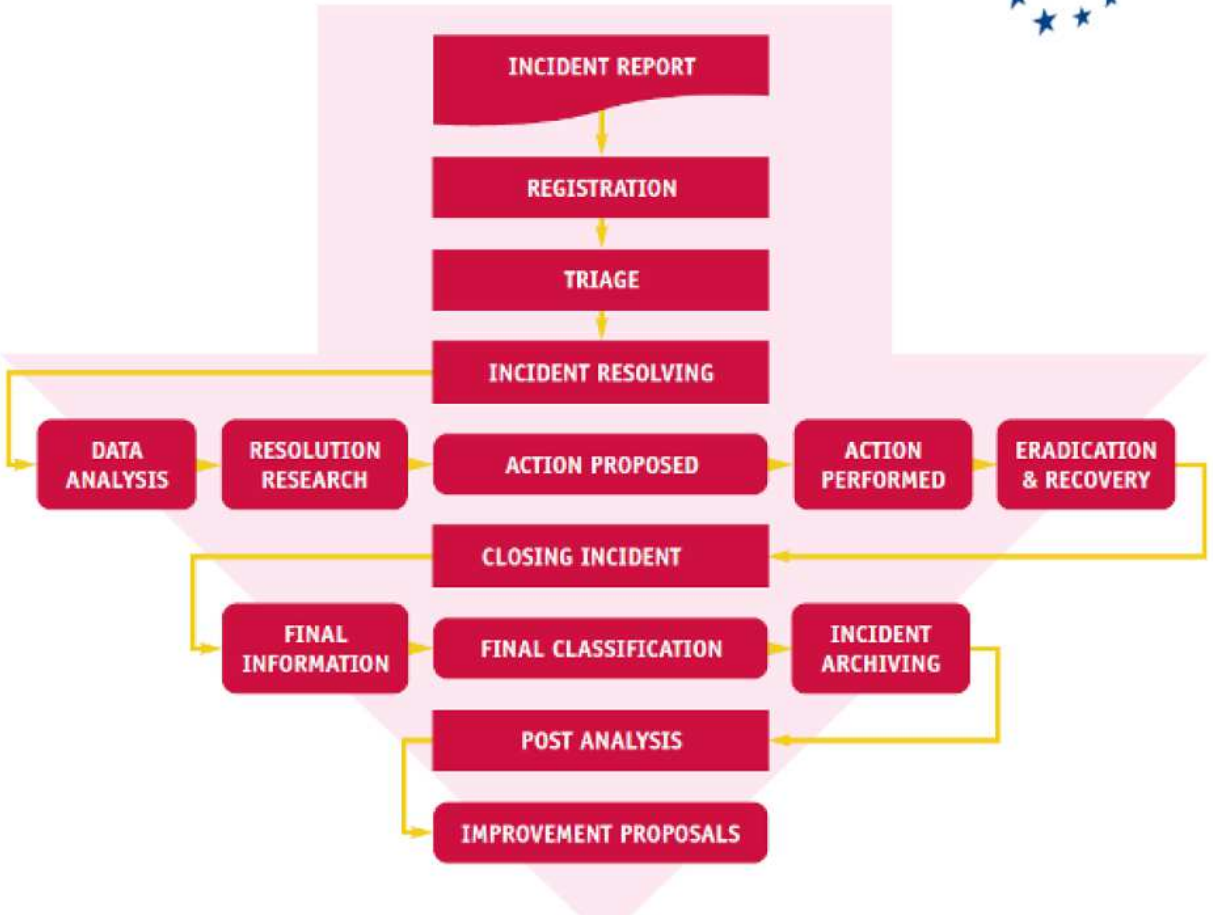
More information: "Computer Security Incident Handling Guide", NIST 2012

How to manage the incidents?

More information: "Incident Handler's Handbook", SANS Institute 2011

How to manage the incidents?

enisa European Union Agency for Network and Information Security

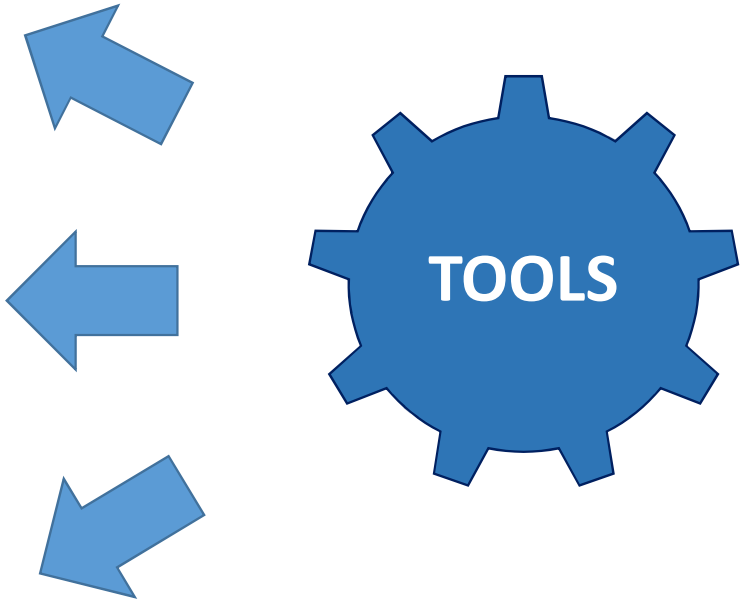


More information: "Strategies for incident response and cyber crisis cooperation", ENISA 2016

ars | CLICO

How to manage the incidents?

1. Incident Identification
2. Triage
3. Classification
4. Notification
5. Containment
6. Evidence Collection
7. Chain of Custody
8. Eradication
9. Recovery
10. Forensics Analysis
11. Root Cause Analysis
12. Lessons Learned



Legacy SIEM

and when the destination port is one of the following 53
and when the IP protocol is one of the following UDP.udp_ip
and when the source packet rate is greater than 3 packets/second
and NOT when the source IP is one of the following 10.1.75.10/32

and when the source IP is one of the following 10.1.11.0/24
and when the event category for the event is one of the following Access.Access Denied, Access.ACL Deny

and when the source IP is one of the following 10.1.75.10/32
and NOT when the destination IP is one of the following 10.1.11.200/32
and NOT when the destination port is one of the following 22

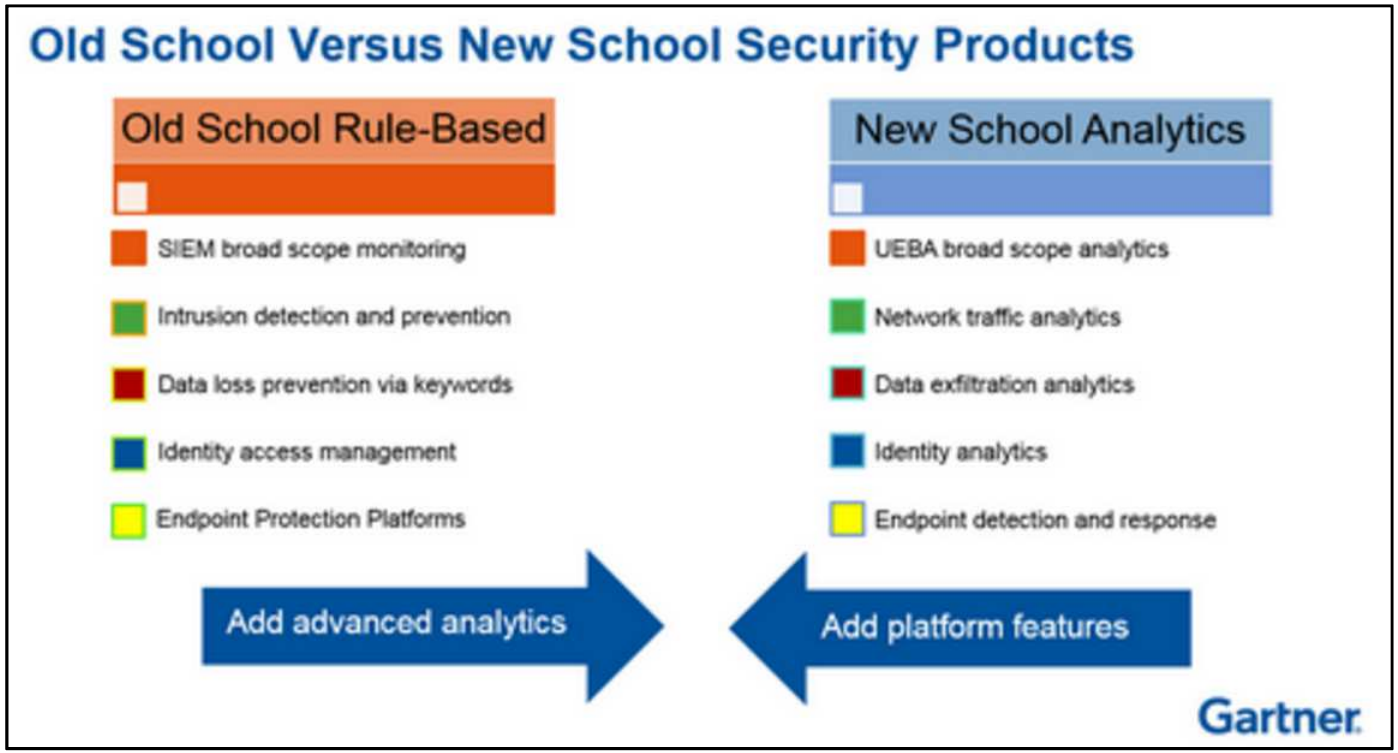
STATIC RULES

Manually added and updated rules, IP addresses, port numbers, etc.

LOG SERVER

25 years | CLICO

„The Coming UBA / UEBA – SIEM War!" - Gartner

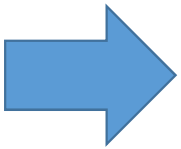


More information: http://blogs.gartner.com/anton-chuvakin/2016/11/07/the-coming-uba-ueba-siem-war/

How to manage the incidents?

Legacy SIEM (static rules)

Legacy IDS/IPS (patterns)



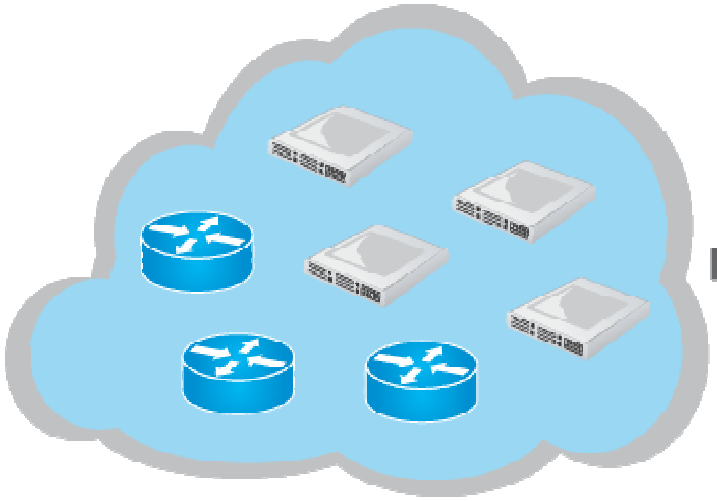
exabeam

Flowmon Networks

25 years | CLICO

Network Behavior Analysis

Flowmon Networks



LAN/WAN with FlowMon Probes
or NetFlow compatible devices

NetFlow
Export

FlowMon
Collector

Network Visibility
Traffic Monitoring

Network Security
Anomaly Detection

Troubleshooting
Network Optimization

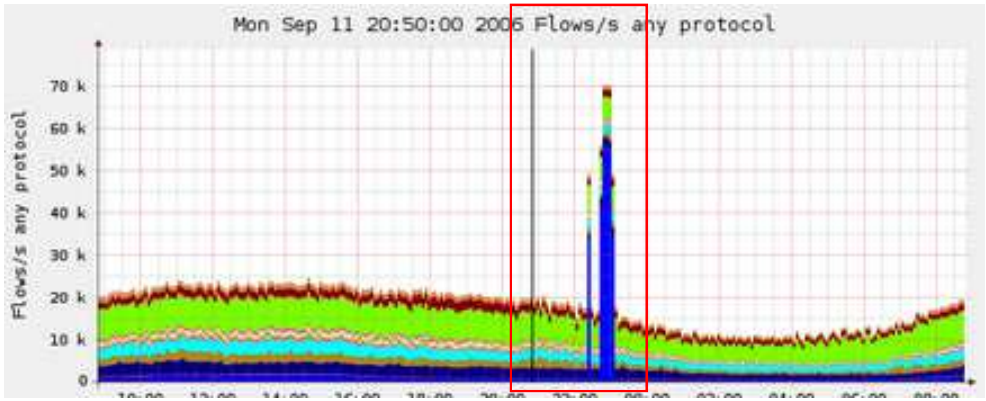
Alerting, Reporting
Billing & Accounting

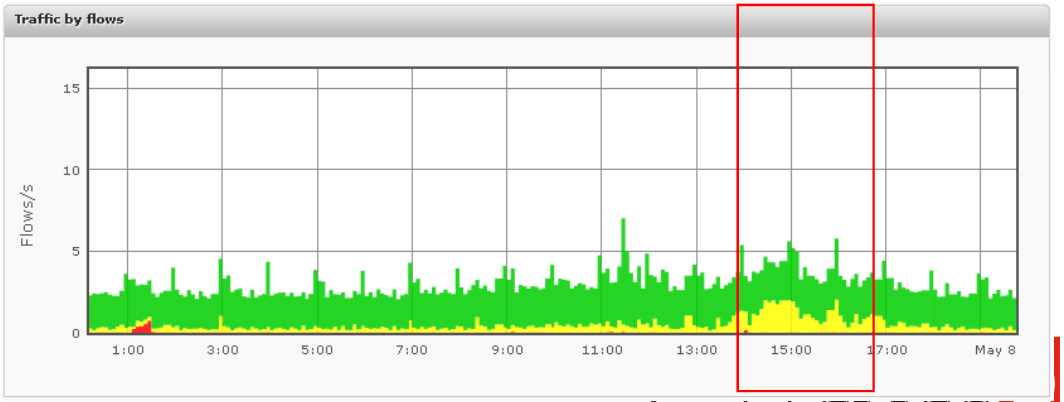
25 years | CLICO

Network Behavior Analysis (NBA)

Flowmon Networks

- Creates profiles of normal computers behavior from flows read from the network devices (as well as SPAN ports and network taps)
- Identifies security incidents based on deviations from the behavior profiles and typical anomalies (e.g. DNS tunneling, port scanning, C&C connections)





years | CLICO

Network Behavior Analysis (NBA)

Flowmon Networks

Flowmon ADS

- Machine Learning
- Adaptive Baselining
- Heuristics
- Behavior Patterns
- Reputation Databases

15 years | CLICO

Key facts about Flowmon

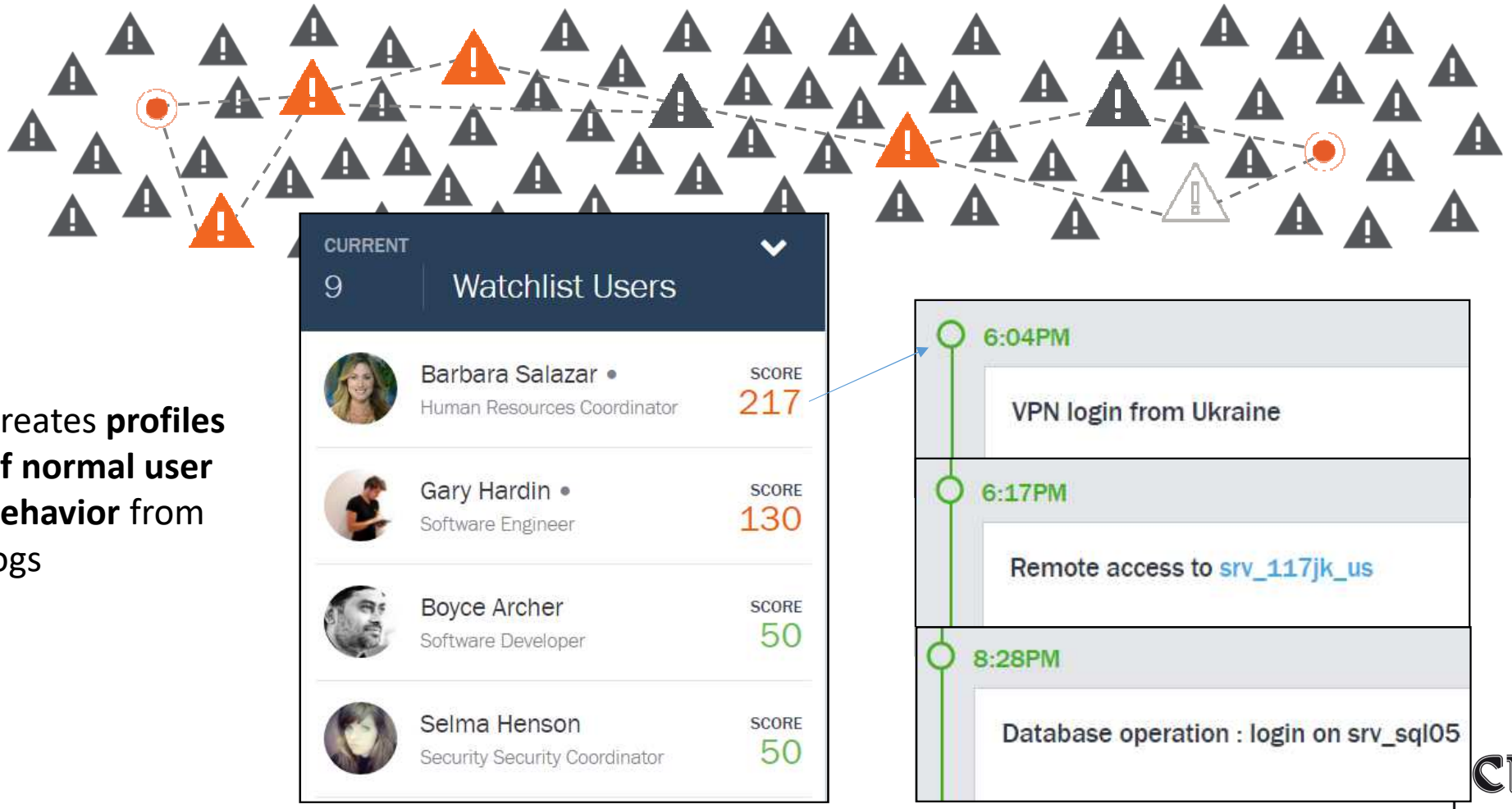
Flowmon Networks

1. Creates **profiles of normal computers behavior** from flows read from the network devices
2. Identifies security **incidents based on deviations** from the behavior profiles
3. Detects **incidents automatically**, no need for writing of correlation rules
4. It does **not require installation of the agents** on user computers
5. Useful in incident management as well as **application performance monitoring and network troubleshooting**

25 years | CLICO

User and Entity Behavior Analytics (UEBA / UBA)

exabeam



Creates **profiles of normal user behavior** from logs

CLICO

UEBA / UBA

exabeam

From 2013

2015 Gartner Cool Vendor
Security Intelligence

2016 IBM Beacon Award
Outstanding Security Solution

Network World Asia, Information Management Awards 2016
Most Promising User Behavior Analytics Solution

Network Products Guide IT World Awards 2016
Gold – Innovative Company of the Year
Gold – Hot Companies
Silver – New Products and Services
Silver – Best IT Company of the Year (Software)
Bronze – Insider Threat Detection and Solutions
Bronze – Startup of the year (founded 2013)

Silicon Review Top 10
Analytics Companies

Dark Reading Top 20
Cyber Security Startup

CRN Emerging Vendor Awards 2015
Winner—Emerging Security Vendor Award

Cyber Security Excellence Awards 2016
Finalist—Most Innovative Cybersecurity Company

Co-Founder

Shlomo Kramer

25 years | CLICO

Key facts about Exabeam

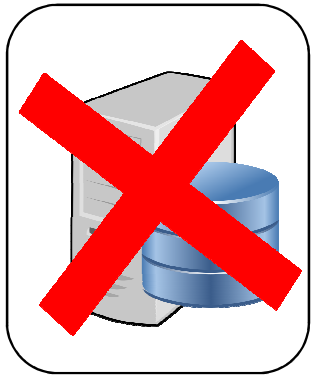
exabeam

1. Creates **profiles of normal user behavior** from logs read from SIEM and other data sources
2. Identifies security **incidents based on deviations** from the user behavior profiles
3. Detects **incidents not visible to SIEM**, including security breaches with passwords stolen for legitimate users
4. Provides **easy-to-understand and easy-to-proof evidence** of the incident, including list of specific user actions
5. It does **not require installation of the agents** on user computers
6. It can **operate with SIEM or replace it** with its own Log Management System

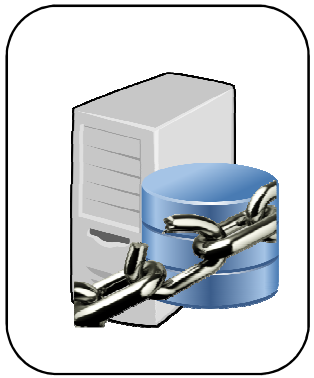
25 years | CLICO

SOC: Identify and manage security risks

Avoid serious breaches

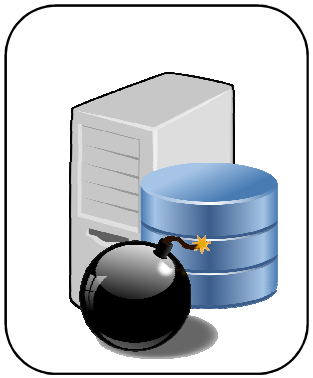


SAFE



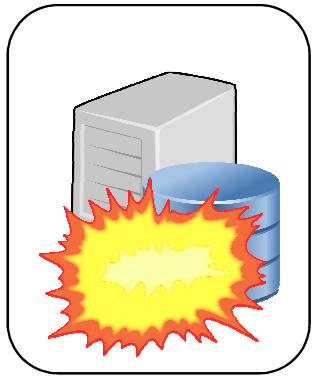
VULNERABLE

- Errors in operating systems, applications, databases, etc.
- Errors in hardware, software, configuration, human factor, etc.



INCIDENT

- Malware/intruder takes control over the system
- Hardware failure
- DoS attack



BREACH

- Disruption of business processes
- Leakage of confidential data
- Loss of image and customer confidence
- Legal consequences

Mitigate serious vulnerabilities

25 years | CLICO