

SECURITY MONITORING OF INFORMATION TECHNOLOGIES

DO YOUR EMPLOYEES NOT COMMIT CRIMINAL ACTIVITIES WITH YOUR TECHNOLOGY?

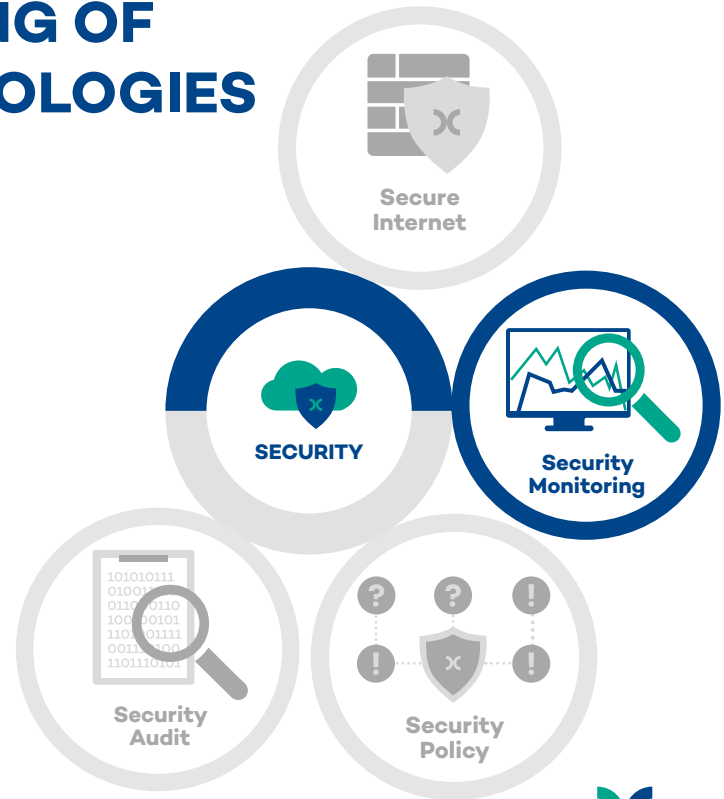
- We reliably save everything and provide you the necessary evidence.

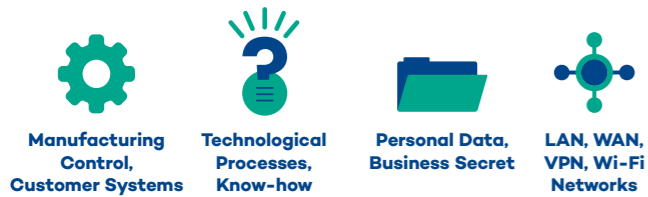
DO YOU KNOW OF CYBERNETIC ATTACKS ON YOUR DATA?

- We will find out whether you are concerned by them, and recommend appropriate measures.

ARE YOU CONCERNED BY THE CYBERNETIC LAW?

- We will set everything to meet the current legislative demands on monitoring.





```

10101101110101011010111010110101010101011000000101011
0101 DATA THEFT 01001101010010011110111101010100101110
0000101010101001 PORNOGRAPHY PROPAGATION 0110101
01010101010101010101010101011001010101110010
10101 SERVICE UNAVAILABILITY 101101010101101
0110110101110101001101011100101011011101
010101120111 PERSONAL DATA MISUSE 101
010110210101010110101011011010101
1011 FILMS DOWNLOAD 101101010
1011010110010001100100110
101011011010101101101
  
```

SECURITY MONITORING PAYS OFF

The costs spent on security monitoring will prevent much higher damages caused by:

- data loss, e.g. theft of your know-how via Internet or by employees,
- reputation loss, e.g. by putting the company on the e-mail blacklist,
- service unavailability, e.g. by disconnecting the company from e-mail and cloud services,
- misuse by IT employees for private purposes, and sometimes for illegal ones as well.

WE MONITOR IMPORTANT MATTERS

Security Events Monitoring (SIEM)

- **Collects** endless **entries** from all IT devices.
- **Archives** them for later usage.
- **Evaluates links** between entries.
- **Recognizes** only those signifying a **real threat**.
- **Presents and reports** them **understandably**.



Network Operation Monitoring

- Recognizes which **data flows** come through your network.
- Records **unusual events** in the network signifying a possible threat.
- Enriches your reports by **information from network operation**.

Vulnerability Scanner

- **Checks** all IT systems automatically and regularly, and reveals their **weak points**.
- Enables to focus on **real threats**.
- Completes the summary of real vulnerable systems, thereby **reduces the amount and increases the warning relevance**.

Application Operation Monitoring

- Monitors which **applications** mostly **use the network to full capacity** and in which time.
- Displays how much network capacity is exploited by **critical corporate applications**.
- **Finds out** which applications have **slow responses** and whether the slow responses are caused by server or by network.

SECURITY MONITORING SERVICES ACCORDING TO THE CUSTOMER NEEDS	SERVICE LEVEL	
	BASIC	PROFESSIONAL
Summary of operation, extreme events, problems with sources.	YES	YES
Reliable longtime saving of events for analyses and probative proceedings.	YES	YES
Helpdesk services.	in working hours	continuous
Automatically generated understandable reports.	monthly	monthly/weekly
Reports personally presented by our consultee.	yearly	quarterly/monthly
Real-time alarms in the form of e-mail, SMS or signal to the selected contacts.	NO	YES
Time of security consultee which can be used for Security Monitoring consultations, optimizing of its settings, involvement of new systems into monitoring and related activities in the field of security.	NO	2/4/8 hours monthly



Order
the first vulnerability scan
free of charge.

HelpDesk 24 x 7

t: +420 266 063 333 – Czech Republic
t: +421 232 292 700 – Slovakia
e: helpdesk@ixperta.com

InfoLine

t: +420 266 061 111 – Czech Republic
t: +421 232 292 722 – Slovakia
e: info@ixperta.com

PRAHA BRATISLAVA BRNO OSTRAVA ŽILINA
www.ixperta.com