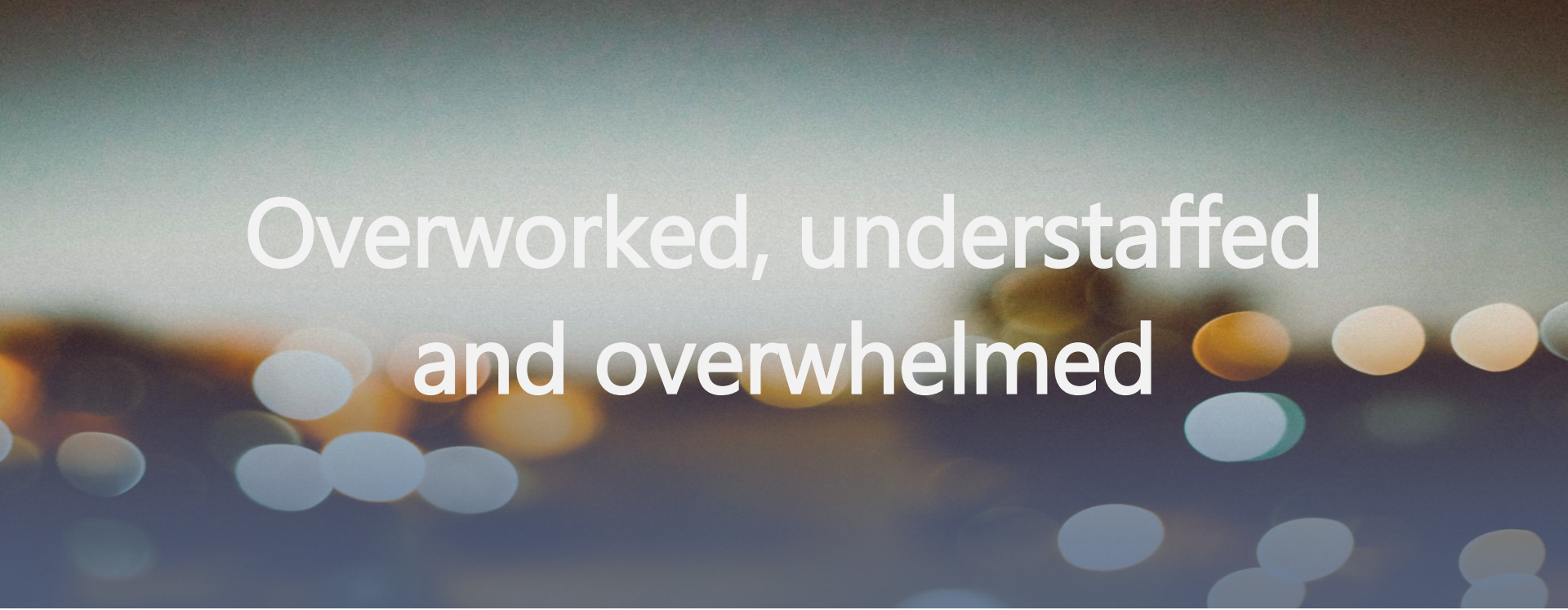
IBM Security

Automate Your SOC with AI

Lisa Unkelhäußer
Security Channel Leader

October 2019

IBM



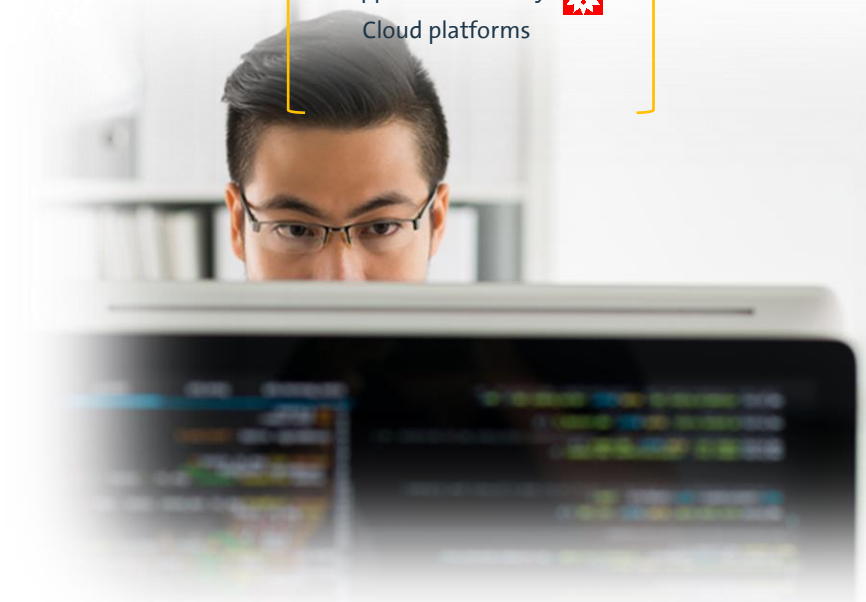
Overworked, understaffed and overwhelmed

According to ESG research, 51 percent of organizations report having a "problematic shortage" of cybersecurity skills in 2018. This is up from 45 percent in 2017.

Investigating an incident without AI

- Endpoints
- Network activity
- Data activity
- Users and identities
- Threat intelligence
- Configuration information
- Vulnerabilities and threats
- Application activity
- Cloud platforms

Gain local context leading to the incident → **Gather the threat research, develop expertise** → **Apply the intelligence and investigate the incident** → **Escalate for remediation**



Time consuming and inconsistent threat analysis

There's got to be a better way!

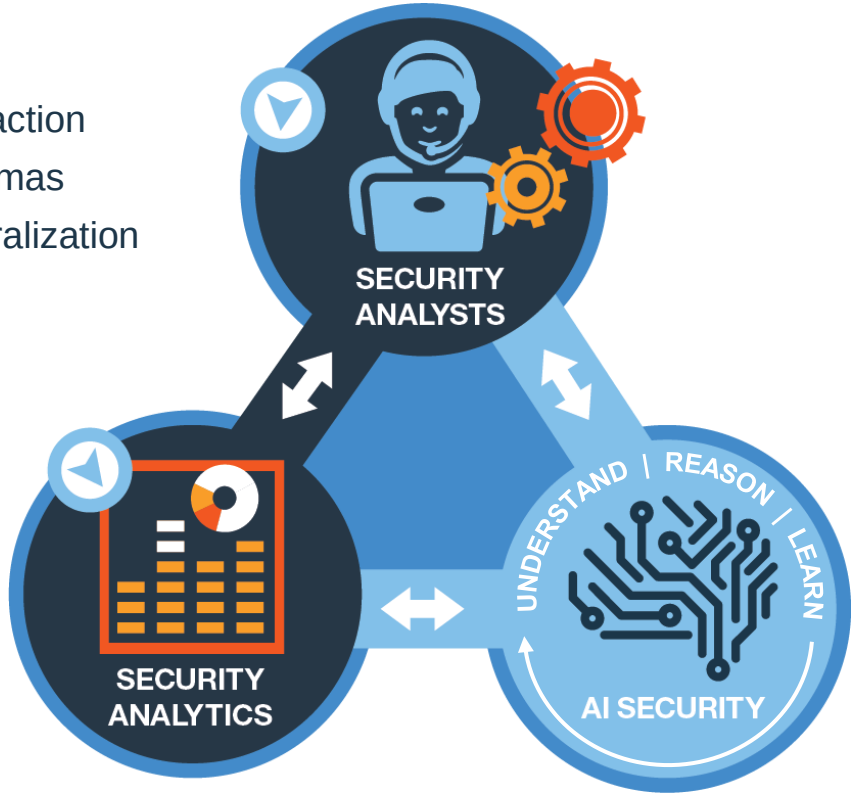
Unlock a new partnership between analysts and their technology

Human Expertise

- Common sense
- Morals
- Compassion
- Abstraction
- Dilemmas
- Generalization

Security Analytics

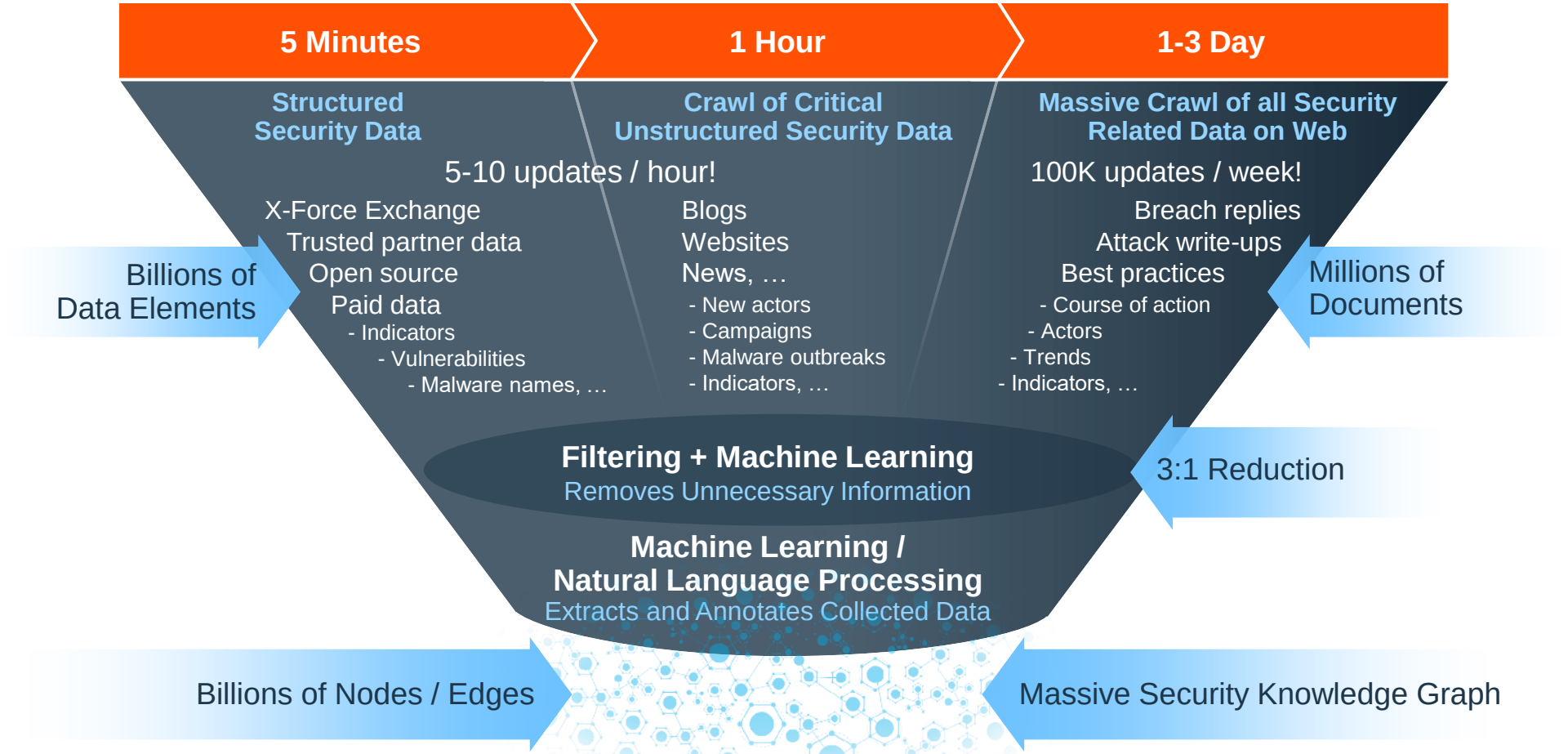
- Data correlation
- Pattern identification
- Anomaly detection
- Prioritization
- Data visualization
- Workflow



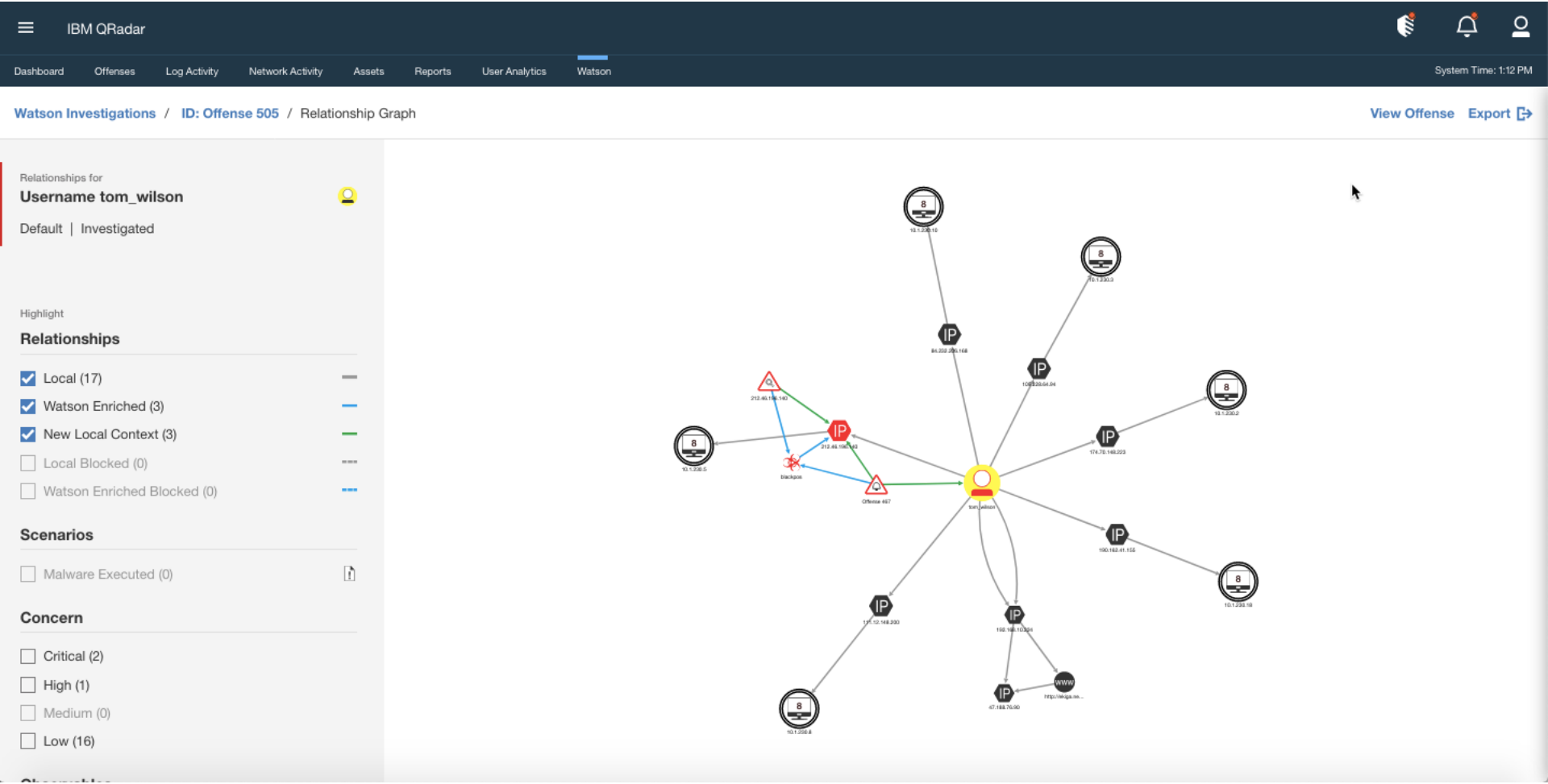
Artificial Intelligence

- Cognitive capabilities
- Unstructured analysis
- Natural language
- Machine learning
- Bias elimination
- Tradeoff analytics

How it works – Building the knowledge (internal and external)



Attach the knowledge into your SIEM

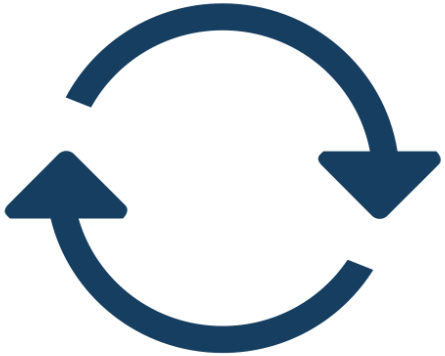


Using analyst feedback to drive better decisions

Learning

Tier 2 Analysts

In-depth investigations; incident response



Tier 1 Analysts

First line triage; gather info and escalate to Tier 2

Applying

Offense #152

Advisor Recommendation:
De-prioritize this investigation.

Offense #152 is similar to Offense #29, #53 and #112, all of which you marked as false positive in the past.

Offense #221

Advisor Recommendation:
Escalate this investigation.

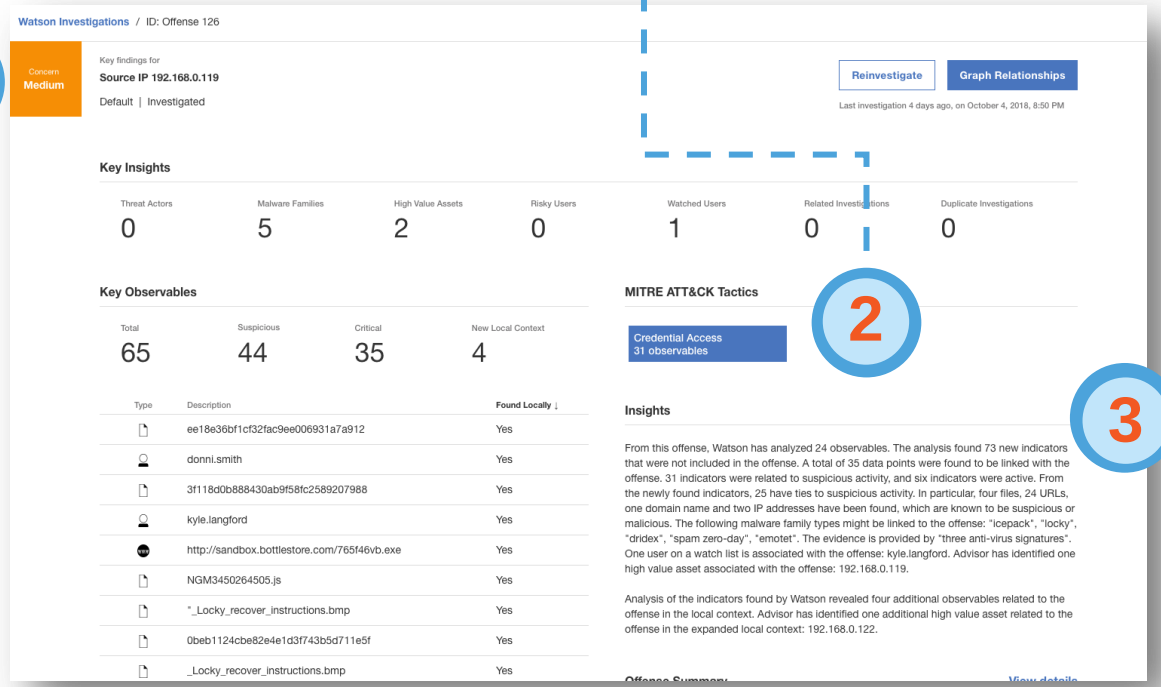
Offense #221 is similar to Offense #42 and #68, both of which you escalated in the past.

And finally aligning incidents to the ATT&CK chain

Confidence level for each progression validates the threat

Visualize how the attack has occurred and is progressing

Uncover what tactics can still possibly occur



IBM Security

THANK YOU

FOLLOW US ON:

- ibm.com/security
- securityintelligence.com
- xforce.ibmcloud.com
- @ibmsecurity
- youtube/user/ibmsecuritysolutions

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.

IBM