

Automate Your SOC with AI



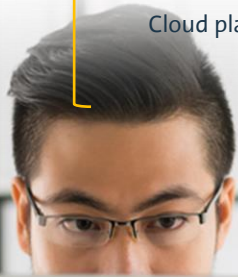
Lisa Unkelhäußer
Security Channel Leader

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



There's got to be a better way!

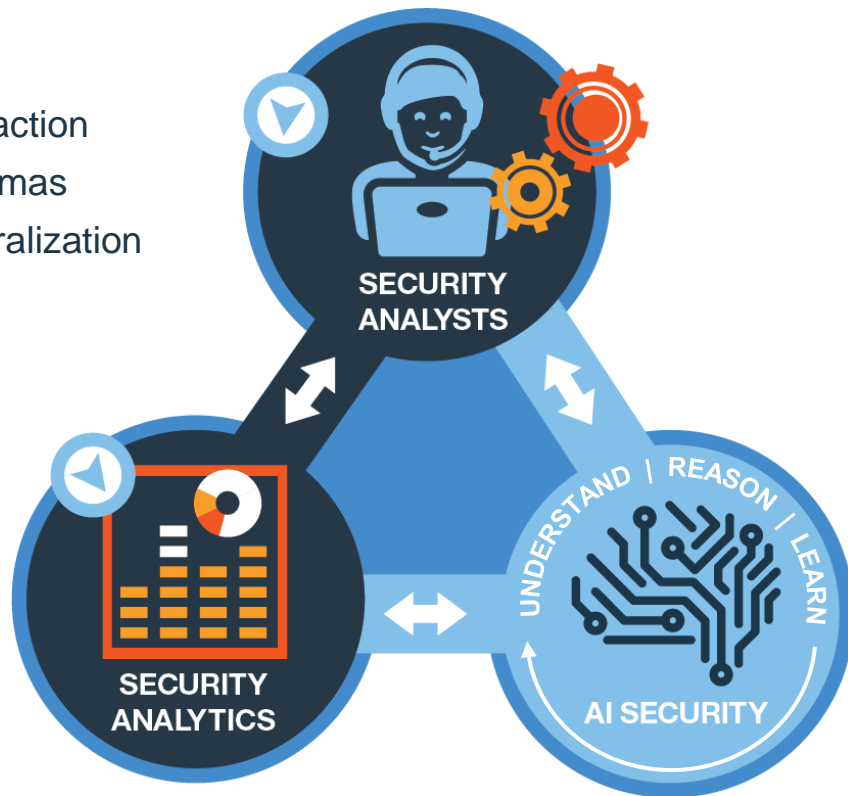
Unlock a new partnership between analysts and their technology

Human Expertise

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

Security Analytics

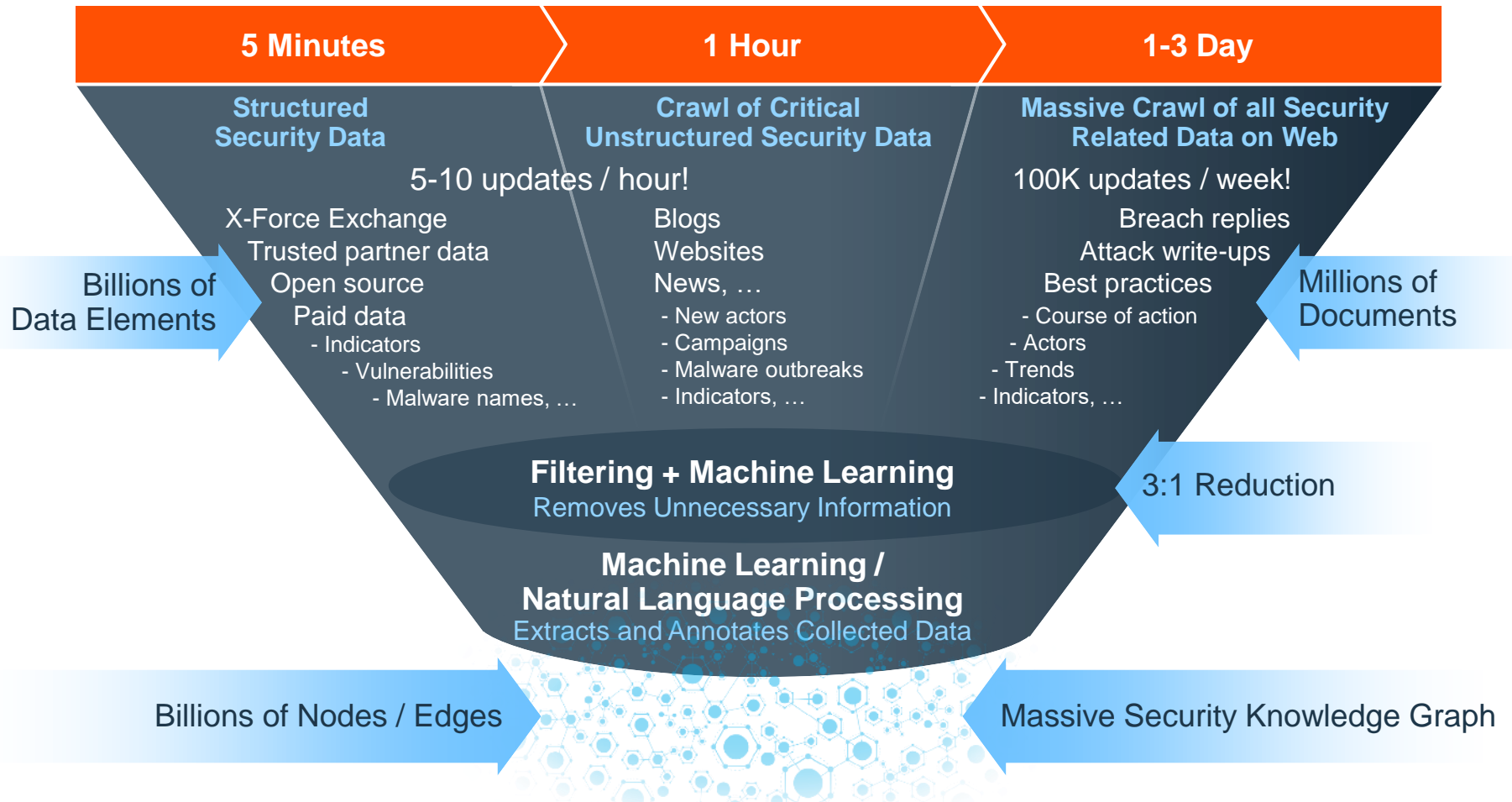
- Data correlation
- Pattern identification
- Anomaly detection
- Prioritization
- Data visualization
- Workflow



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

Relationships for **Username tom_wilson**

Default | Investigated

Highlight

Relationships

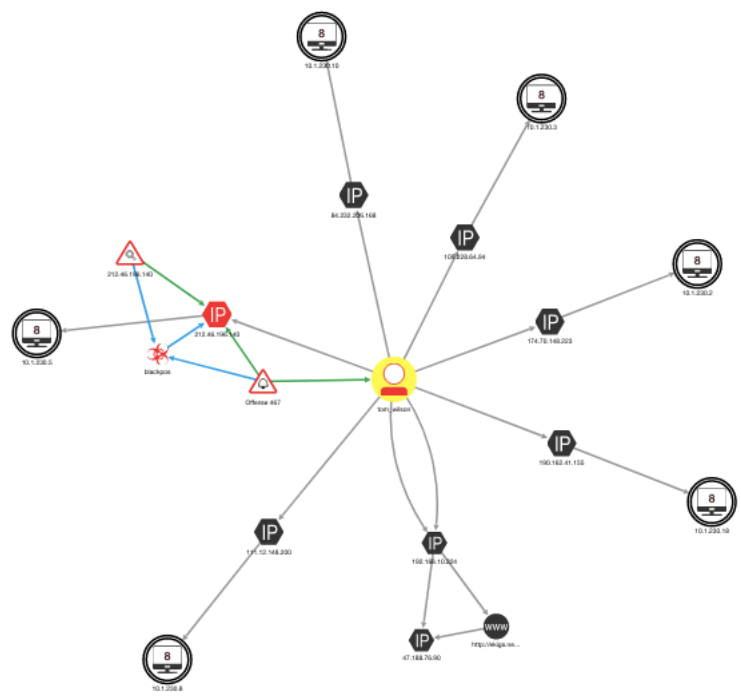
- Local (17)
- Watson Enriched (3)
- New Local Context (3)
- Local Blocked (0)
- Watson Enriched Blocked (0)

Scenarios

- Malware Executed (0)

Concern

- Critical (2)
- High (1)
- Medium (0)
- Low (16)



Using analyst feedback to drive better decisions

Learning

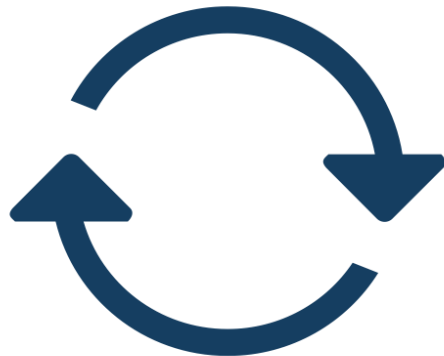
Tier 2 Analysts

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

1

Visualize how the attack has occurred and is progressing

2

3

Uncover what tactics can still possibly occur

Watson Investigations / ID: Offense 126

Key findings for
Source IP 192.168.0.119
Default | Investigated

Reinvestigate | Graph Relationships
Last investigation 4 days ago, on October 4, 2018, 8:50 PM

Concern Medium

Key Insights

Threat Actors	Malware Families	High Value Assets	Risky Users	Watched Users	Related Investigations	Duplicate Investigations
0	5	2	0	1	0	0

Key Observables

Total	Suspicious	Critical	New Local Context
65	44	35	4

MITRE ATT&CK Tactics

Credential Access
31 observables

Insights

From this offense, Watson has analyzed 24 observables. The analysis found 73 new indicators that were not included in the offense. A total of 35 data points were found to be linked with the offense. 31 indicators were related to suspicious activity, and six indicators were active. From the newly found indicators, 25 have ties to suspicious activity. In particular, four files, 24 URLs, one domain name and two IP addresses have been found, which are known to be suspicious or malicious. The following malware family types might be linked to the offense: "icepack", "locky", "dridex", "spam zero-day", "emotet". The evidence is provided by "three anti-virus signatures". One user on a watch list is associated with the offense: kyle.langford. Advisor has identified one high value asset associated with the offense: 192.168.0.119.




Analysis of the indicators found by Watson revealed four additional observables related to the offense in the local context. Advisor has identified one additional high value asset related to the offense in the expanded local context: 192.168.0.122.

Offense Summary | View details



THANK YOU

FOLLOW US ON:

-  ibm.com/security
-  securityintelligence.com
-  xforce.ibmcloud.com
-  [@ibmsecurity](https://twitter.com/ibmsecurity)
-  youtube.com/user/ibmsecuritysolutions

© Copyright IBM Corporation 2016. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

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.