Eurocase 2017

How to Increase your SOC efficiency

CYBER

Staffing

Attacks

Staffing

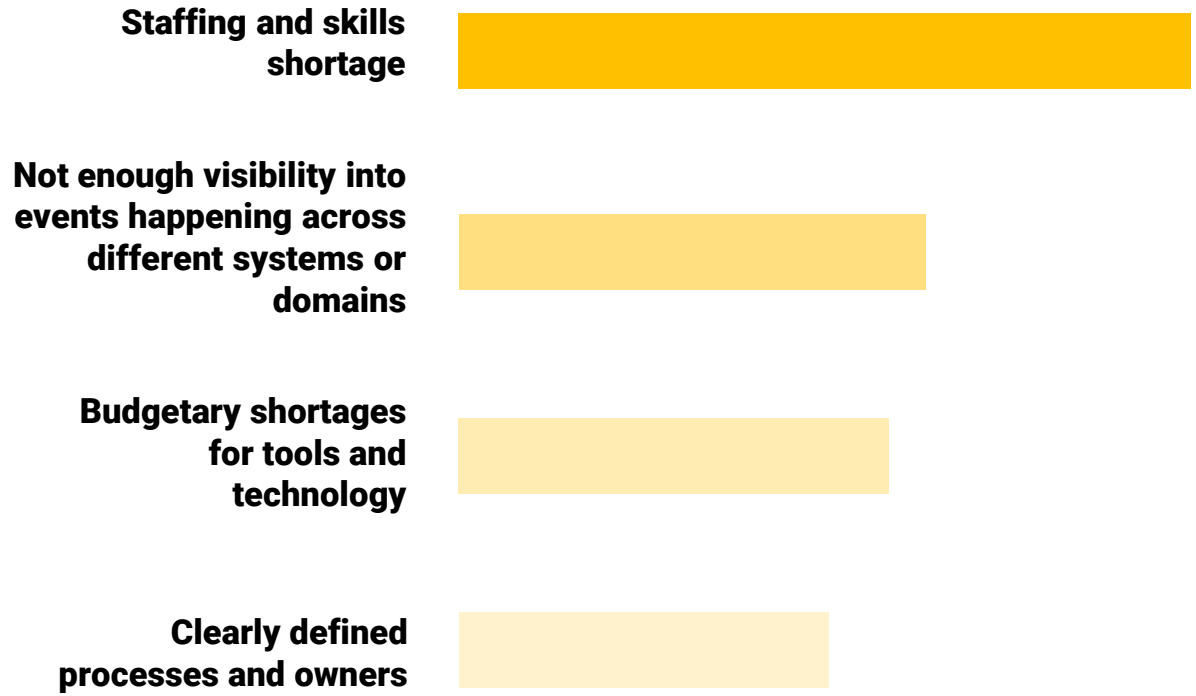
Complexity

Attacks

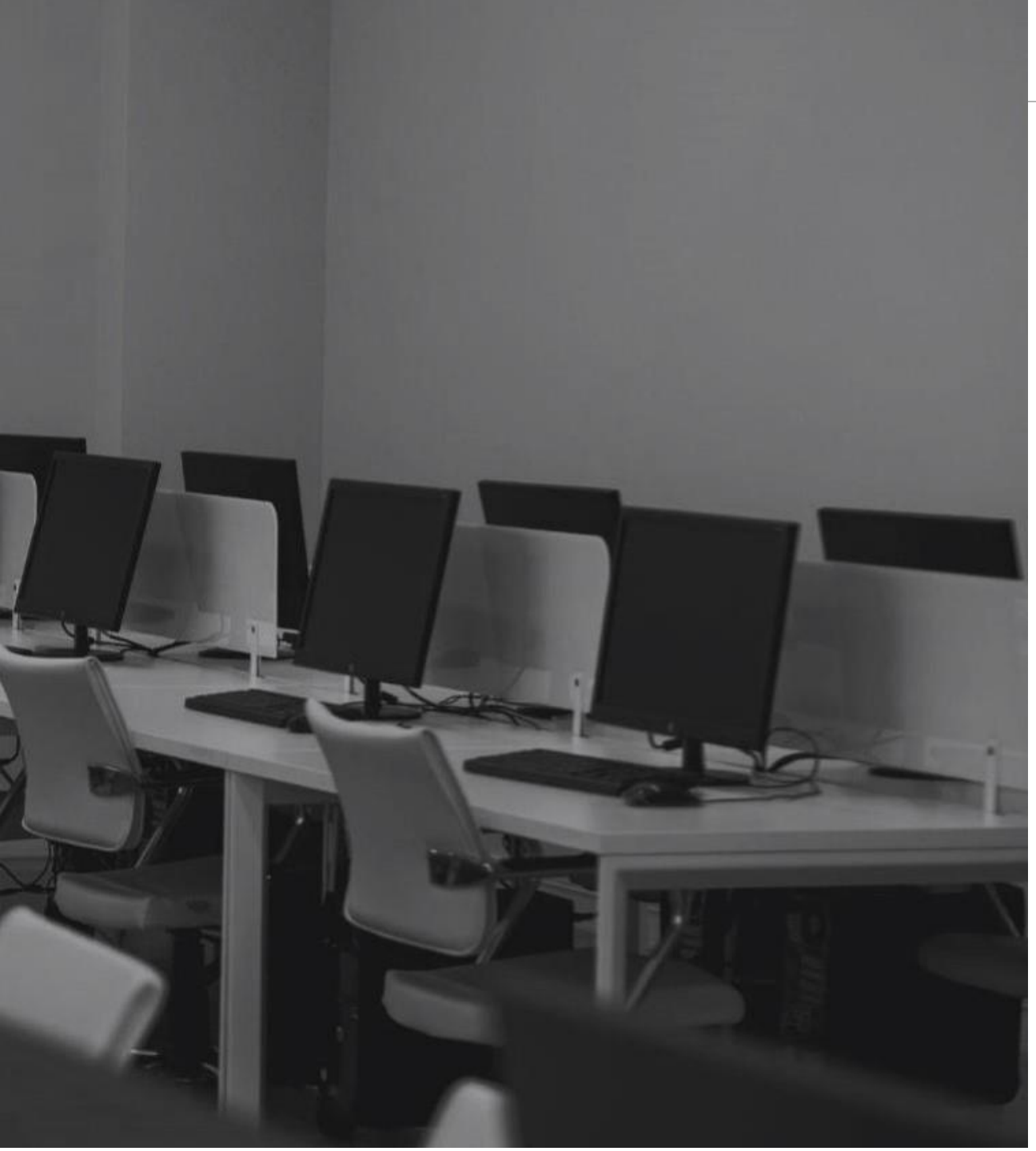
Staffing

THE #1 OBSTACLE TO EFFECTIVE INCIDENT RESPONSE IS SKILL SHORTAGE

What do you believe are the key impediments to effective IR at your organization?



Hacking the skills shortage, CSIS and Intel Security, July 2017



But Staffing Shortage Will Not Be Solved in the Near Future

1 million cybersecurity job openings today

6 million openings projected for 2019

Hacking the skills shortage, CSIS and Intel Security, July 2017

RATHER THAN FOCUSING ON HIRES, SUCCESSFUL SECURITY LEADERS STRIVE TO DO MORE WITH LESS

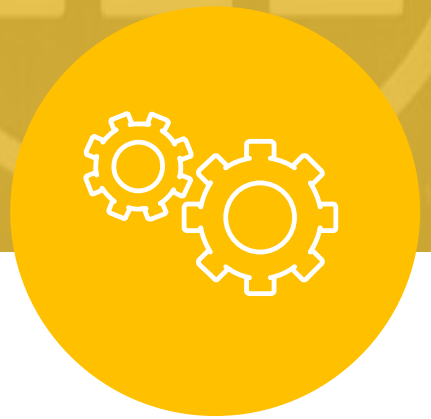
Increase SOC team impact

Reduce skill level requirements

Improve SOC efficiency and maturity

THE TRADITIONAL SOC IS GIVING WAY TO AUTOMATION AND ORCHESTRATION

SIEM
2013



Automation
2015

Orchestration
2017

SOC 3D: Your Gateway to the Future of SEC-OPS

What Is SOC-3D

The only SOC management platform combining **automation, orchestration** and **big-data security analytics** for real-time investigation

Your **Single Pane of Glass** for managing your entire security operations

Provides **more accurate and actionable high priority alerts**

Your SOC Hub

ALERTS

- SIEM
- Ticketing
- Email
- CRM
- Helpdesk
- UBA
- EDR

API's

SOC 3D

API's

Big-Data

Enrichment

- Threat Intel
- CMDB
- HR Systems
- GRC
- Compliance
- Vulnerability Assessment

RESPONSE TOOLS

- IPS
- EDR
- WAF
- Active Directory
- NAC
- Memory Dump

WITH SOC-3D, YOUR SOC IS

Efficient

Faster to respond
Reduces SOC team workload
Measurable

Business-Driven

Focuses on what matters the most
Keeps executive level informed
Engages the entire organization

SOC User-Centric

Reduces the expertise barrier
Engages your team
Increases analyst impact
Simplifies complex investigations

Increase Efficiency

THE TRADITIONAL SOC: MULTIPLE TOOLS AND FEEDS

Threat Intelligence

SIEM

Endpoint Detection

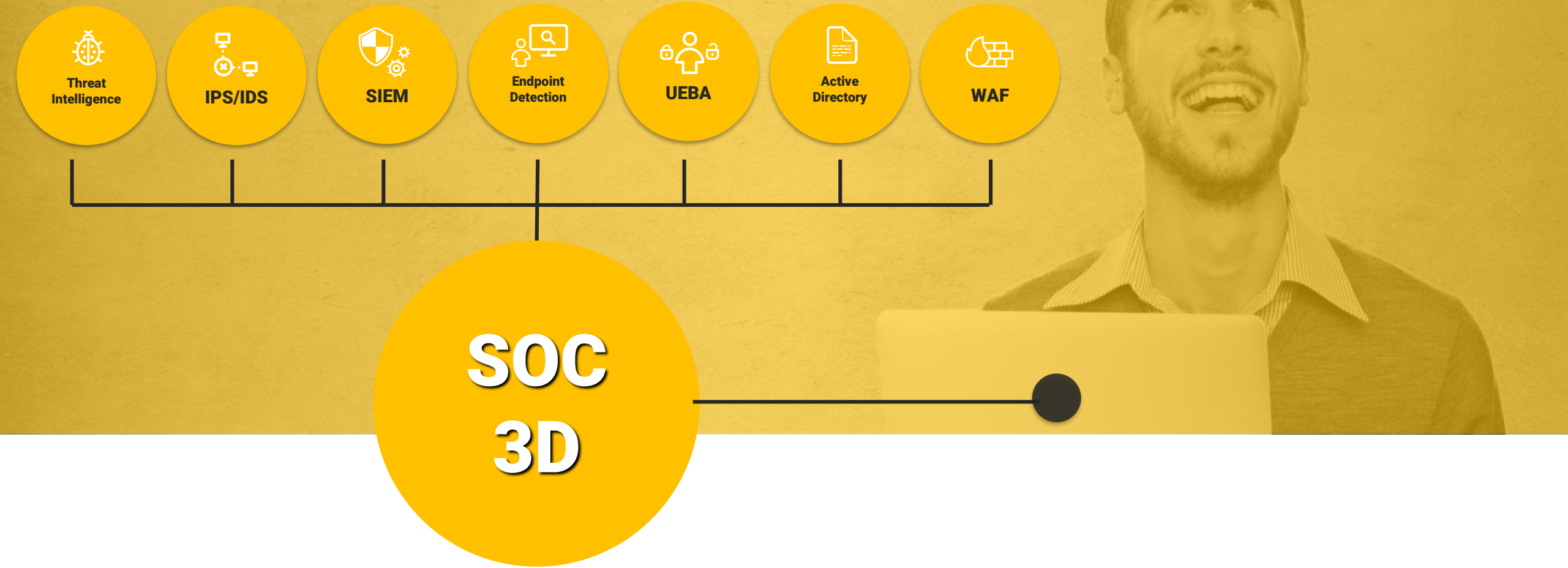
Active Directory

WAF

UEBA

IPS/IDS

With SOC-3D: A Single Pane of Glass

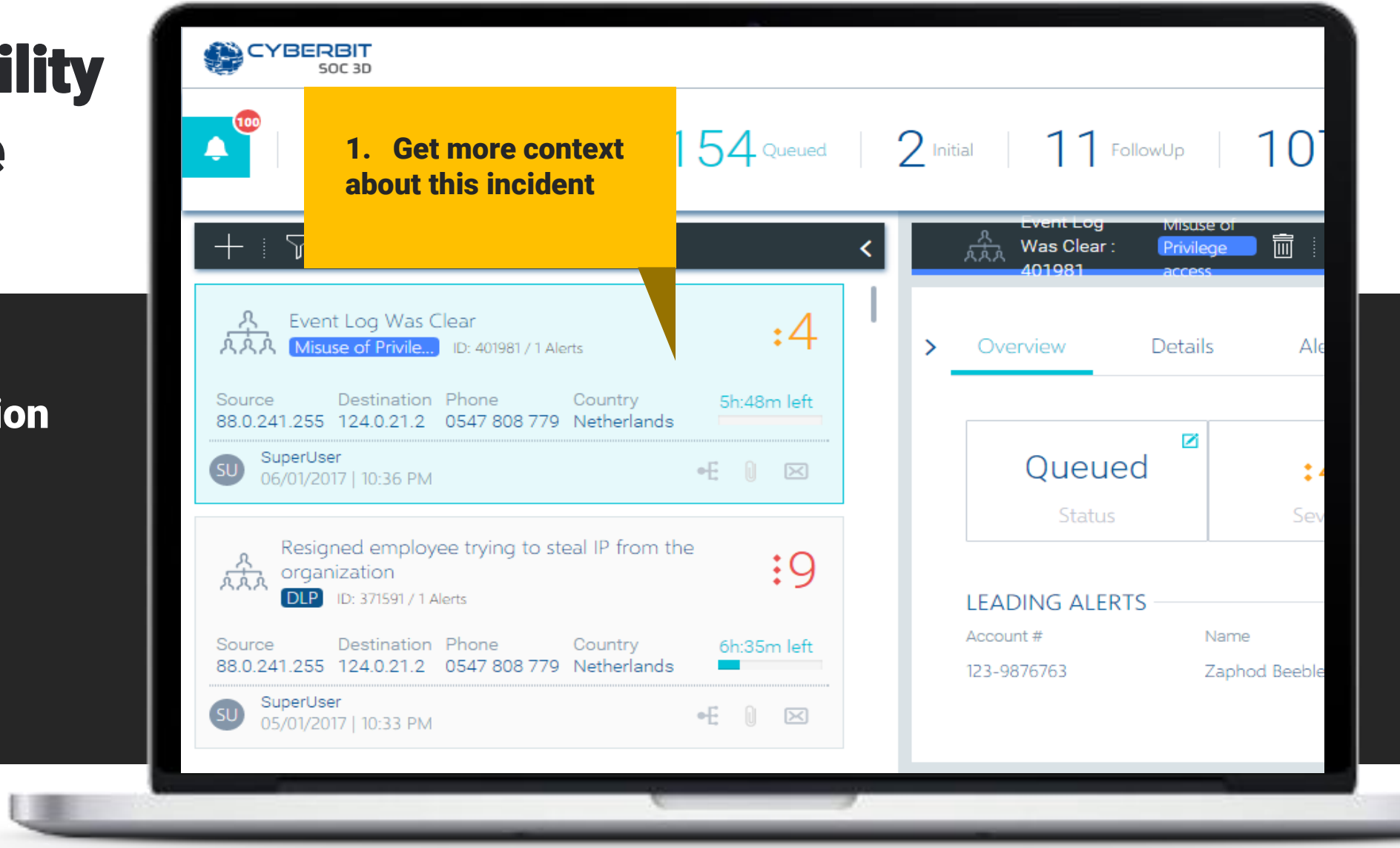


Manage Multiple Response Tools via SOC 3D

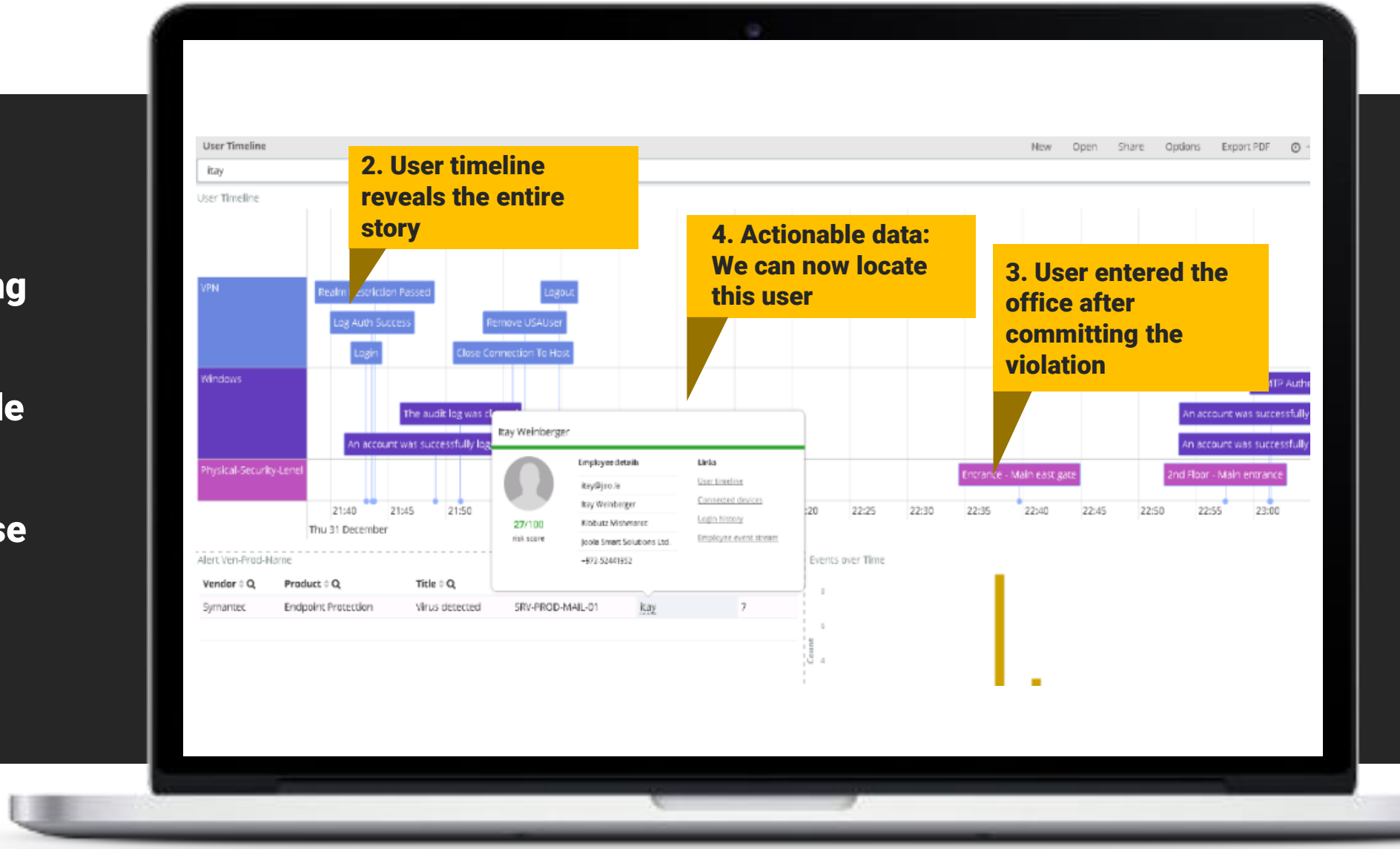
- **Reduce the expertise barrier**
- **Empower tier-one SOC operators**
- **Reduce time-to-response**

Real-time Visibility Across Multiple Domains

Use Case:
Privilege Access Violation

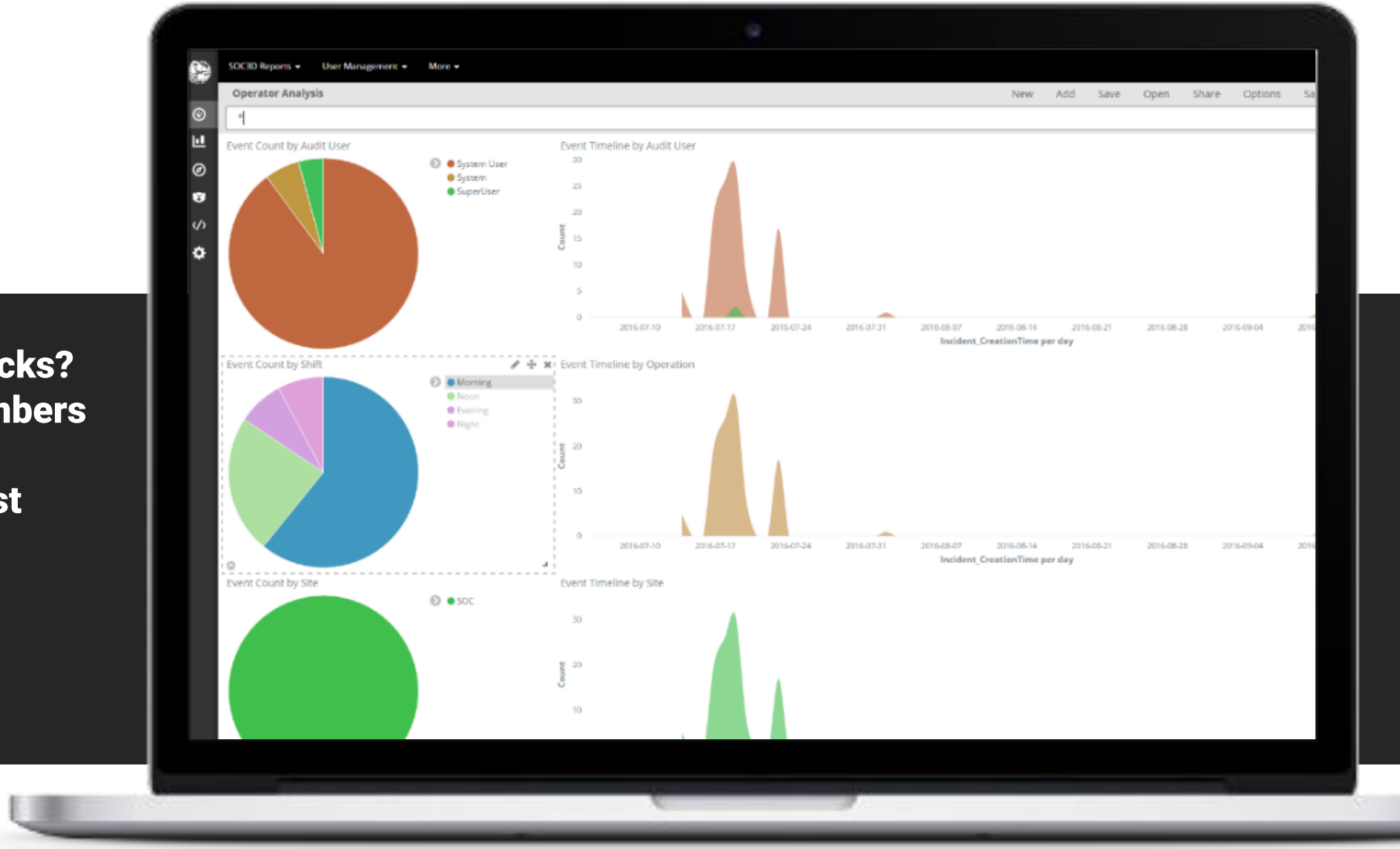


- **Empower tier-one operators with managing complex investigations**
- **Visibility across multiple domains**
- **Reduce time to response from hours to minutes**



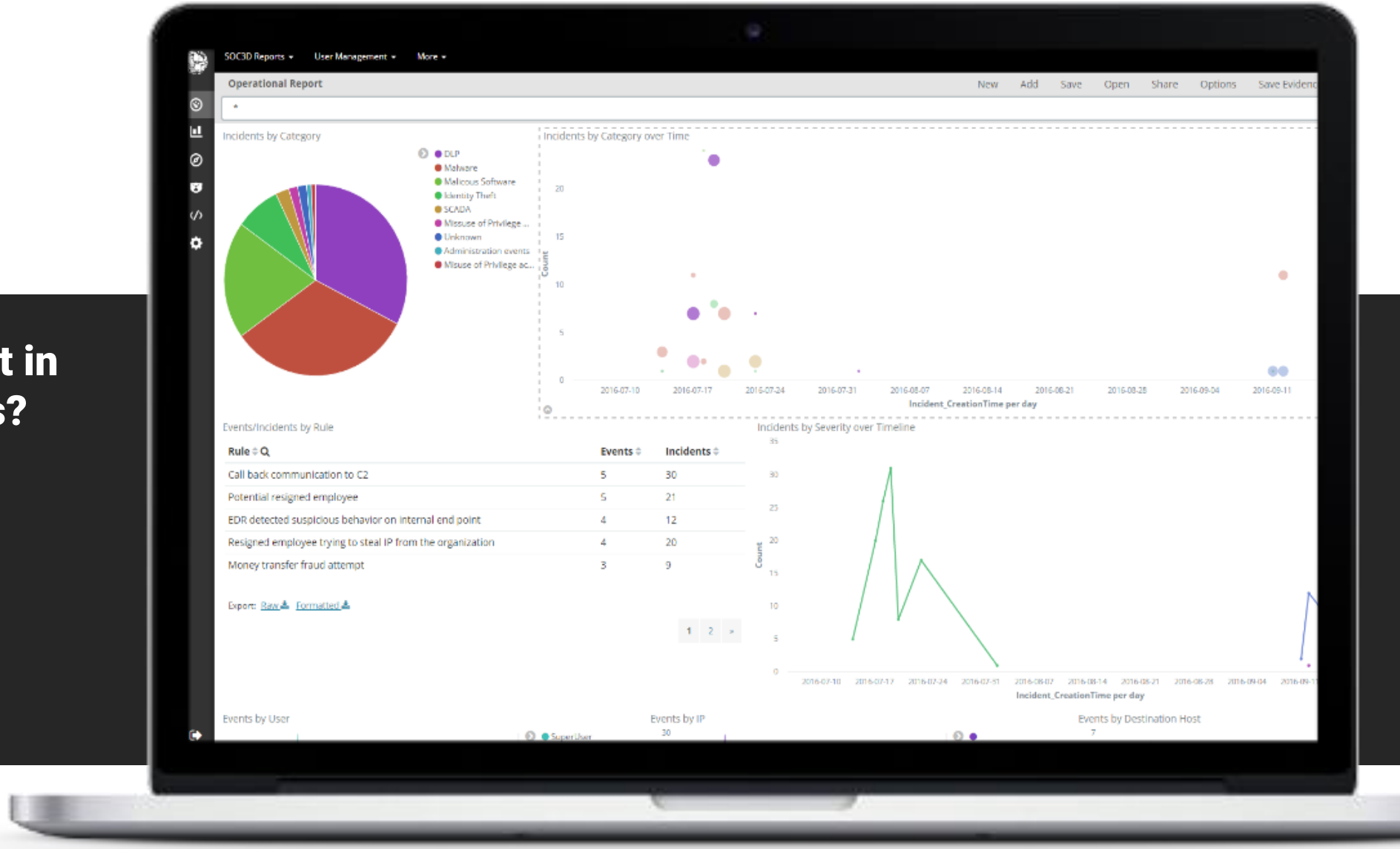
Measure And Improve SOC Performance

- Where are my bottlenecks?
- Which of my team members are slower to respond?
- What are my SOCs most effective or ineffective shifts?



Measure And Improve SOC Performance

Which alert types result in the most severe events?



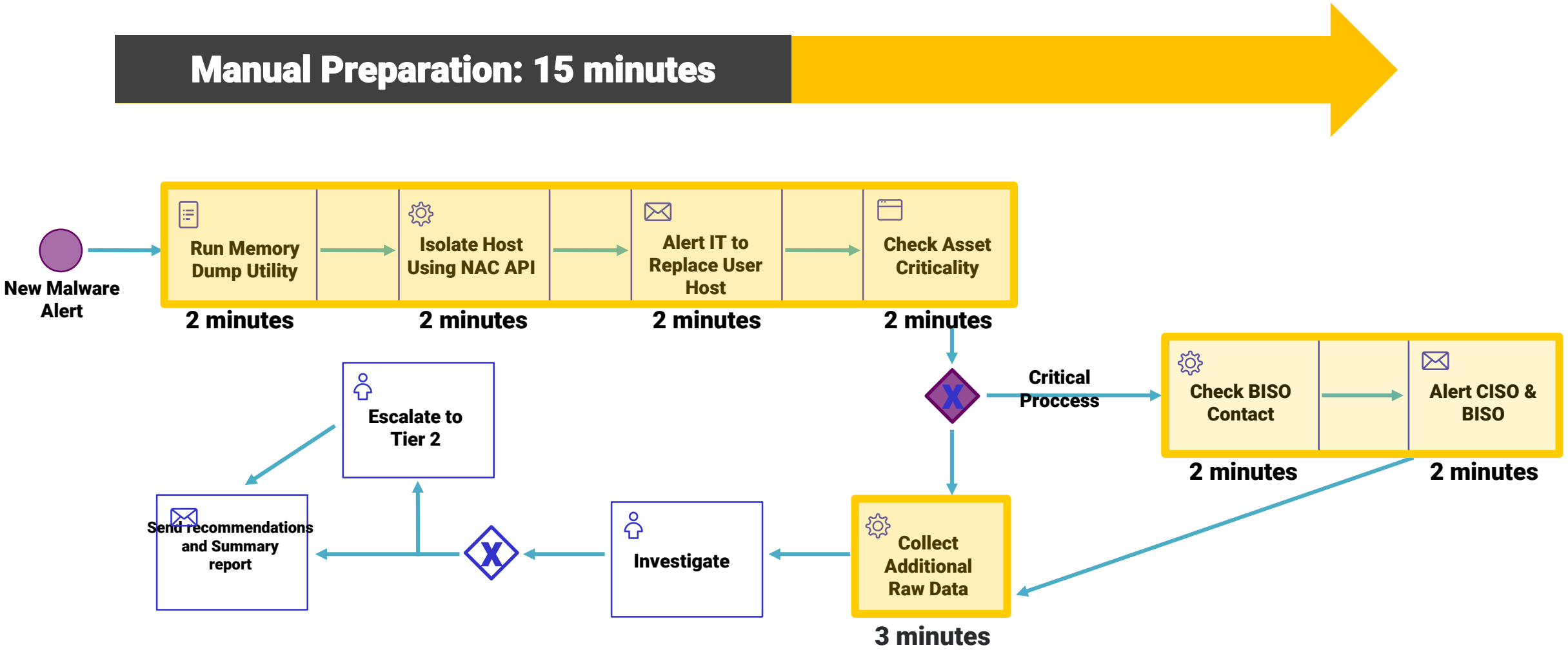
SMART AUTOMATION
ACCELERATE ANALYST
WORK ACROSS THE ENTIRE IR CYCLE

Automate
Decision Making
By automating data collon
prior to response

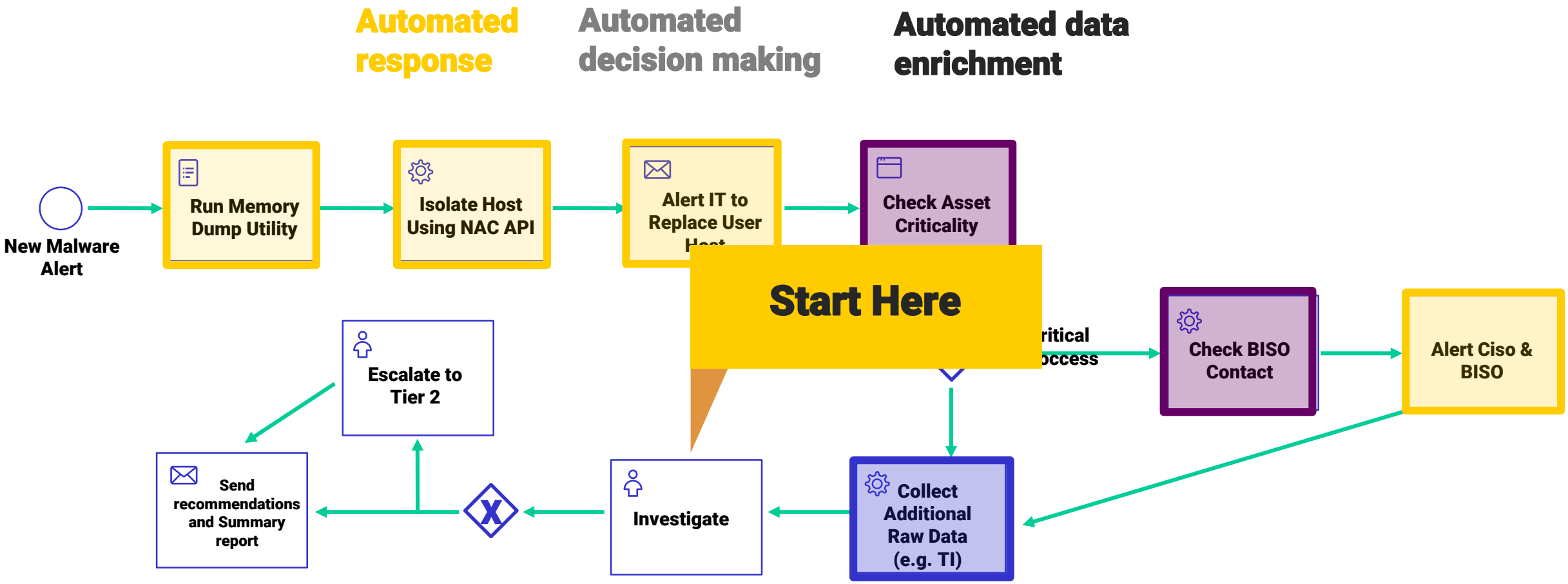
Automate
Data Enrichment
Get all relevant data for
investigation

Automate
Response
Automate SOC operator and analyst
response tasks

THE RESPONSE PROCESS: TRADITIONAL SOC



THE RESPONSE PROCESS: WITH SOC-3DD AUTOMATION



IMPACT ON TTR AND TCO

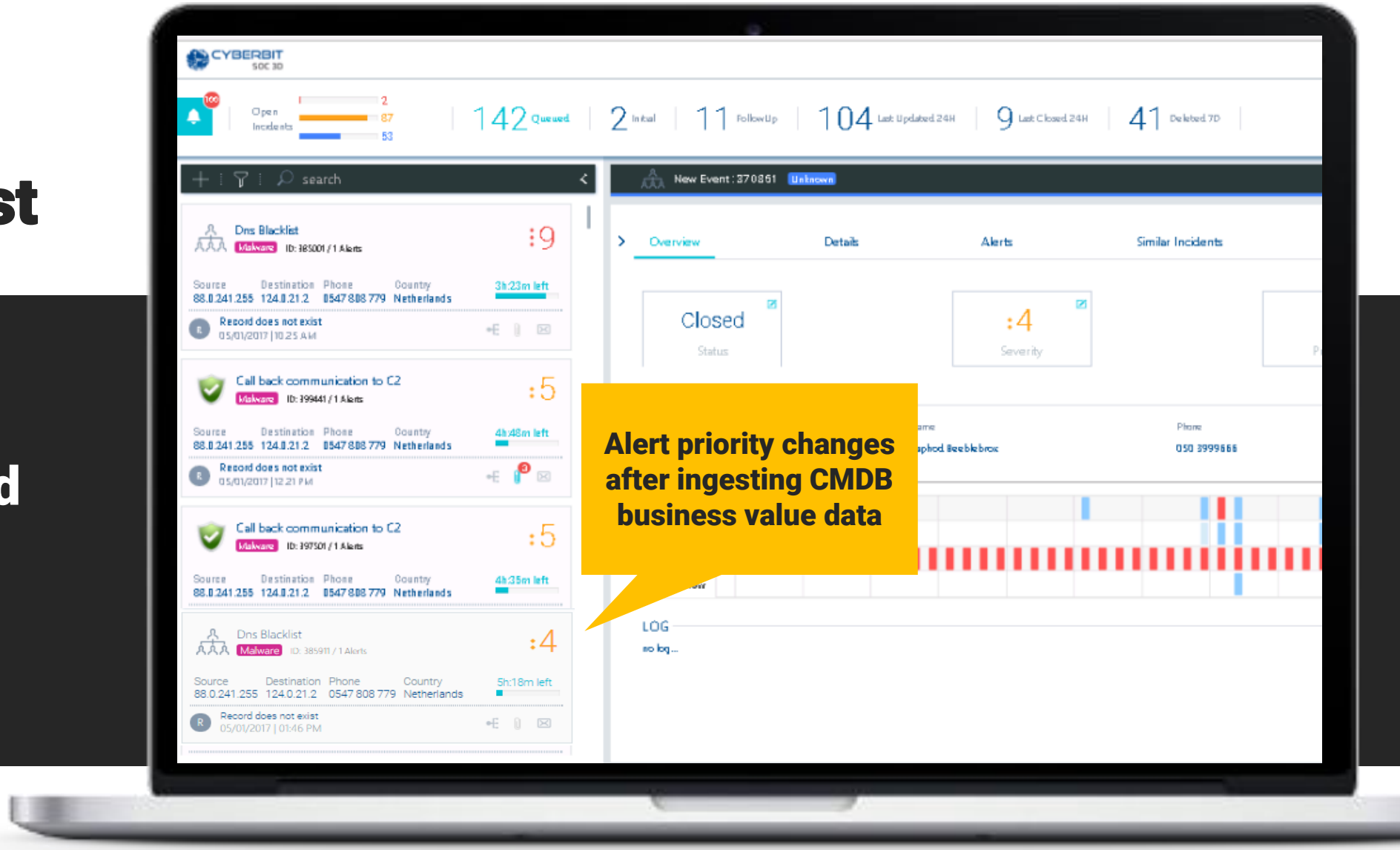
Average number of stages per incident	6
Average time saved by SOC 3D per stage	2 minutes
Total time saved by SOC 3D per incident	12 minutes
Number of daily incidents	100
Time saved by SOC 3D every day	20 hours
TCO saving per day	$2000
TCO saving per month	$44,000

Create a Business-driven SOC

Manage the right threat at the right time

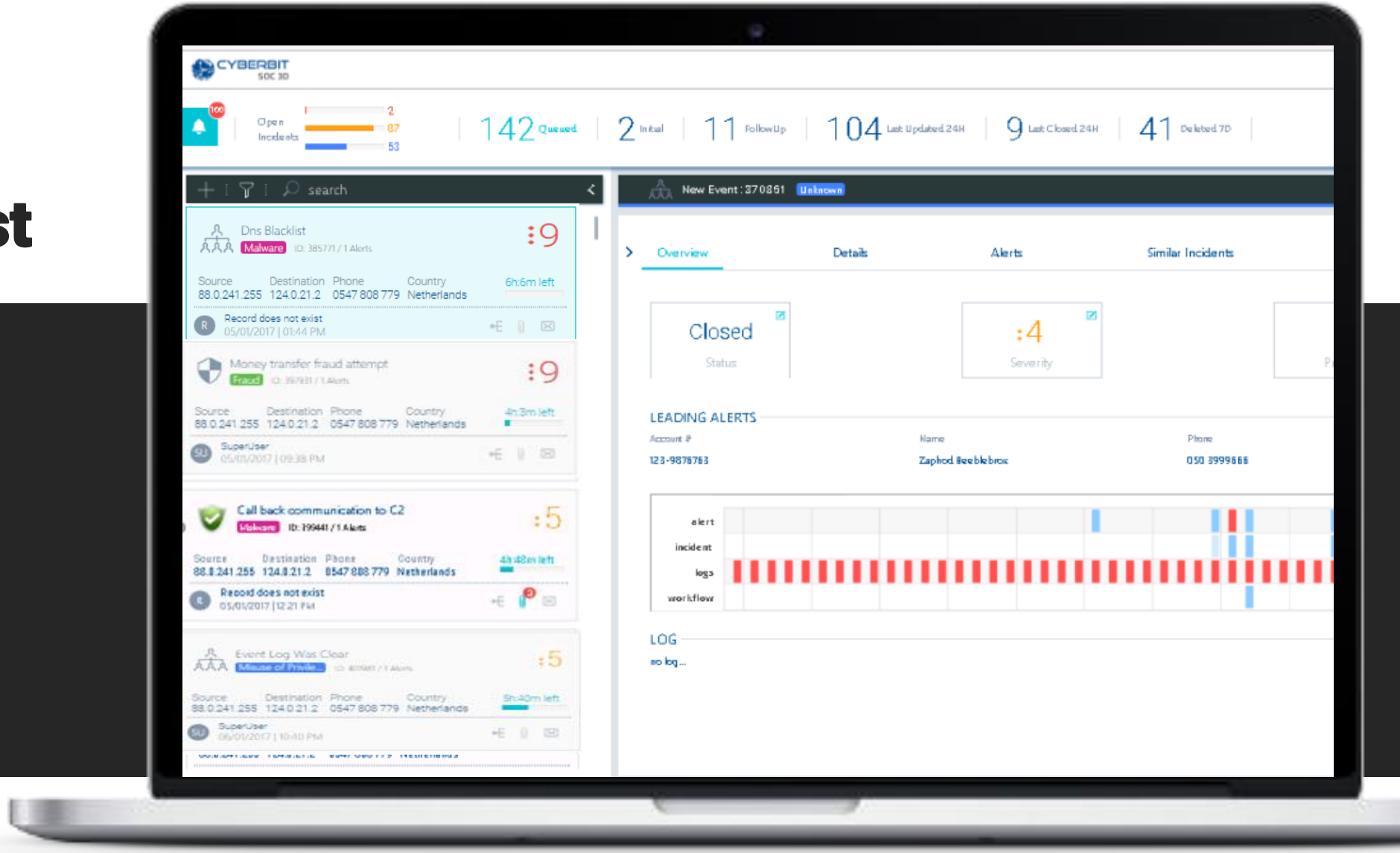
Focus on What Matters the Most

Smarter threat management based on business risk



Focus on What Matters the Most

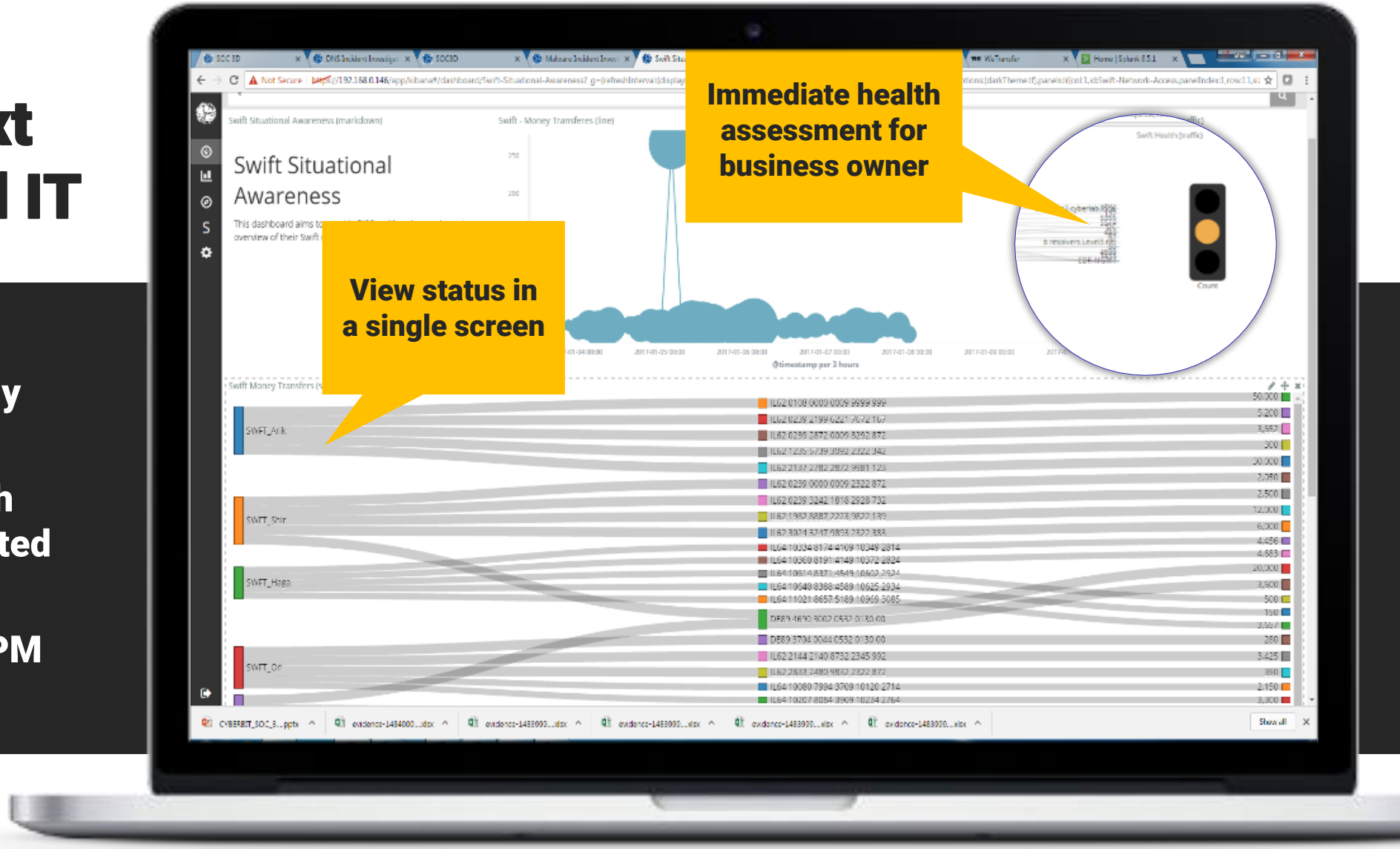
High priority alerts are addressed first



Investigate by Business Context Beyond SOC and IT

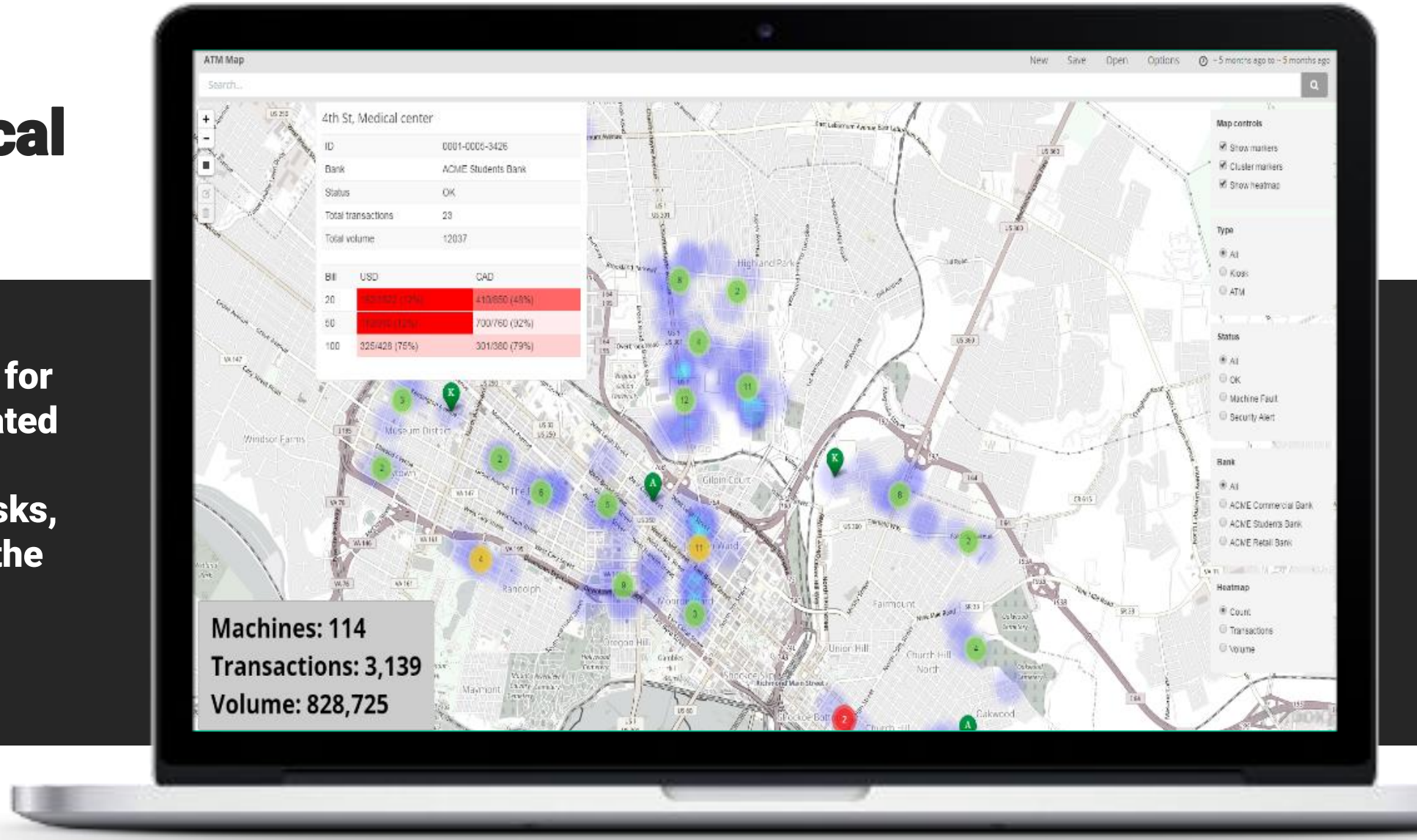
Use Case:

- I suspect an attack on my SWIFT process
- I need to know the health status for all SWIFT related entities
- Leverages CMDB and BPM info



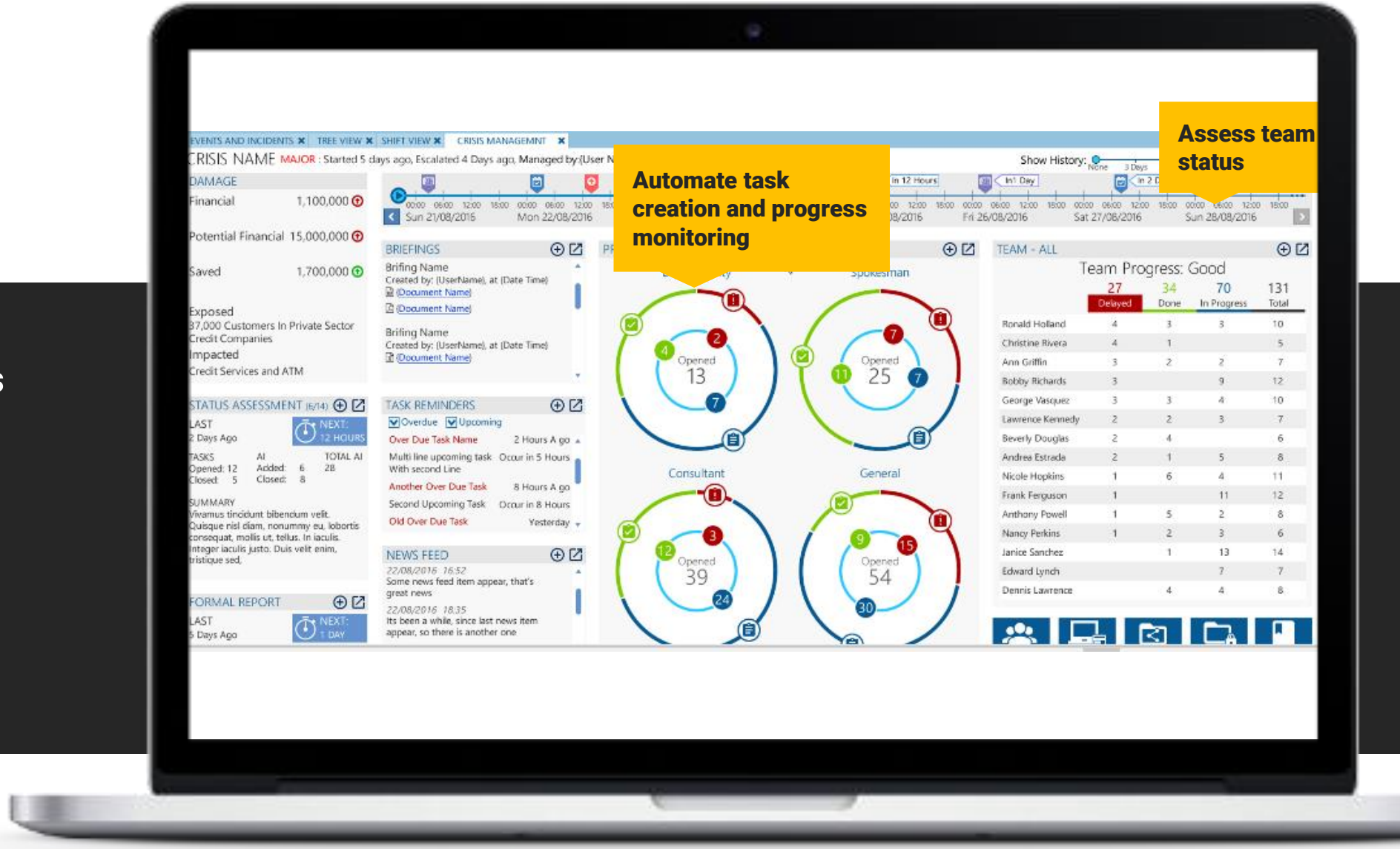
Monitor Your Business-critical Areas 24/7

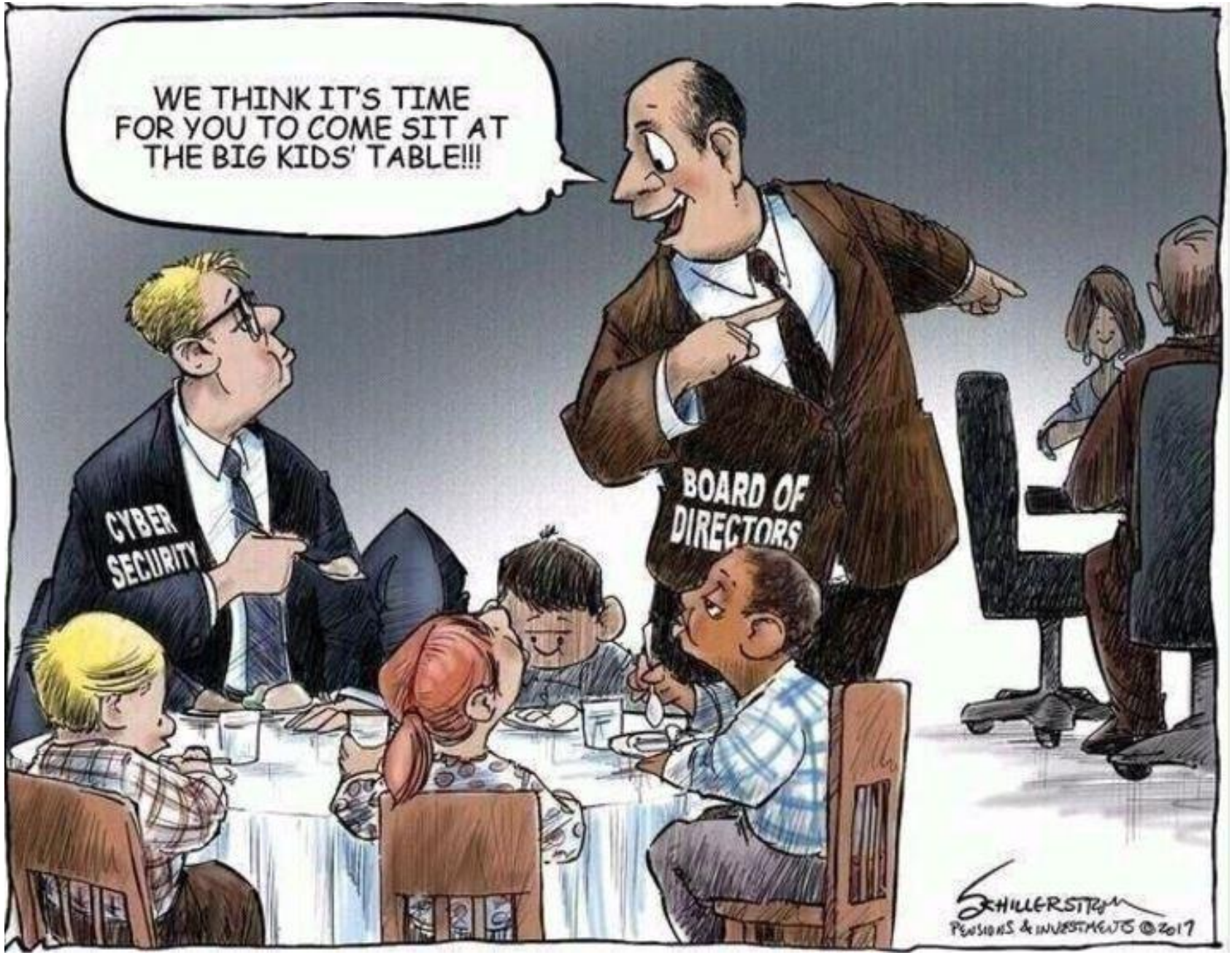
- **Situational awareness for areas that need dedicated attention**
- **Monitor operational risks, demonstrate value to the organization**



Crisis Management

- **Manage crisis workflows and tasks beyond the SOC team**





Security Analytics

Big-data driven for faster insights and visibility

SECURITY ANALYTICS
VISUALIZE ANYTHING. INVESTIGATE FREELY

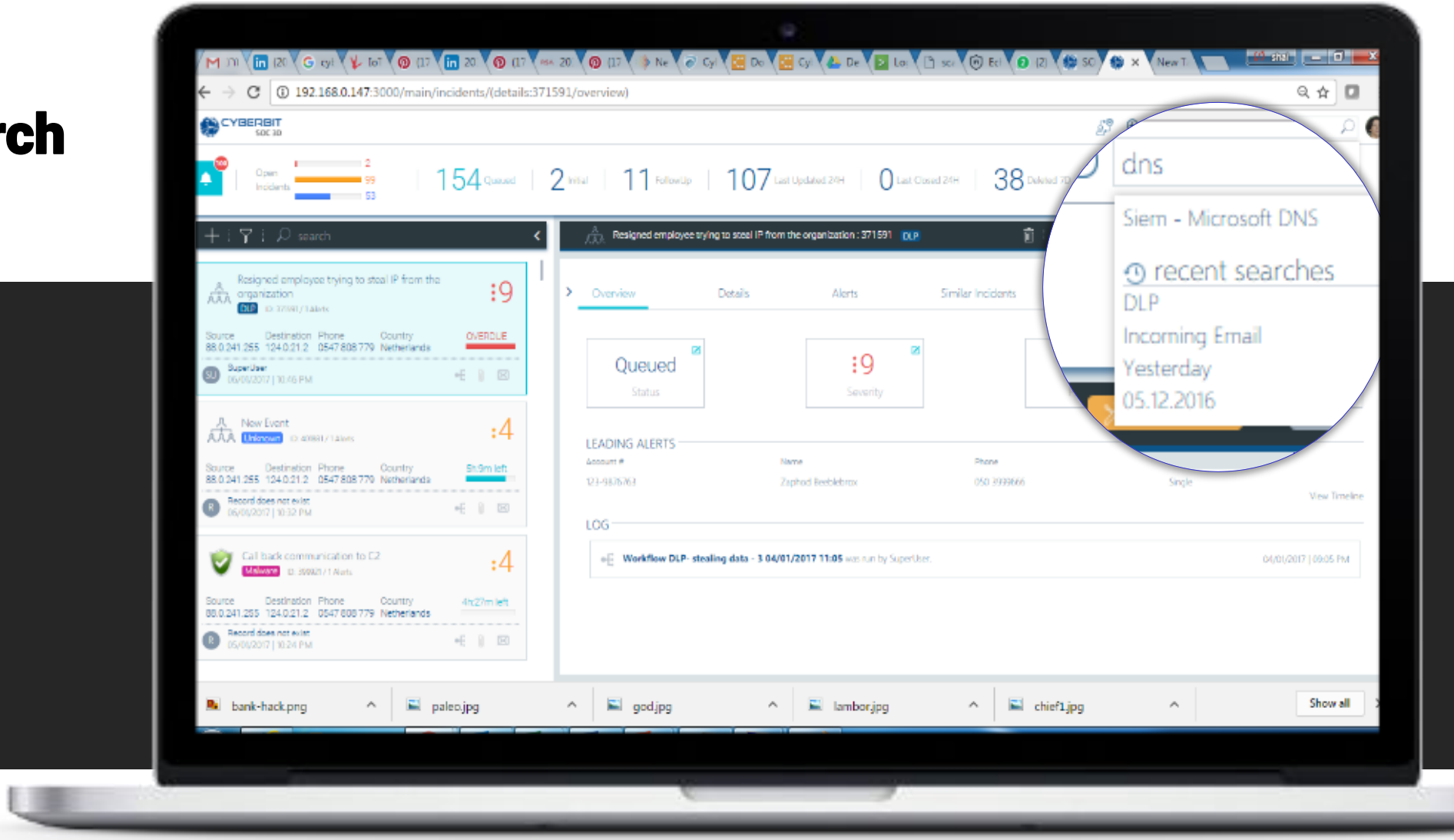
Explore raw data for forensics

Real-time access via big-data platform

Real-time visualization for faster insights

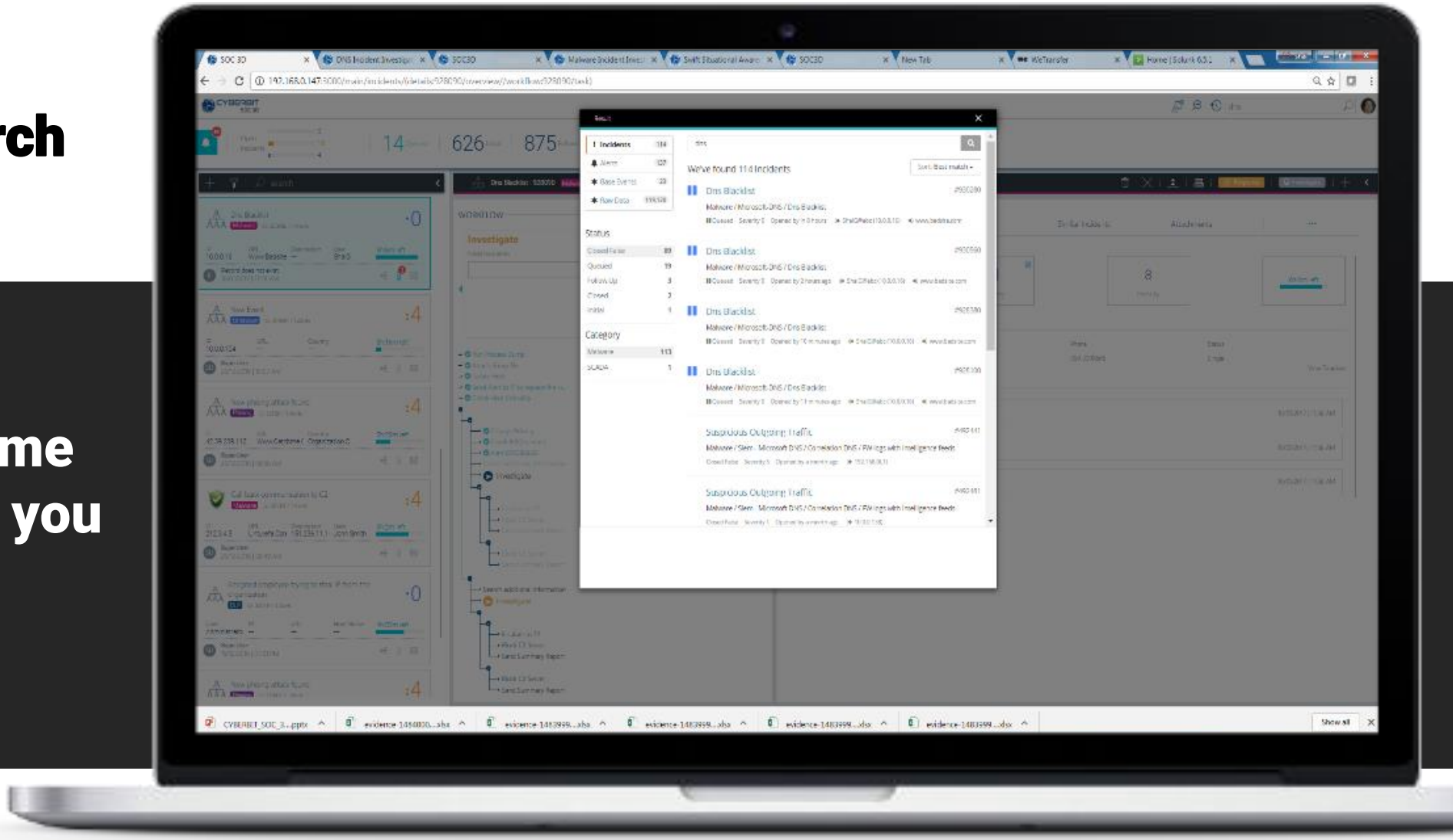
Natural Language “Google Like” Search for Incident Data

Continue an investigation, or proactively search for data



Natural Language “Google Like” Search for Incident Data

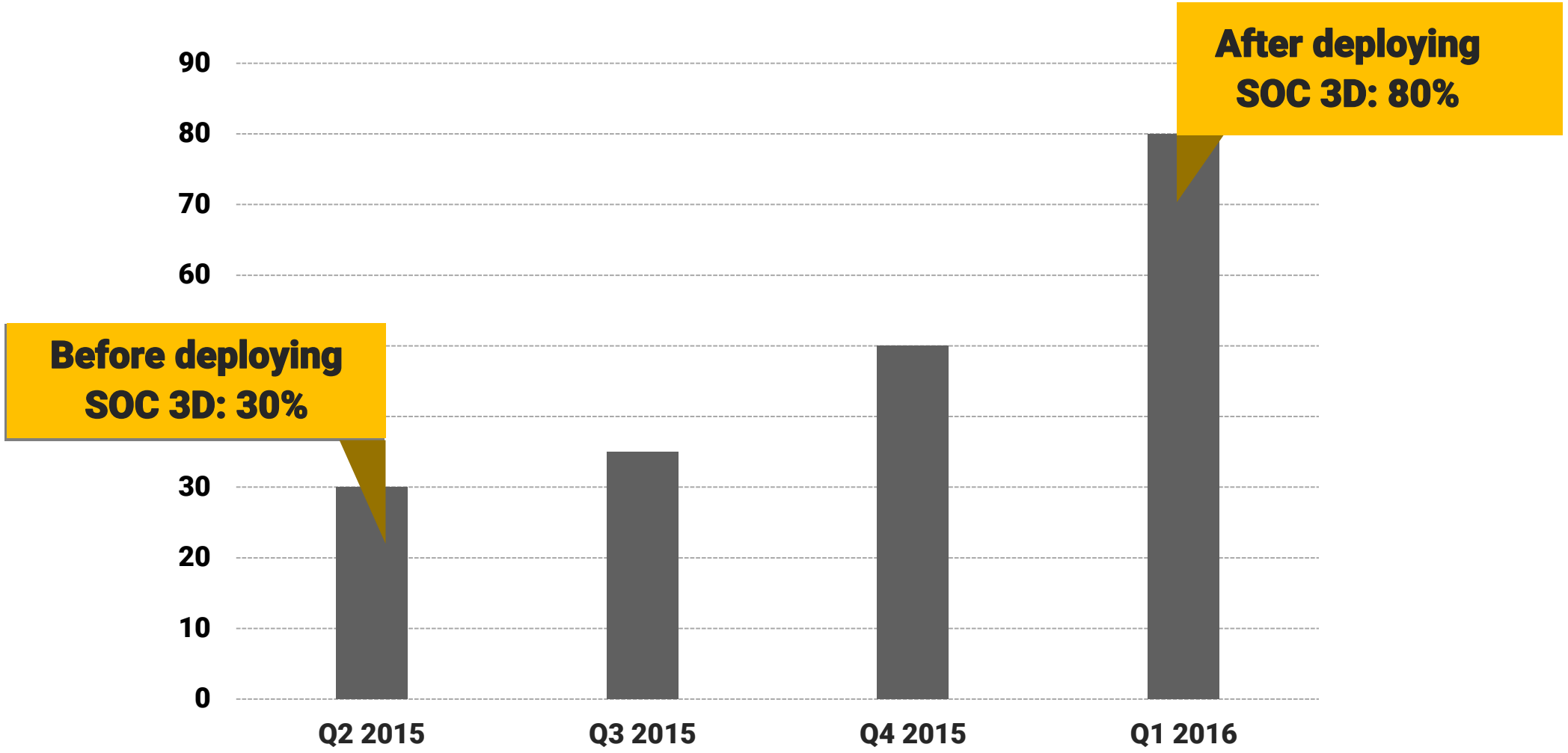
Search results: granular an real-time access to the data you needed



Case Study

- **Large Enterprise**
- **20,000 SIEM alerts/month**
- **50 long-duration events/month (longer than a week)**
- **150 unknown malware/month**

PERCENTAGE OF INCIDENTS CLOSED WITHIN 6 HOURS



Complements Any SIEM

IBM

ArcSight

IBM Radar

splunk>

ALIEN VAULT

LogRhythm

Rich 3rd Party Integration

- Accepts all major product types and vendors: IPS, IDS, WAF, Firewall, TI endpoint,
- Generic API – scripts, REST, and Web Services

Deployment Models

Single SOC

Fusion SOC/distributed SOCs

MSSP

Thank you

Paul Franka

VT Cyber sp. z o.o.
8, Zygmunta Vogla Str.
02-963 Warsaw, Poland

info@vtcyber.pl
www.vtcyber.pl

CYBER