



Security in knowledge

From Hours to Seconds

Making Security Management Real Time

Gretchen Hellman

McAfee

The Information Arms Race

OLD ATTACKS



- Amateurs
- Noisy
- Curious/mischievous
- Script driven
- Untargeted

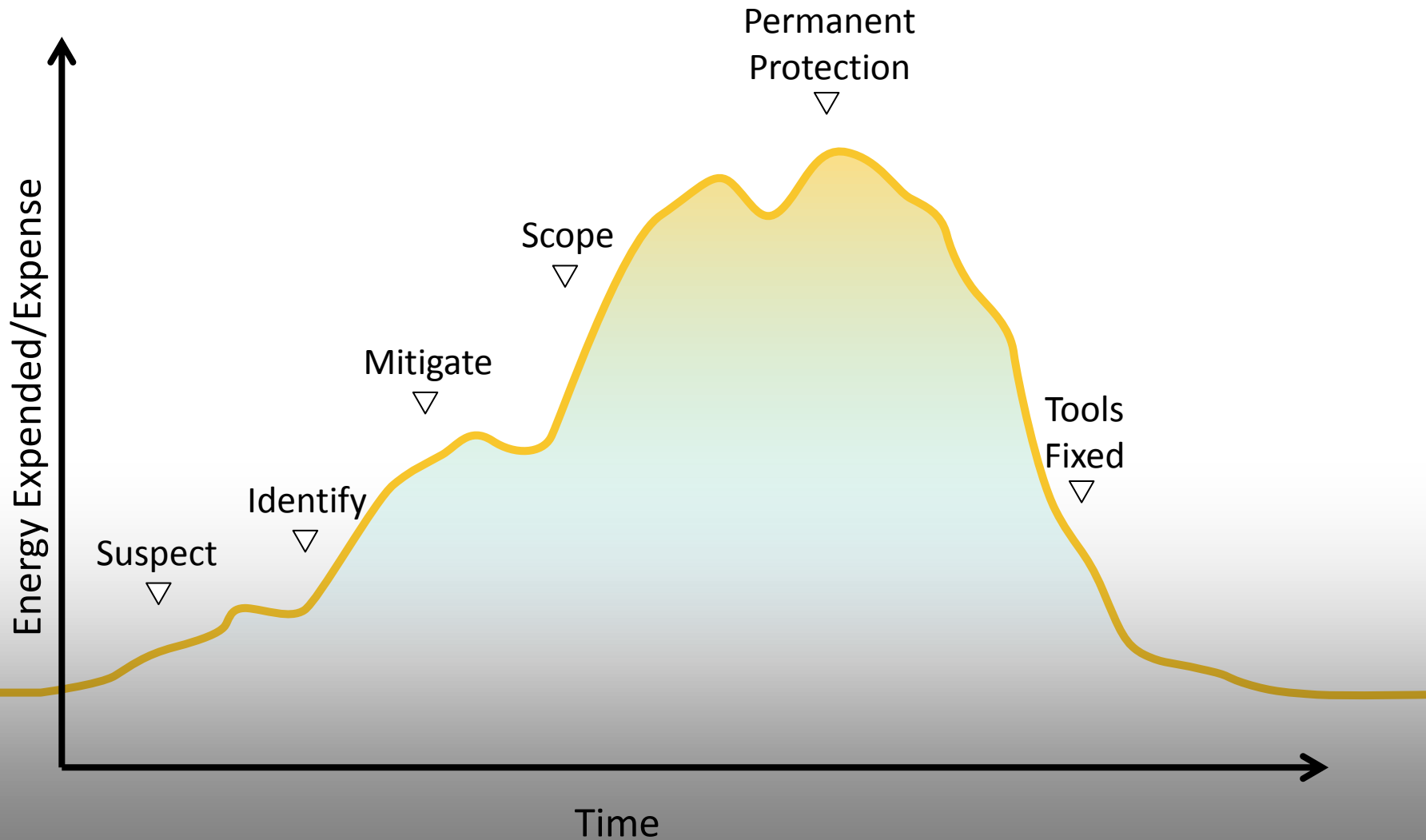


NEW ATTACKS

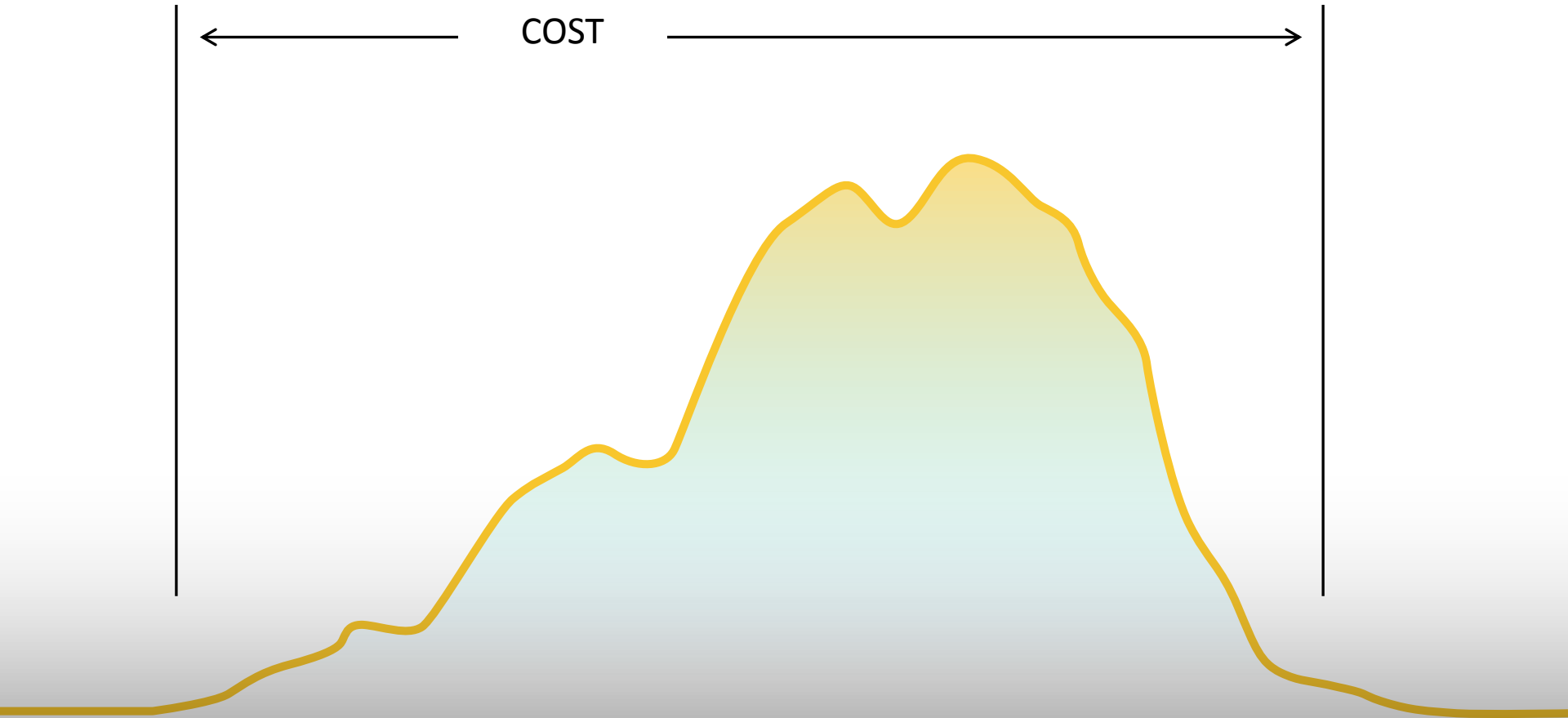


- Professionals
- Stealthy
- For profit/intentional damage
- Professionally developed
- Targeted

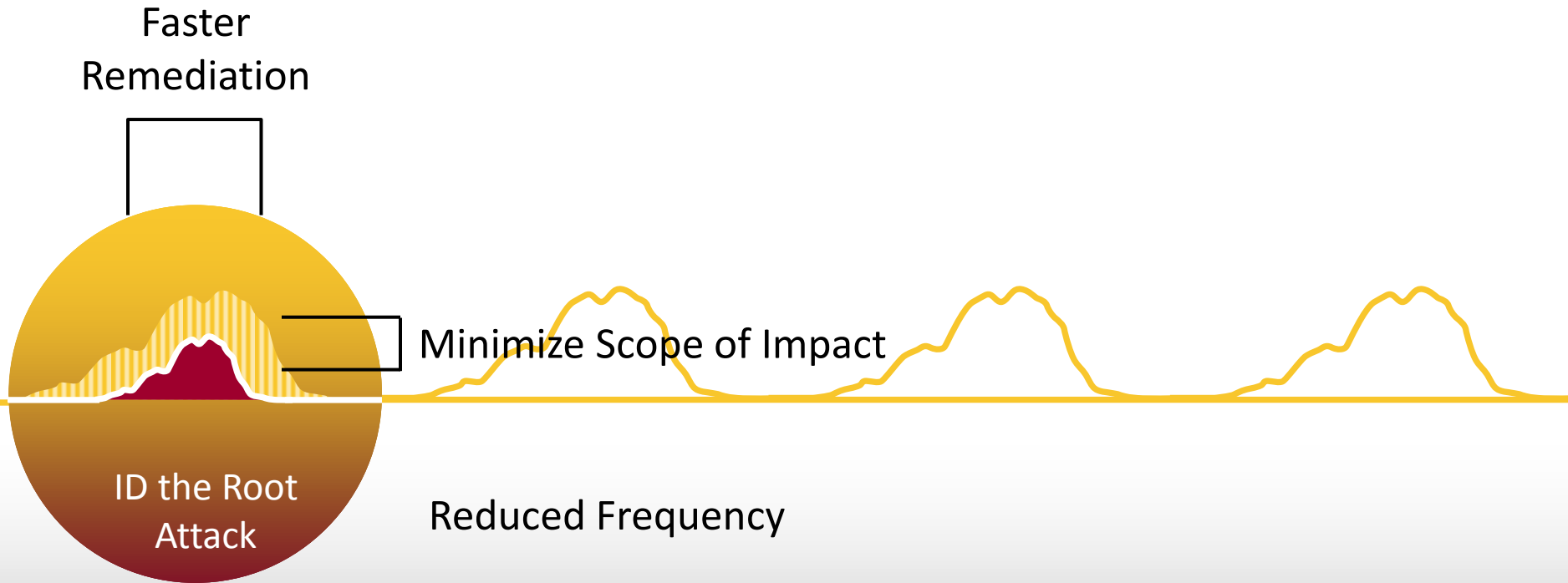
Incident Response Lifecycle



Incident Response Lifecycle

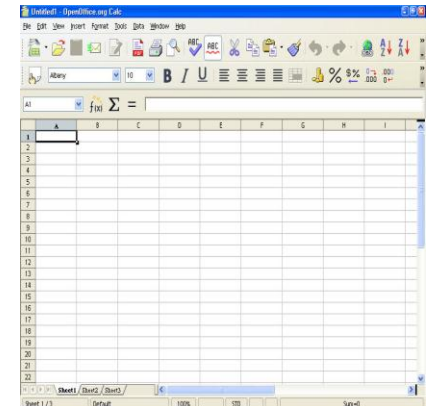


Incident Response Lifecycle



Security Management Chaos

- Console hopping
- Manual investigation
- Waiting for answers
- Waiting for updates
- Missing what's important



days	hours	minutes	seconds
02	23	54	00

Shortening the Process

- Intelligent recognition of threats
 - Rich context, risk based analysis
- Real-time active inspection of system state
 - Moving from spreadsheets and phone calls to real-time queries
- Respond with precision
 - Automate key steps and surgically addressing threat



Getting There

How?

Security Maturity Model

REACTIVE

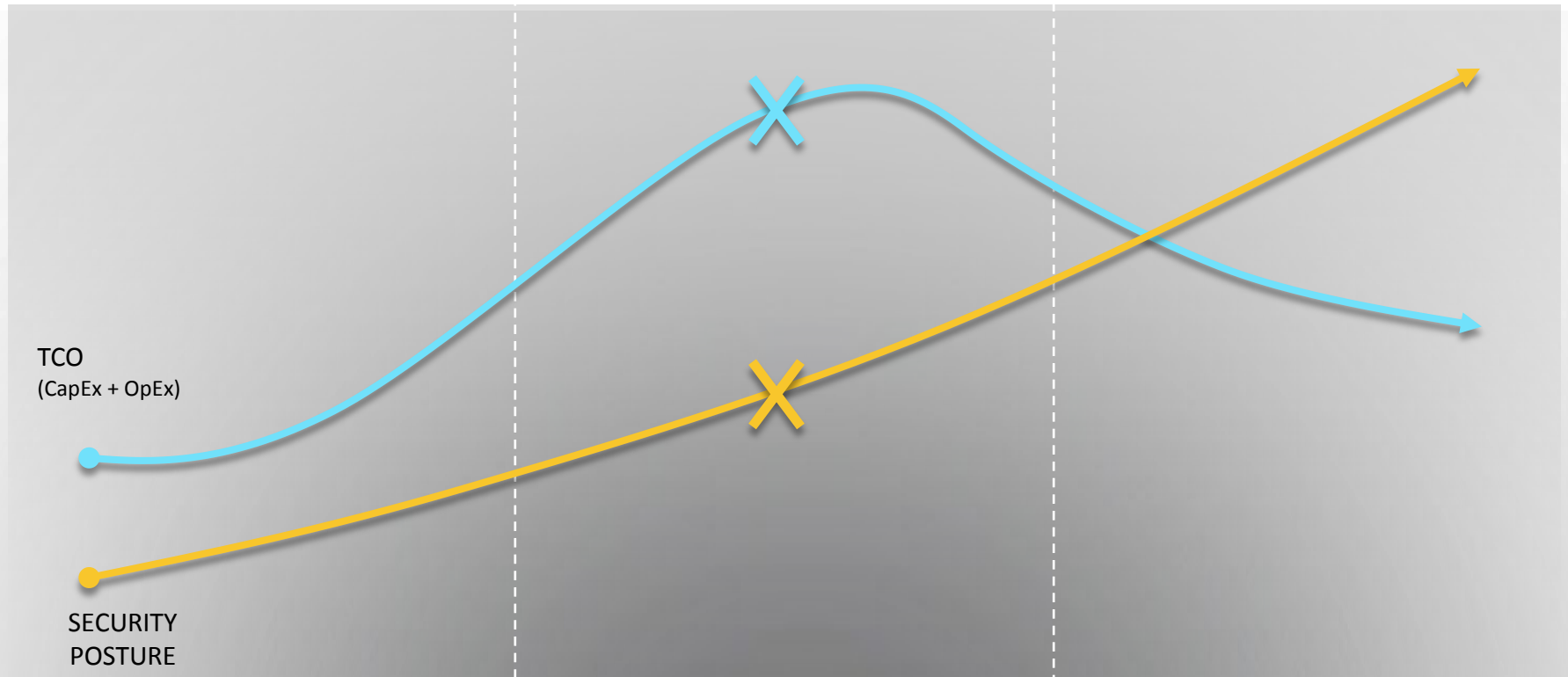
(~3% of IT Budget on Security)

COMPLIANT/PROACTIVE

(~8% of IT Budget on Security)

OPTIMIZED

(~4% of IT Budget on Security)



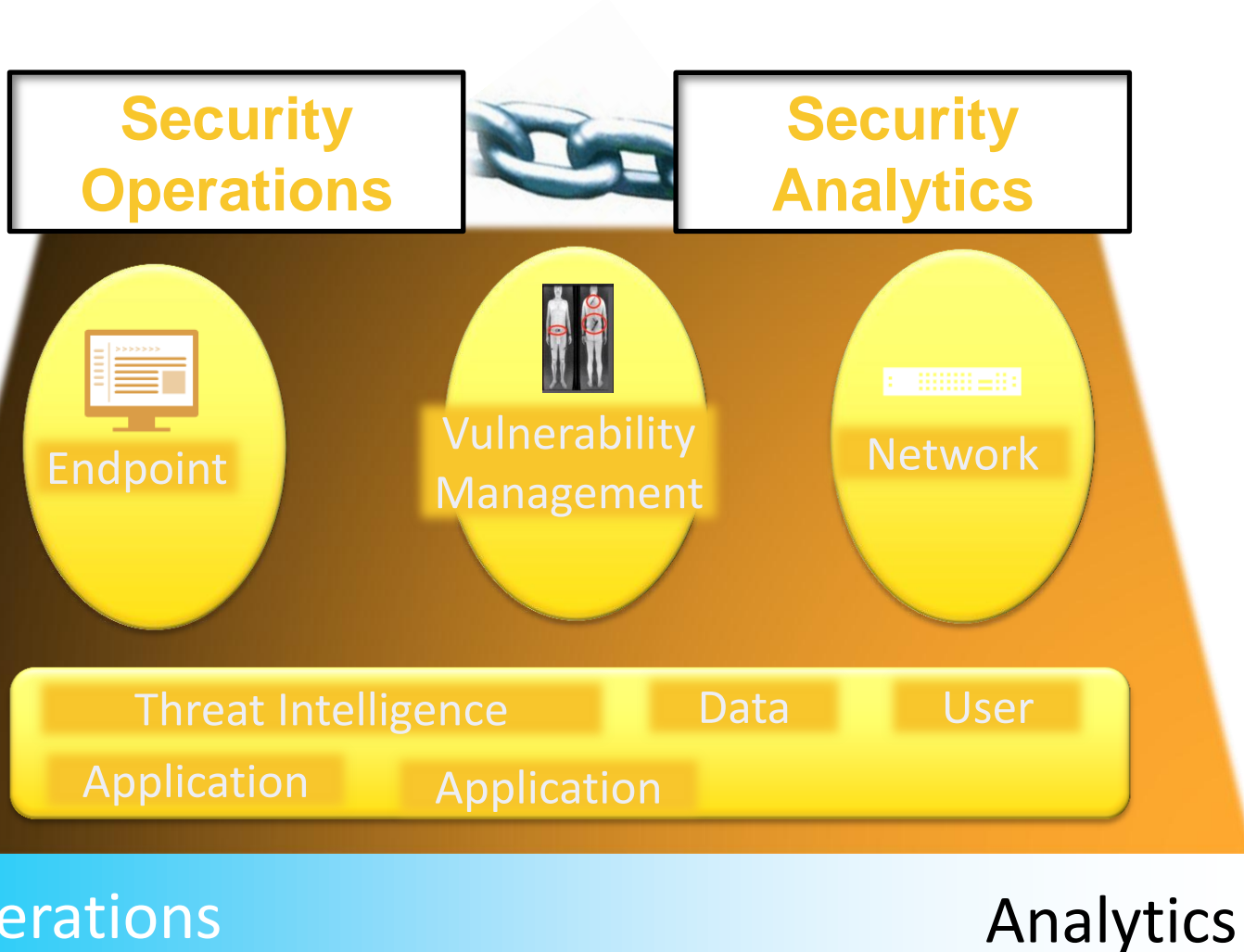
TCO
(CapEx + OpEx)

SECURITY
POSTURE

SECURITY OPTIMIZATION

Bridge Silos

Connected, Intelligent, Real Time



Security Analytics Needs



MOVE FAST

Performance in all areas – insertion, enrichment, queries, dashboards, analytics – is essential



LEARN QUICKLY

Turn billions of “so what” events into Actionable Information via context, content and advanced analytics



ACT DECISIVELY

Understand common scenarios, automate steps, streamline processes

Missing Something?

January

:

Email
Sent

February

:

File Share
Access



March:
UDP

Internal Services

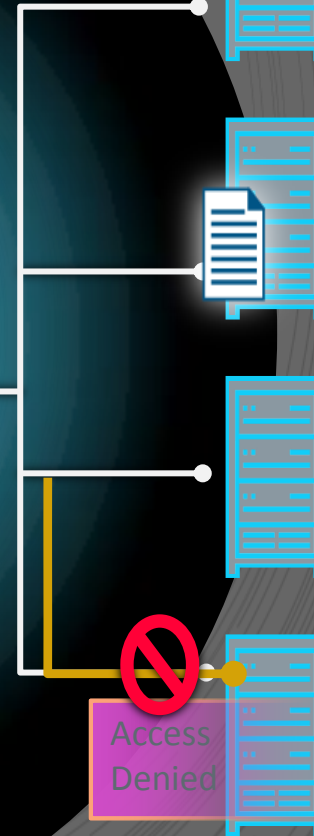
External
IP 1



HTTP
File
Download



External
IP 2

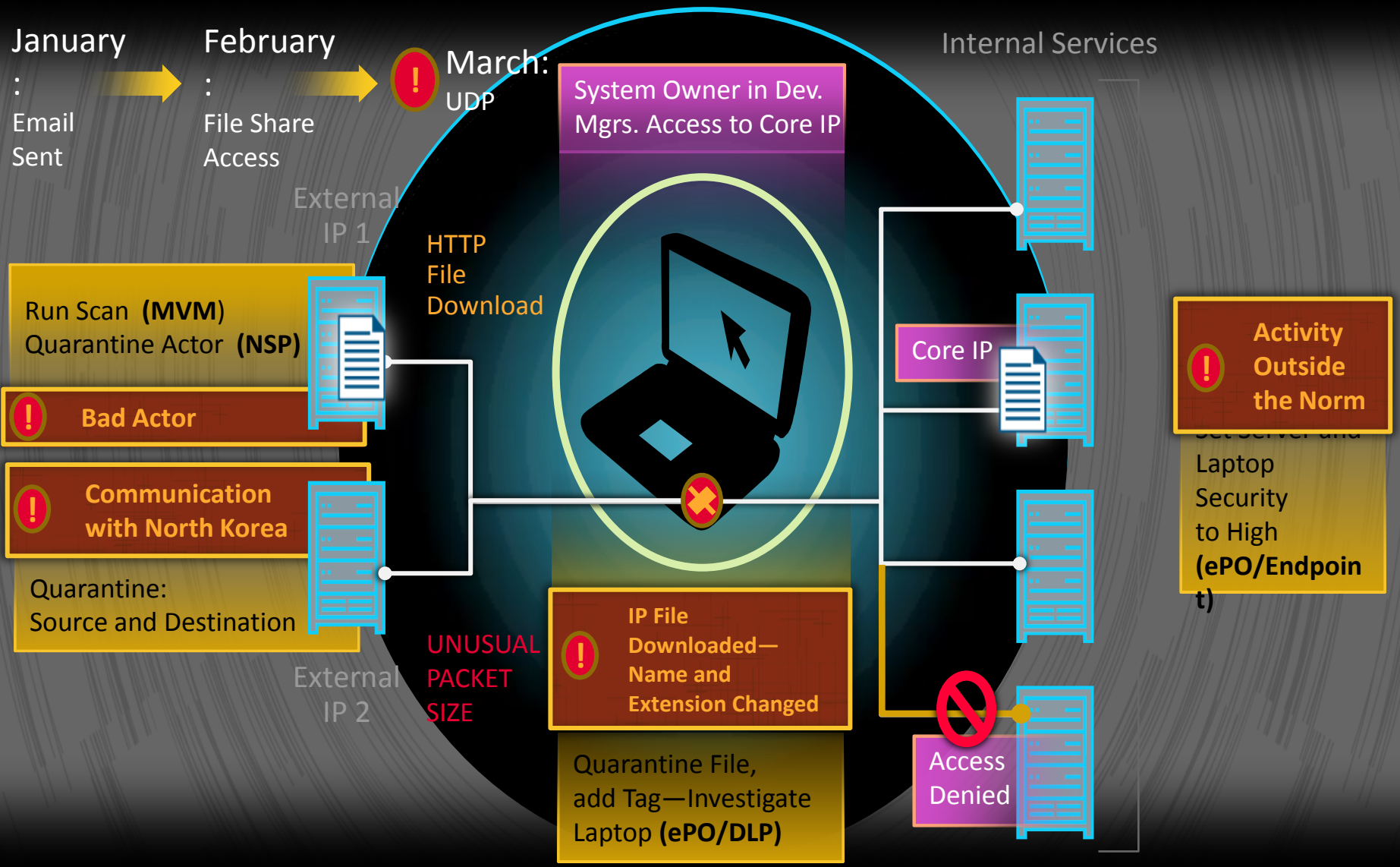


Verdict
Misconfiguration

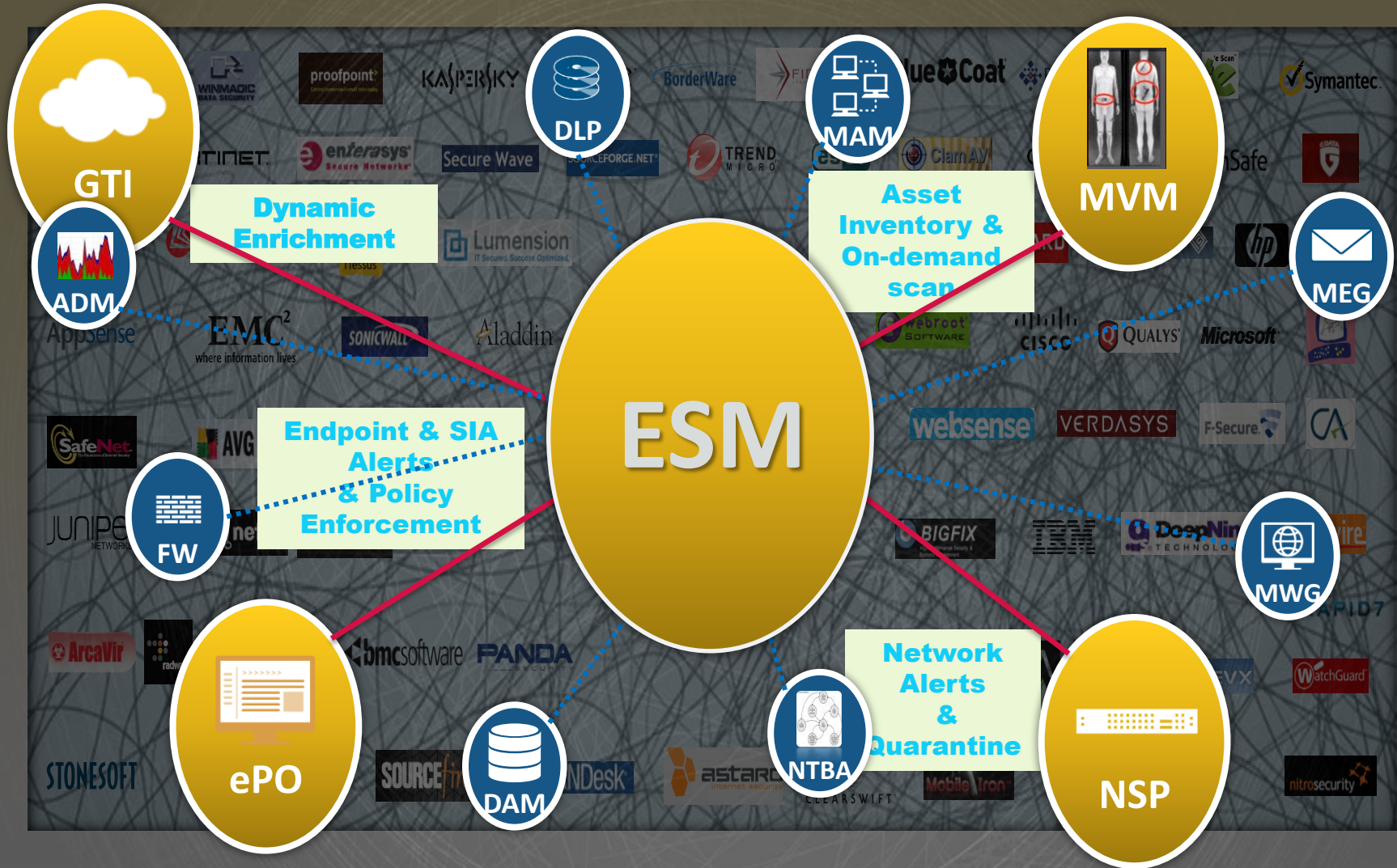
Access
Denied

Verdict:
USER
ERROR

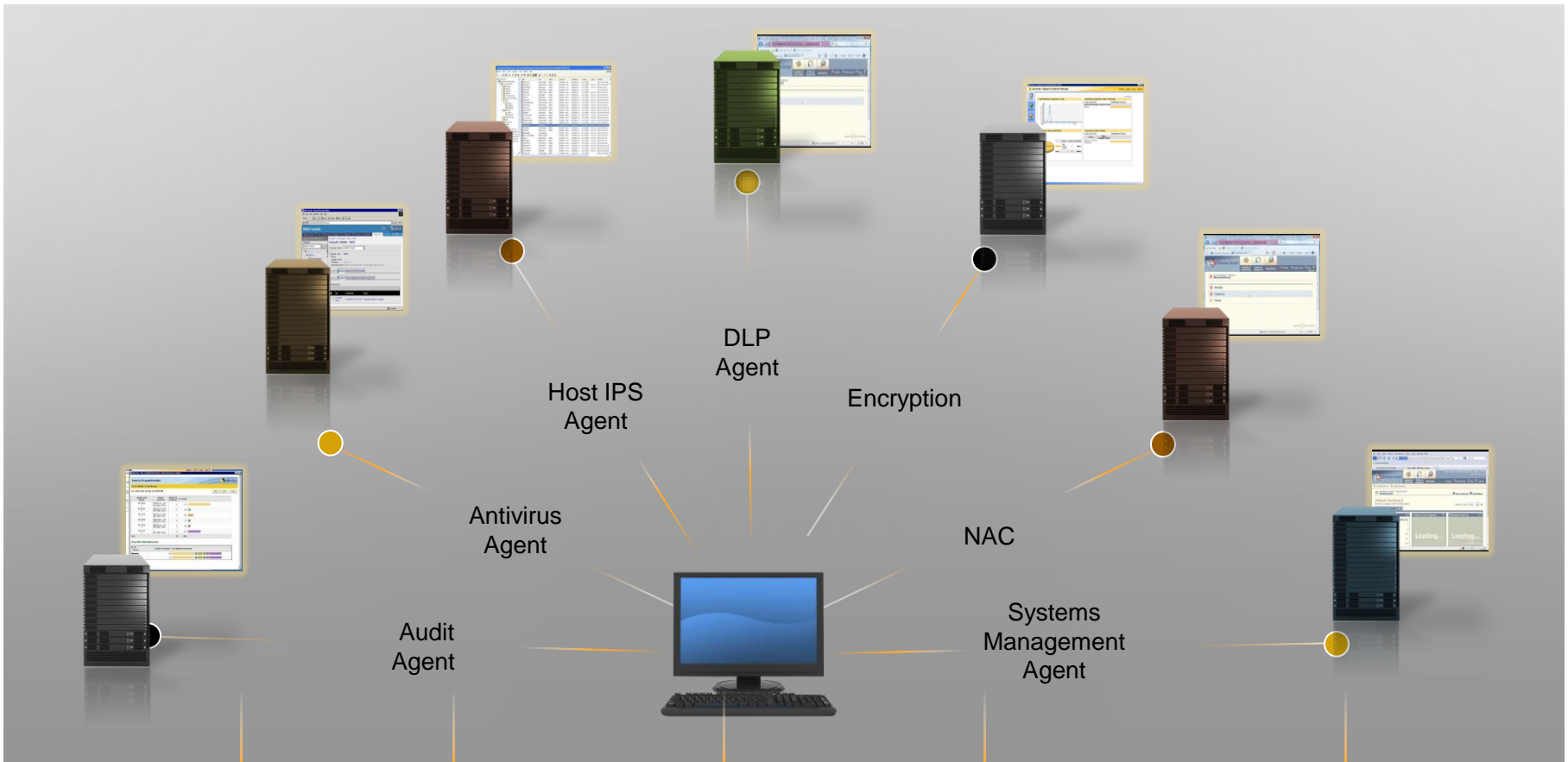
Acting with Context



Intelligent Integration Example



Consolidating Operations



EVERY SOLUTION HAS AN AGENT

EVERY AGENT HAS A CONSOLE

EVERY CONSOLE REQUIRES A SERVER

EVERY SERVER REQUIRES AN OS/DB

EVERY OS/DB REQUIRES PEOPLE, MAINTENANCE, PATCHING

WHERE DOES IT END?

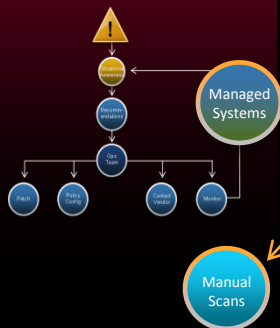
Common Security Use Cases

Unknown Threat

Non-Optimized

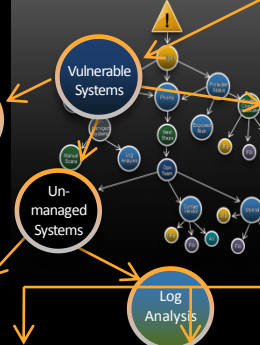


Optimized

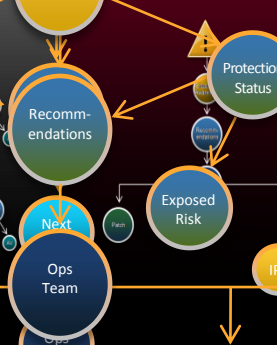


Consumption of IT

Non-Optimized



Optimized



Advanced Persistent Threats

Non-Optimized



Optimized



Continuous Compliance

Non-Optimized



Optimized



Data Protection

Non-Optimized



Optimized



Next Generation Network Security

Non-Optimized



Optimized



Streamlining Security Management

AUTOMATIC,
INTELLIGENT,
CONNECTED

- Drastically shorten time to respond and improve visibility
- Actionable intelligence through contextual SIEM
- The answers you need....Now