



HP Enterprise Security Services

Technology View of the Management and Monitoring of Security Incidents

Markus Muessig – HP Enterprise Security Services

29.04.2015 / Bratislava

Agenda

- ▶ Excerpt
- ▶ The Basis: A Changing Threat Landscape
- ▶ Conclusion: Strategic Preparation
- ▶ Technology: A “modern” SIEM approach
- ▶ Overall Picture: A SIEMs role in Incident Management



Excerpt

Technology View of the Management and Monitoring of Security Incidents



Modern SIEM Solutions and their role in Incident Management

Excerpt

Modern SIEM Solutions and their Role in Incident Management

To face modern threat landscape, detection capabilities have to evolve on all three areas, processes, people and technology.

This short introduction explains what a modern SIEM solution must contribute to the overall companies incident monitoring and response capabilities not failing to support modern threat scenarios including missing user awareness and “Advanced Persistent Threats”.

It covers its own claim in attack detection, its role in incident monitoring and how it covers modern attack scenarios.



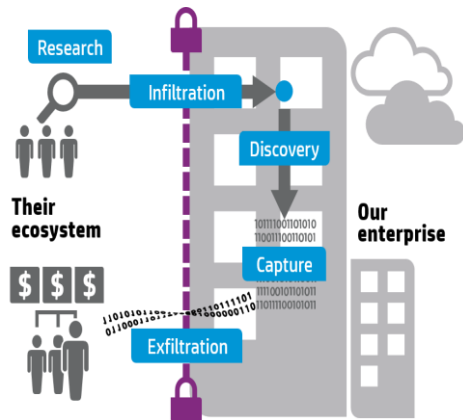
The Basis:

A Changing Threat Landscape

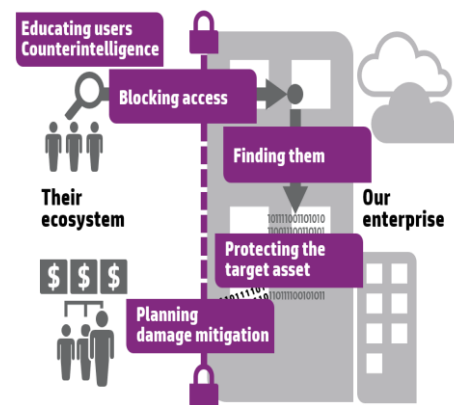


The Basis: A Changing Threat Landscape

What we need to deal with has changed



The Adversary	The Good Boys
Time	Business Knowledge
Budget	Infrastructure Knowledge
People	Proven Methodologies
Creativity	



The Conclusion:

Strategic Preparation



The Conclusion: Strategic Preparation

What we need to deal with has changed

Modern Threats force us to

- Better understand our business, especially in the IT departments
- Use our internal knowledge to our advantage
- Prepare for the inevitable
- Align our mindsets to the real world (e.g. zero trust, you will get hit, prepare yourself)
- Train our personnel, especially in the awareness sector
- Make your VIPs aware of being one

Start a journey for more security and business awareness and efficiency



The Technology:

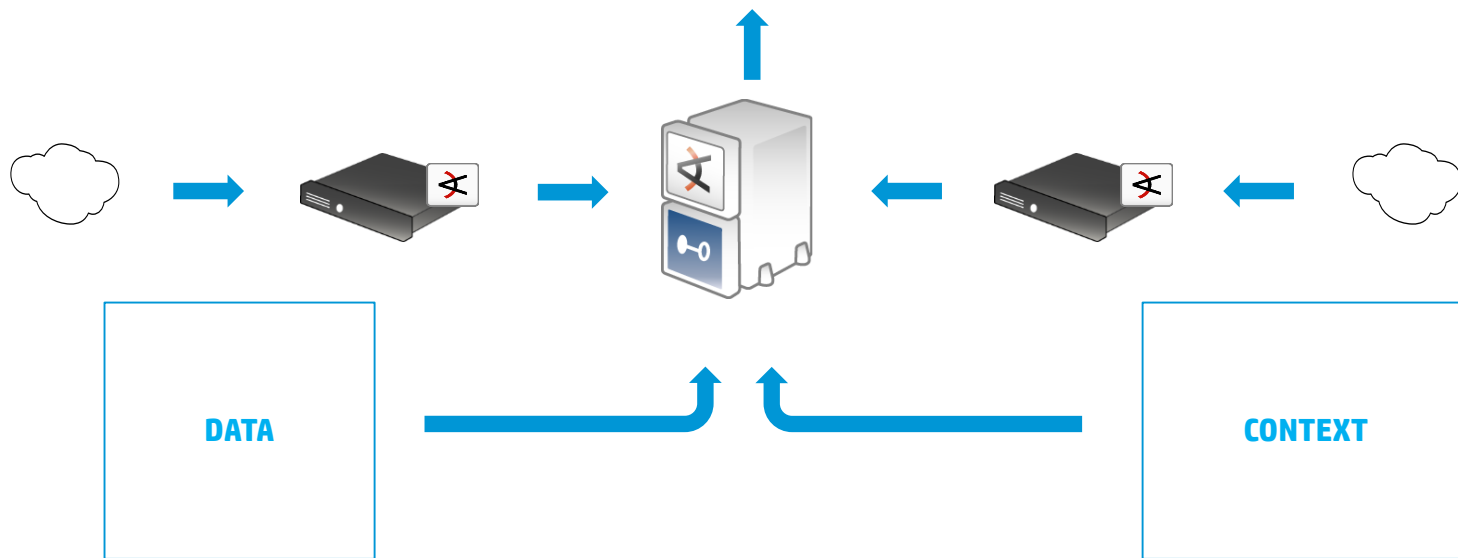
A “modern” SIEM approach



The Technology: A “modern” SIEM approach

Is it really modern?

Value added security monitoring protecting your business



The Overall Picture:

A SIEMs Role in Incident Management



The Overall Picture: A SIEMs role in Incident Management

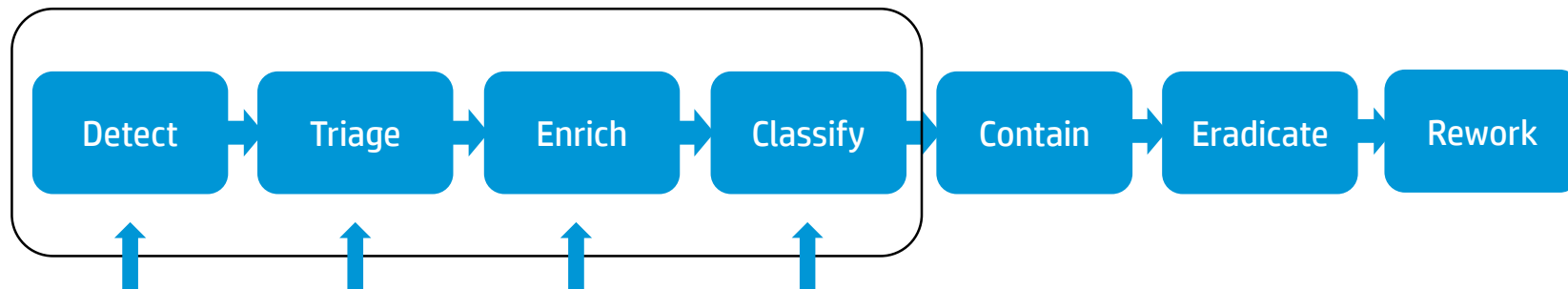
What to expect from a SIEM and what not?

Incident Management and Response



The Overall Picture: A SIEMs role in Incident Management

What to expect from a SIEM and what not?



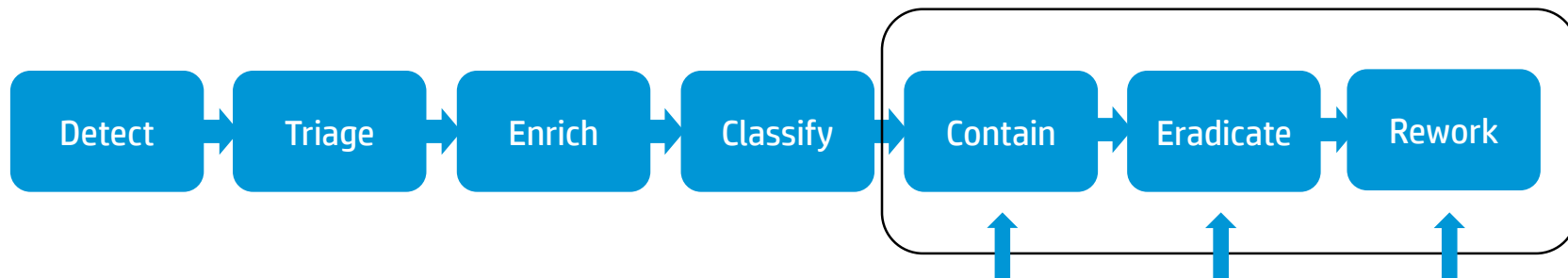
A well performing SIEM solution can:

- Report a critical event directly into your IM process
- Initially tell you about a priority and type of threat
- Give you directions with regards to locality and user context
- Give you business impact indicators



The Overall Picture: A SIEMs role in Incident Management

What to expect from a SIEM and what not?



Additionally, it can

- support containment by giving you information for an efficient response
- Support your countermeasure definition by giving you details about the network behavior of the reported alert
- Support your forensic investigation
- Support your CSI (continuous service improvement) by detailing, what would have avoided the incident

Takeaways

What were the major takeaways from the last 25minutes

25 minutes is way to short for such a topic 😊



Takeaways

What were the major takeaways from the last 25minutes

Summary

- Take care of your SIEM and it will take care of your business.
- A SIEM solution can NEVER protect, but enable for efficient reaction.
- A SIEM solution requires not just log- or event data to function properly.
- Do not trust “out of the box” solutions. They never deliver good context.
- SIEM solutions are as good as the information you feed into them (at a minimum).
- Pay as much attention as you can on context data.
- Contact me, if you have further questions or require project support.



Thank You

Markus Muessig

Lead Solution Consultant – SIEM/SOC/TVM/DIS

Mail: markus.muessig@hp.com

Mobile: +49 173 34 75 275

