Schopnosti a zralost kybernetické obrany organizací

HP Enterprise Security

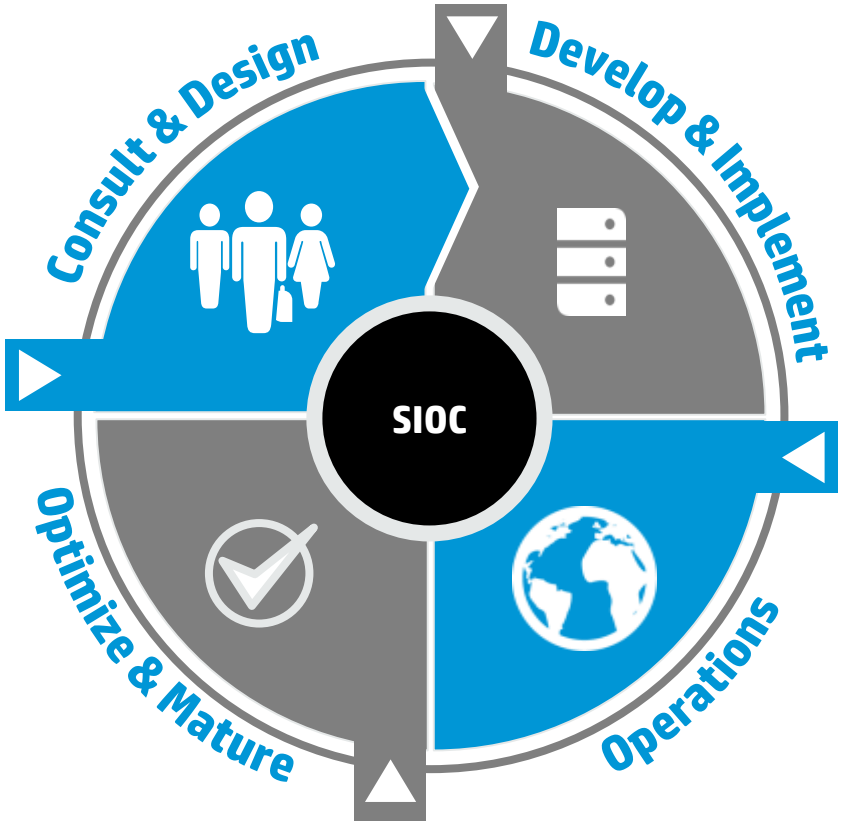
31.3.2015

Petr Hněvkovský, CISA, CISSP, CISM

Senior Security Architect

Security Intelligence & Operations Consulting

Založeno: 2007



hp.com/go/sioc

Zkušenosti:

- 40+ SOC postaveno
- 117+ SOC hodnocení (Assessments)
- 30+ SIOC konzultantů

Filozofie:

- Byznys priority
- LPT – Lidé, Procesy, Technologie

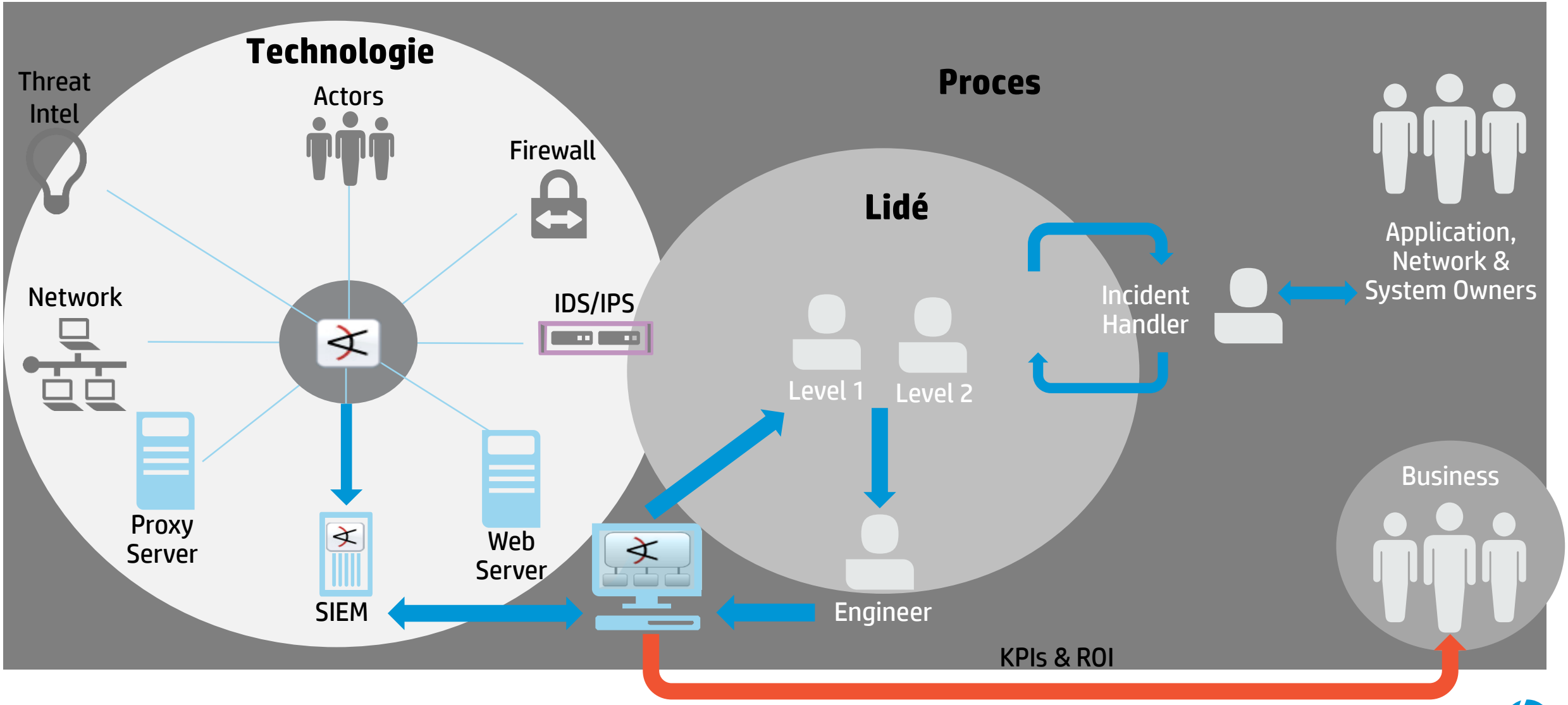
Zrychlený úspěch:

- Metodika zralosti a schopnosti SOMM
- Best Practices
- Široké znalosti a zkušenosti

Účel:

Zajištění, aby naši zákazníci byli úspěšní, poskytnutním správných **Lidí**, vybudováním řádných **Procesů** a dodáním efektivní **Technologie**.

SIOC koncept provozu SOC



SIOC Metodika SOMM

Byznys

- Mise (54)
- Odpovědnost
- Sponzor
- Vztahy
- Výstupy
- Angažovanost
- Vybavení

Lidé

- Obecné (65)
- Výcvik
- Certifikace
- Zkušenosti
- Dovednosti
- Kariérní cesta
- Vedení

Proces

- Obecné (65)
- Provozní
- Analytické
- Bysnysové
- Technologické

Technologie

- Obecné (56)
- Architektura
- Sběr dat
- Monitorování
- Korelace
- Integrace

Příklad – workflow eskalace hrozby

Categories	SIEM Priority Levels				
	0-2	3-4	5-6	7-8	9-10
Unauthorized Root/Admin Access	A	A	A	C1	C1
Unauthorized User Access	A	A	I2	C2	C1
Attempted Unauthorized Access	A	A	A	I3	C3
Successful Denial of Service	A	A	I2	C2	C1
Policy Violation	A	A	T3	T2	T1
Reconnaissance	A	A	A	I3	I2
Malware Infection	A	A	T3	T2	C2

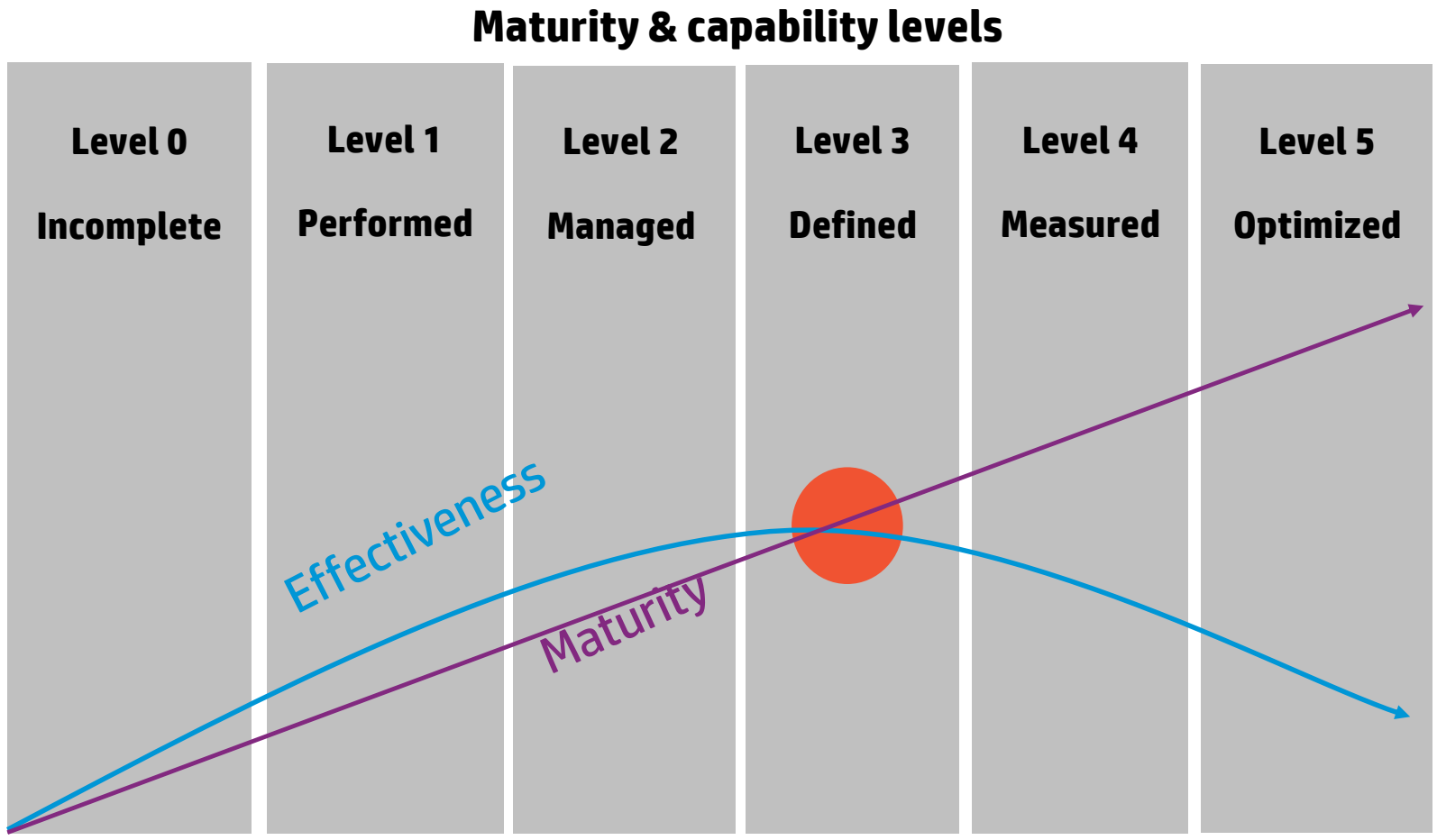
Legend

- **C1:** Critical callout –15 min
- **C2:** Urgent callout –30 min
- **C3:** Routine callout –2 hr
- **I2:** Urgent investigation
- **I3:** Routine investigation
- **T1:** Critical ticket opened
- **T2:** Urgent ticket opened
- **T3:** Routine ticket opened
- **A:** Active monitoring

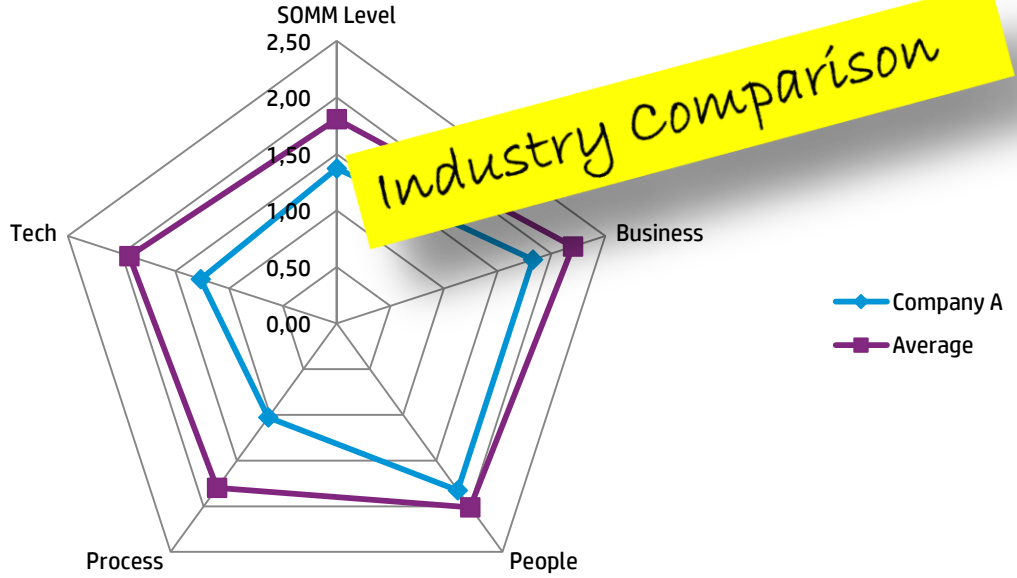
Zralostní model SOMM – Maturity and Capability model

Metodika

- Kvantitativní hodnocení BLPT (Byznys, Lidé, Process, Technologie)
- Derivát Carnegie Mellon – *Software Engineering Institute's - Capability Maturity Model for Integration* (SEI-CMMI)
- Meziroční a také oborové srovnání



SIOC zralostní model



Industry Comparison

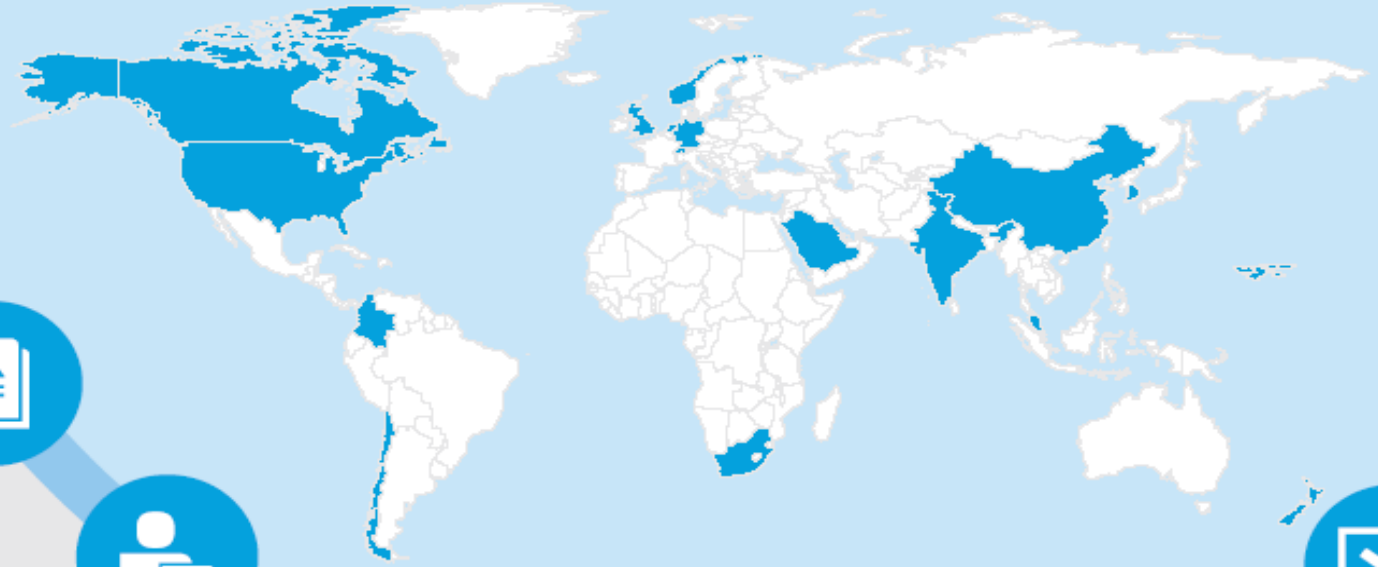
Maturity Assessment	Jan-14	Dec-14	Year-to-Date Change
BUSINESS	**1.67**	**2.82**	**69.00%**
Mission	2.77	2.84	[illegible]
Accountability	1.16	2.29	[illegible]
Sponsorship	2.00	[illegible]	[illegible]
Relationship	[illegible]	[illegible]	180.91%
Deliverables	[illegible]	[illegible]	129.59%
Vendor Engagement	[illegible]	2.24	48.53%
Facilities	2.16	2.23	3.21%
PEOPLE	**1.70**	**2.55**	**50.18%**
General	1.66	2.22	33.87%
Training	1.46	2.89	97.87%
Certifications	1.16	2.22	91.64%
Experience	1.56	2.85	82.58%
Skill Assessments	1.57	2.82	79.78%
Career Path	1.12	2.48	121.65%
Leadership	1.00	2.98	198.00%
PROCESS	**1.20**	**2.52**	**110.24%**
General	1.72	2.30	33.43%
Operational Process	1.65	2.93	77.30%
Analytical Process	1.26	2.82	124.15%
Business Process	1.74	2.30	32.14%
Technology Process	1.16	2.29	97.35%
TECHNOLOGY	**1.00**	**2.89**	**188.52%**
General	1.14	2.30	101.66%
Architecture	1.47	2.28	55.43%
Data Collection	1.75	2.89	65.14%
Monitoring	1.46	2.93	100.61%
Correlation	1.11	2.30	107.20%
Overall SOMM Level	**1.39**	**2.70**	**93.60%**

Maturity Scorecard

	Current	Phase 1	Phase 2	Phase 3
Timeline		6 mos	1 yr	2 yr
SOMM Target	1.6	2.0	2.5	3.0
Use Cases	Logging	Perimeter, compliance	Insider Threat, APT	Application Monitoring
Staffing	Ad hoc	4 x L1, 1x L2	8 x L1, 2x L2	12 x L1, 2x L2, 2x L3
Coverage	8x5	8x5	12x7	24x7

Roadmap

State of security operations | *2015 report of capabilities and maturity of cyber defense organizations*



118 assessments of **87** SOCs in **18** countries across **6** continents

2nd annual report

Median Security Operations Maturity Model (SOMM) score: **1.55**
Target SOMM score: **3**

#1 issue: Finding and retaining skilled resources

Significant increase in sharing of threat intelligence

87% of SOCs are not meeting recommended maturity levels

4 categories assessed: people, process, technology, and business

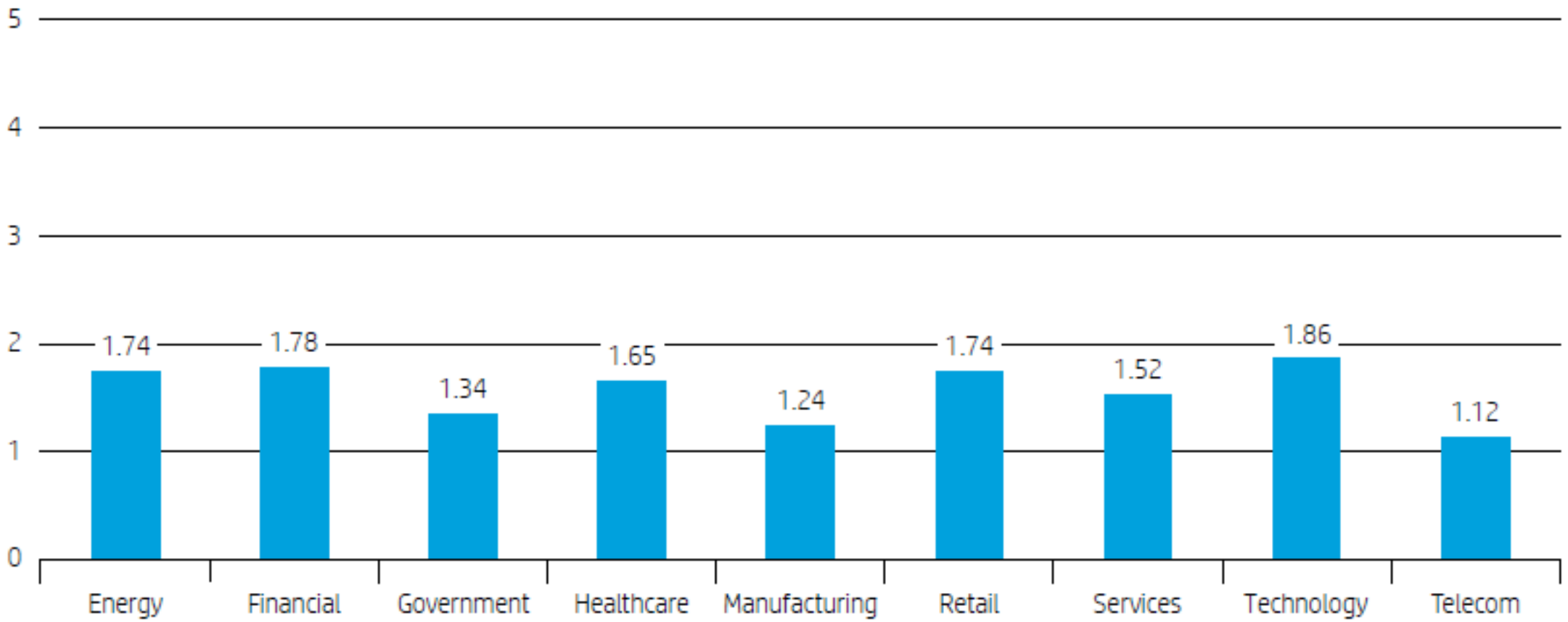
20% of SOCs are failing to achieve minimum security monitoring capabilities

% of SOCs that are achieving minimum security monitoring capabilities without a SIEM: **0**

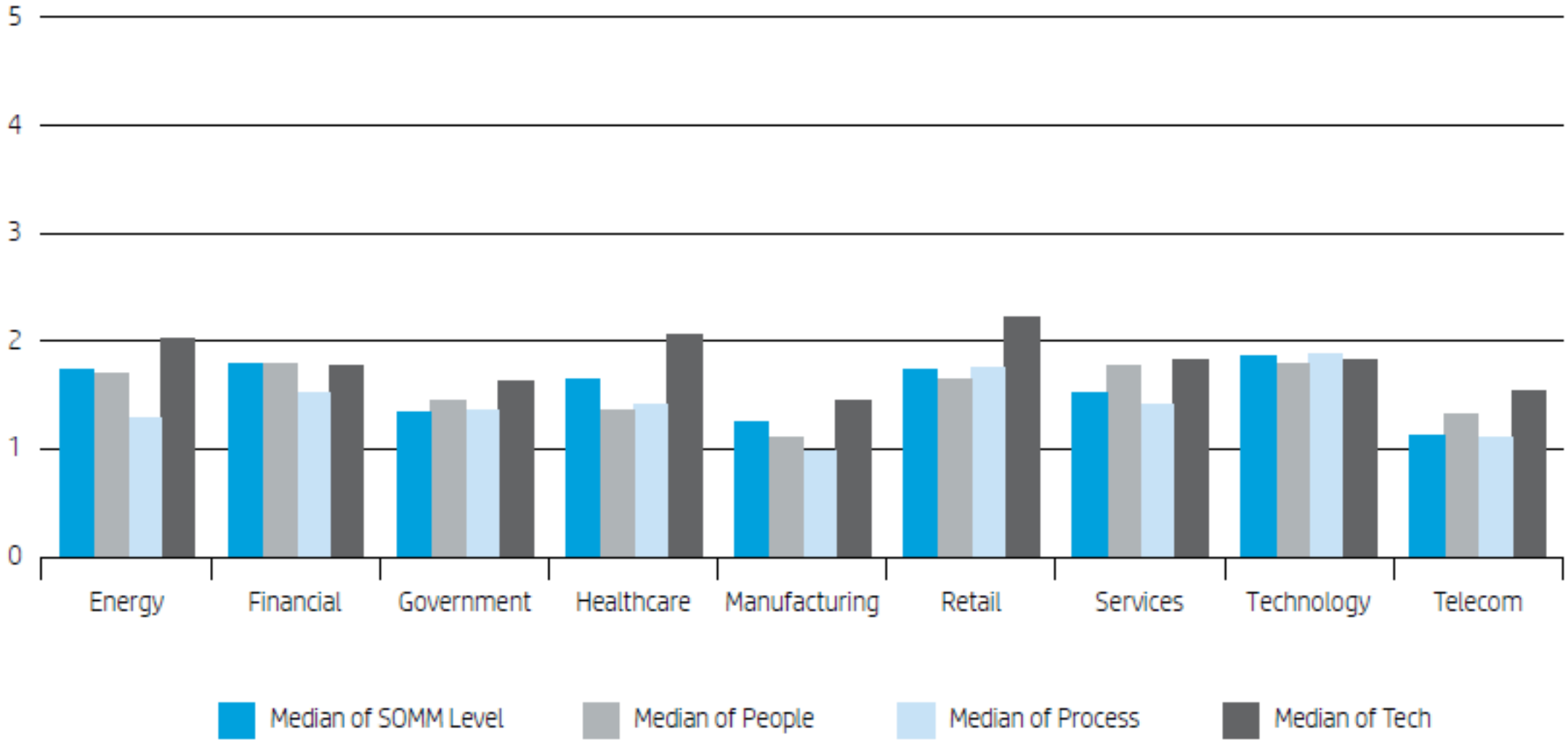
Highest scoring industry: **Technology**
Lowest: **Telecom**

Read the full report at **hp.com/go/StateOfSecOps**

Median SOMM skóre dle oboru



Median SOMM dle oboru a BLPT oblasti



Hlavní trendy

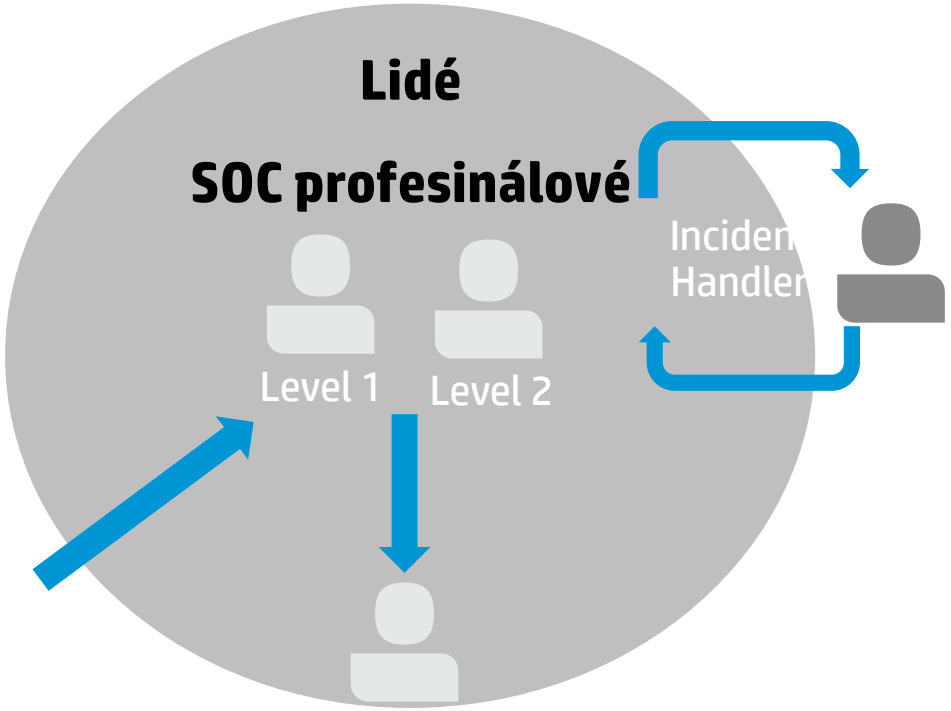
#1 Problém – Nábor a udržení nadaných profesionálů

Znalostní vakuum

Evoluce zevnitř je často rychlejší nežli nábor zvenku

Kariérní postup, směny, přidělení, prostředí

Dobře míněné, ale často zavádějící až nevhodné metriky

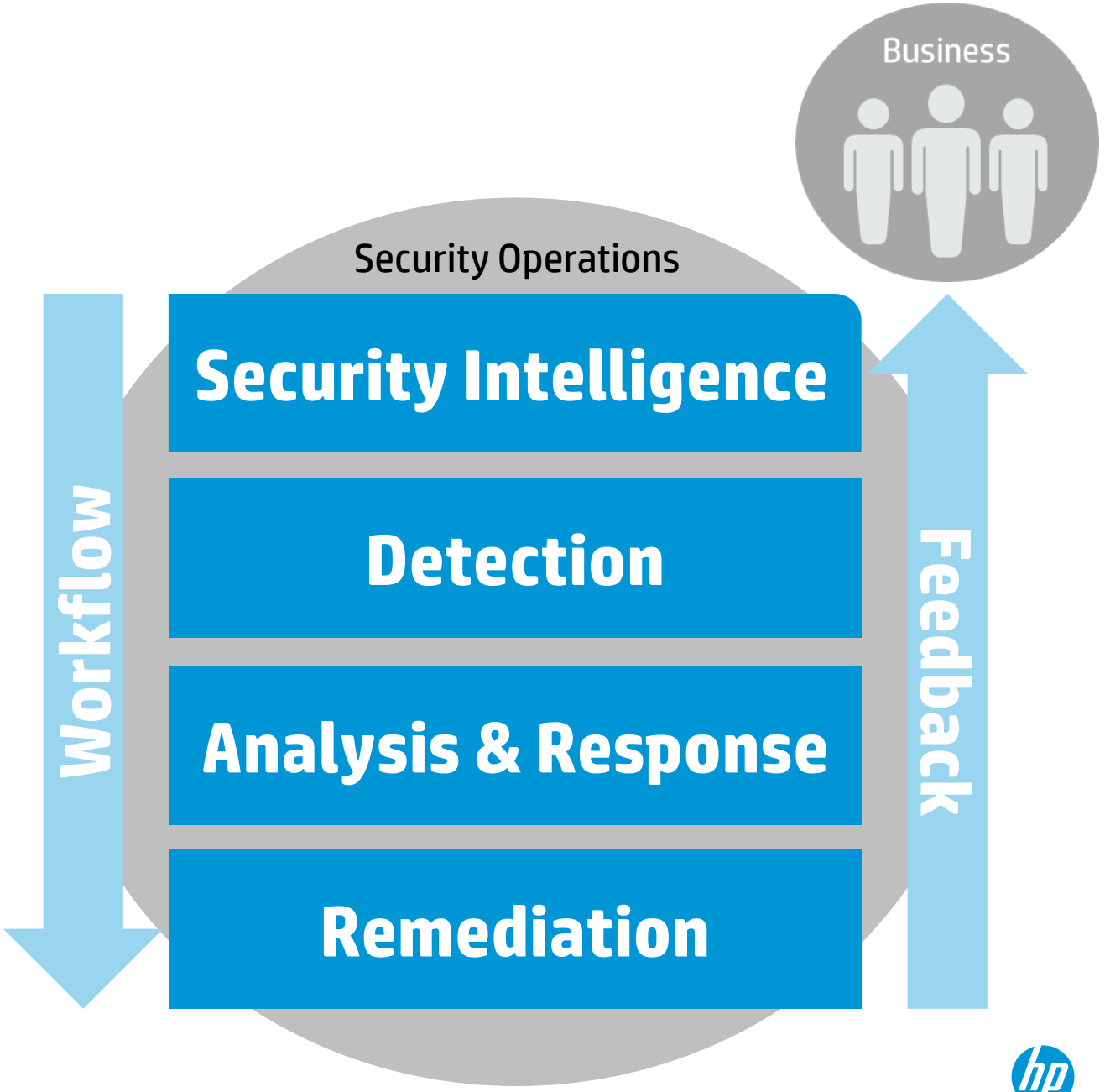


Bezpečnost pro nebezpečáky

Veřejné hrozby a průniky jsou známé

Byznysový reporting – „Co to znamená pro naší misi?“

“Don’t scare them” – Meg Whitman, HP CEO

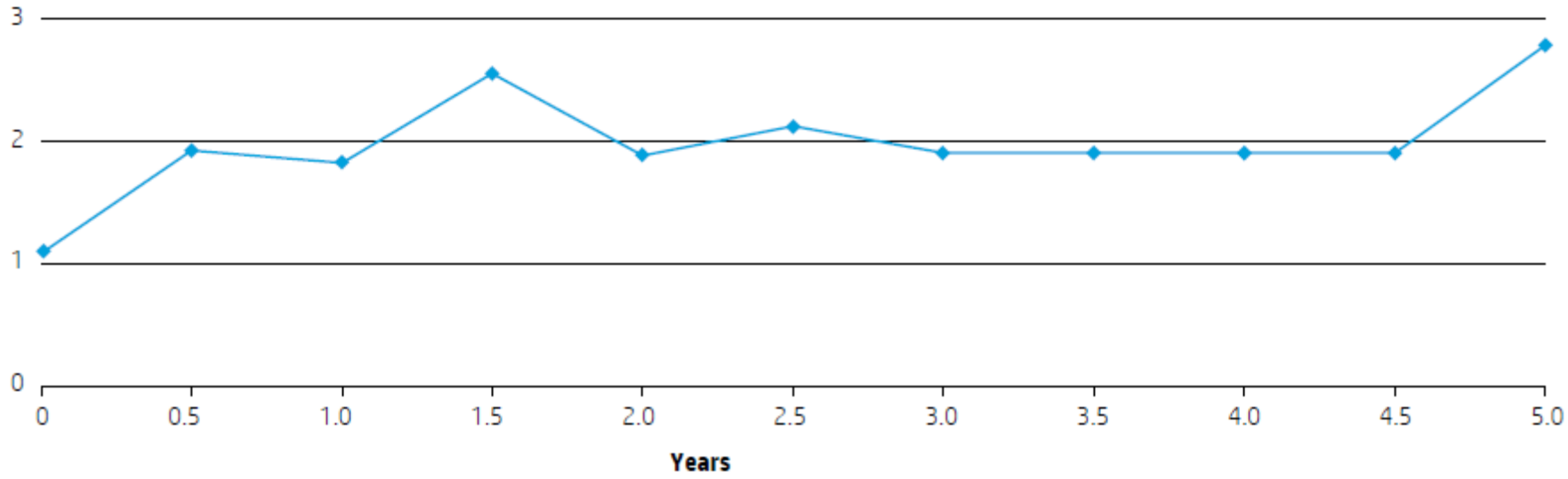


SOC je program a nikoli projekt!

SOMM zralost často dosáhne špičky po cca 18 měsících od zahájení

Nejčastěji díky ztrátě podpory vedení anebo nevhodnému zadání

Figure 5. Median SOMM Score by Age of SOC



Bolestný růst technologií

Společnosti hledají švýcarský nůž na bezpečnost

Některé organizace nezvládají základní bezpenostní principy

Chybí plán do budoucna a připravenost na postupné dozrání

Škálovatelnost a otevřenost

Děkuji za pozornost

hp.com/go/StateOfSecOps

hnevky@hp.com

Backup slides

Ensure the Operations are Repeatable

Subtle Event Detection
- Data Visualization
- Pattern Analysis

Reporting
- Analyst Comments
- Incident Summary
- Threat Reports

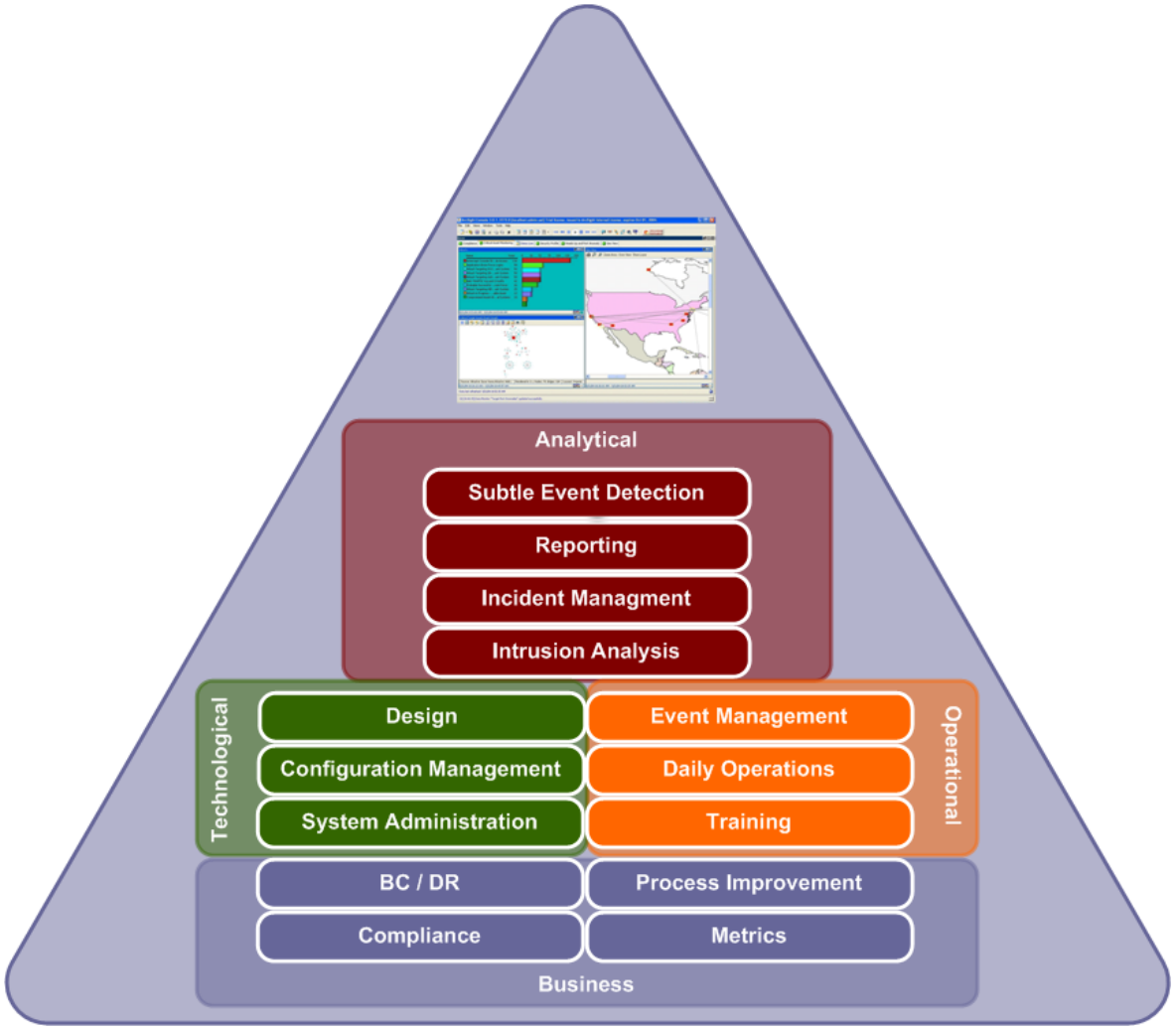
Incident Management
- Incident Research
- Focused Monitoring
- Incident Response

Intrusion Analysis
- Event Analysis
- Threat Intelligence
- Information Fusion

Design
- Developing Use Cases
- User and Asset Modeling

Configuration Management
- SIEM Architecture
- Data Feed Integration
- FlexConnector Development

System Administration
- Access Management
- Maintenance and Upgrades



Event Management
- Triage
- Callouts
- Case Management
- Crisis Response

Daily Operations
- Shift Schedule
- Monitoring
- Problem and Change
- Shift Turn-Over
- Daily Operations Call

Training
- Training plans
- Skills Development tracking

BC/DR
- Business Continuity Plan
- Disaster Recovery Plan

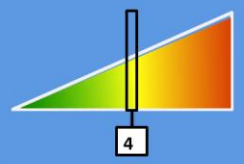
Process Improvement
- Maturity Assessments
- Project Methodology
- Knowledgebase (wiki)

Compliance
- Internal Compliance
- Compliance Support

Metrics
- Reporting KPIs
- SIEM Performance
- Operational Efficiencies

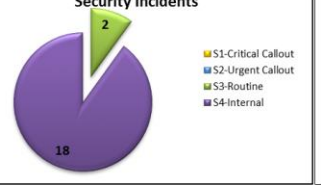
Line of Business Reporting
Answer the “so what?” question

Threat Score



This threat score is a calculated value which is derived from all of the components reported in this monthly threat report. The previous months threat score was 54 for the month of October. All cases investigated this month were routine and thus the score was slightly reduced.

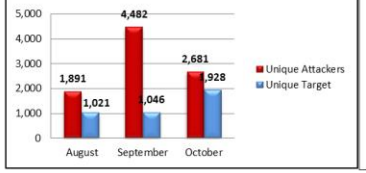
Security Incidents



How many incidents required a response?

The pie chart on the left show the number of cases opened during the previous month sorted by severity. This month the majority of opened cases were internal cases within the GSOC requiring further analysis. The two cases opened for formal incident management ...

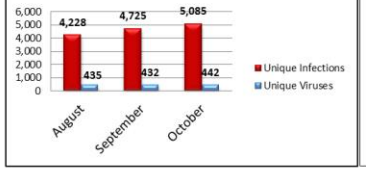
Intrusion Detection



How many attackers are targeting ArcSight?

This bar chart shows the total number of unique attackers and targets detected during the past three months. The ratio of attacker to target is also of particular interest. In October the number of attackers declined but the number of attacked hosts increased significantly.

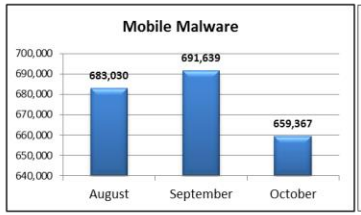
Anti-Virus



What is the malicious code threat?

This bar chart shows the total number of virus infections compared with the number of distinct viruses detected. These values can diverge in several ways all of which are meaningful. This month we saw a minimal increase in unique virus types as well as an increase in unique infections.

Mobile Malware

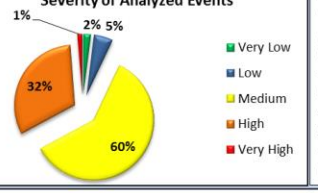


How much mobile malware was detected?

The bar chart on the left shows the unique number of mobile malware infections detected over the previous three months by Fortinet. In the Month of October there was a significant drop in the total number of infected mms messages.

GSOC - Operational KPIs

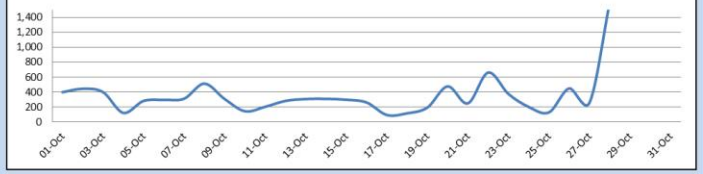
Severity of Analyzed Events



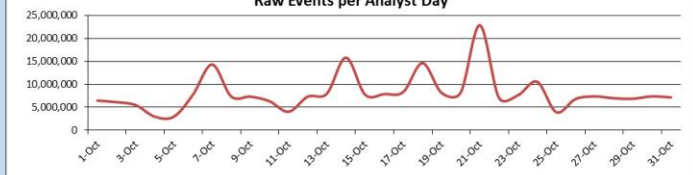
How many and how severe are the potential threats?

The following charts show the event volumes detected and their severity distribution. The bottom chart shows raw events, above that is analyzed events and the pie chart shows the severity distribution. This month with the boarding of the ArcSight Remote Data Center the event counts have spiked but are currently being tuned for more effective monitoring. An increase in raw events and decrease in analysed events is the ideal scenario .

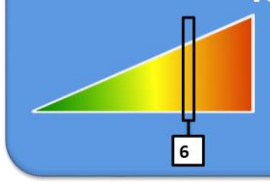
Events Analyzed per Day



Raw Events per Analyst Day

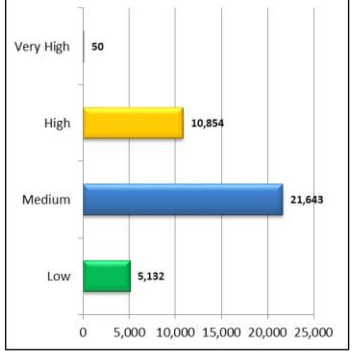


Vulnerability Score

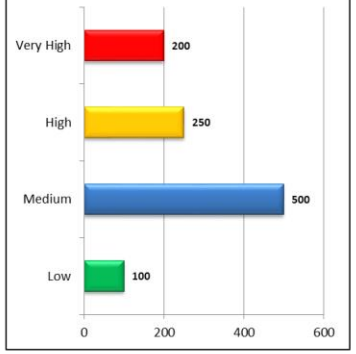


This vulnerability score is derived from the monthly scan information collected by Qualys for Internet addressable ArcSight systems. A score of 63 indicates a medium-high level of vulnerability.

External Scan Results (Qualys)



Internal Scan Results (nCircle)



Analyst Comments:

The monthly threat score is calculated at 41 for the month of October. Contributing factors include the decrease in case severity, the significant decrease in unique attackers and the increase in attacked hosts.

Currently we are monitoring 237 endpoint devices in ArcSight.

We scanned 6184 active hosts with Qualys and found 8116 vulnerabilities in total.

Real life examples how HP ArcSight has helped?

5 minutes to generate IT GRC report

Logger compliance packs generates IT GRC reports that otherwise would take 4 weeks

10 minutes to fix an IT incident

Text based searching and integration with BSM detects and corrects IT incident that otherwise would take 8 hours

3 days to run an IT audit

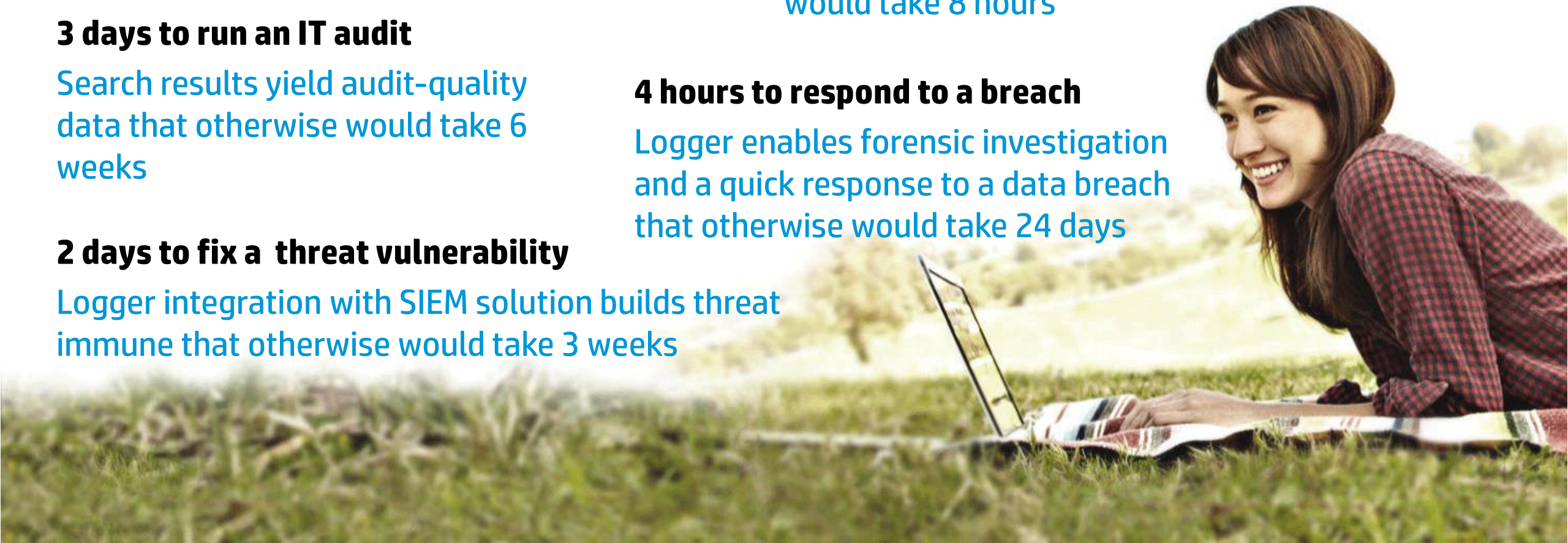
Search results yield audit-quality data that otherwise would take 6 weeks

4 hours to respond to a breach

Logger enables forensic investigation and a quick response to a data breach that otherwise would take 24 days

2 days to fix a threat vulnerability

Logger integration with SIEM solution builds threat immune that otherwise would take 3 weeks



Where do I find more information?

HP Security Intel & Ops Consulting: http://hp.com/go/sioc

Report: hp.com/go/StateOfSecOps

Blog: hp.com/go/securityproductsblog

SOC Maturity Assessment Solution brief:
http://h20195.www2.hp.com/V2/GetDocument.aspx?docname=4AA4-4144ENW&cc=us&lc=en