Key Findings from the 2017 State of Security Operations Report

January 26, 2017

Today's Speaker:

Kerry Matre
Director, Security Portfolio Marketing
Hewlett Packard Enterprise

Hewlett Packard Enterprise

The webinar will begin shortly.

vivit

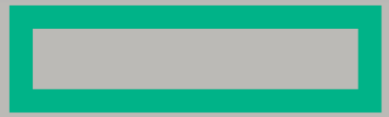
vivit

Discover the independent HPE software user community where you can share, collaborate, exchange, and grow

Key Findings from the 2017 State of Security Operations Report

January 26, 2017

Brought to you by



Hewlett Packard
Enterprise

YOUR INDEPENDENT HPE SOFTWARE USER COMMUNITY

vivit

Hosted By

Dominic Listermann
Managing Partner
Pyrafractal
Security and Privacy SIG Leader

Today's Speaker

Kerry Matre
Director, Security Portfolio Marketing
Hewlett Packard Enterprise

Webinar Housekeeping

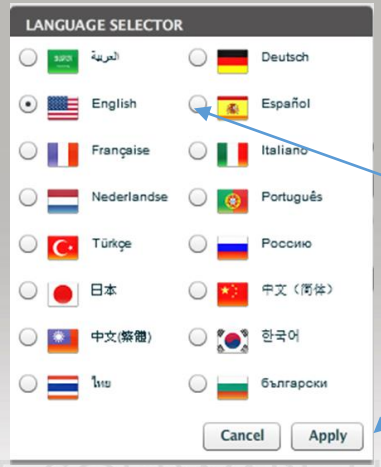
- This “LIVE” session is being recorded
- Recordings are available to all Vivit members
- To enlarge the presentation screen, click on the rectangle in the upper right hand corner of the Presentation pane

vivit

Webinar Control Panel

- Session Q&A:

  Please type questions in the Q&A pane
  and click on "Ask"
- Choose the language in which you would like to ask your questions



2017 State of Security Operations

4th annual report

- Released January 17, 2017
- Introduction by Matthew Shriner, VP HPE Security Professional Services
- 183 assessments since 2008
- 137 discreet SOCS
- 31 countries
- 6 continents
- Level 3 is recommended maturity score (4 for MSS)

Hewlett Packard Enterprise

Who do we assess?

- HPE customers and non-customers
- ArcSight users and non-users
- Organizations with or without a SIEM
- Government organizations, commercial and managed service providers

- Assessment is minimum of 3 days onsite with 2 consultants
- Observe SOC operations, review of documentation, interview with SOC members and interviews with business owners (CEO, CIO, GRC, etc.)

- Focus is less on “are you finding threats” and more on “are you prepared and likely to identify threats and do you have the capacity/processes to handle them quickly”

HPE Security Operations Maturity Model (SOMM)

Assessment Methodology

Business

- Mission
- Accountability
- Sponsorship
- Relationship
- Deliverables
- Vendor engagement
- Facilities

People

- Training
- Certifications
- Experience
- Skill assessments
- Career path
- Leadership

Process

- Operational processes
- Analytical processes
- Business processes
- Technology processes

Technology

- Architecture
- Data collection
- Monitoring
- Correlation

Hewlett Packard Enterprise

Maturity & Capability Levels

Security Operations Maturity Model (CMMI Based)

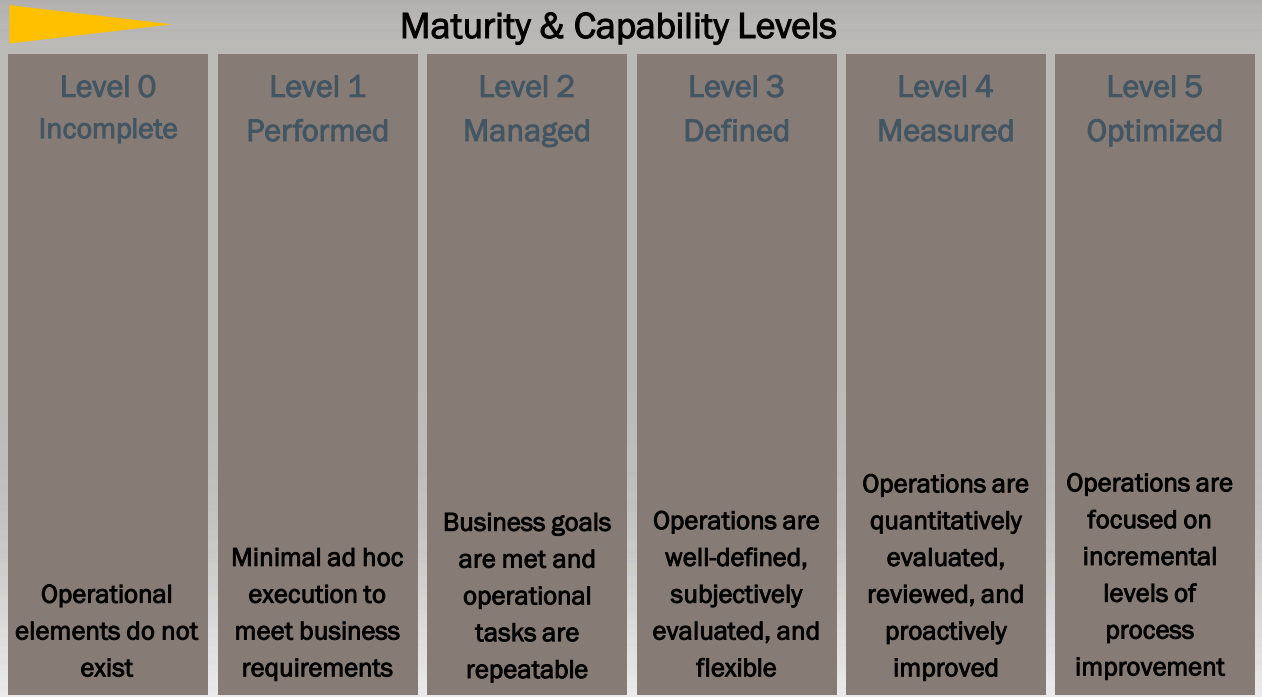
Assessment Methodology

- Quantitative assessment of business, people, process, and technology components
- Framework based on Carnegie Mellon Software Engineering Institute's Capability Maturity Model for Integration (SEI-CMMI)
- Year-to-year trends and comparisons across industries

Maturity & Capability Levels

Hewlett Packard Enterprise

Poll Question

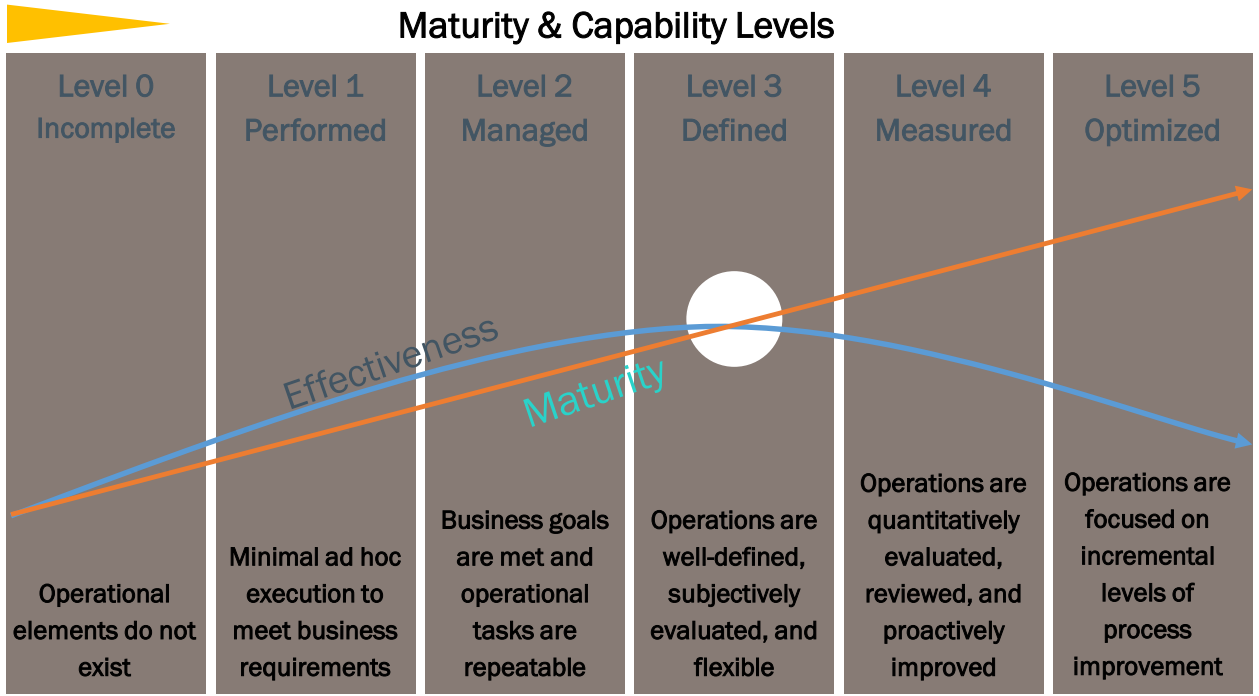


Maturity & Capability Levels

Security Operations Maturity Model (CMMI Based)

Assessment Methodology

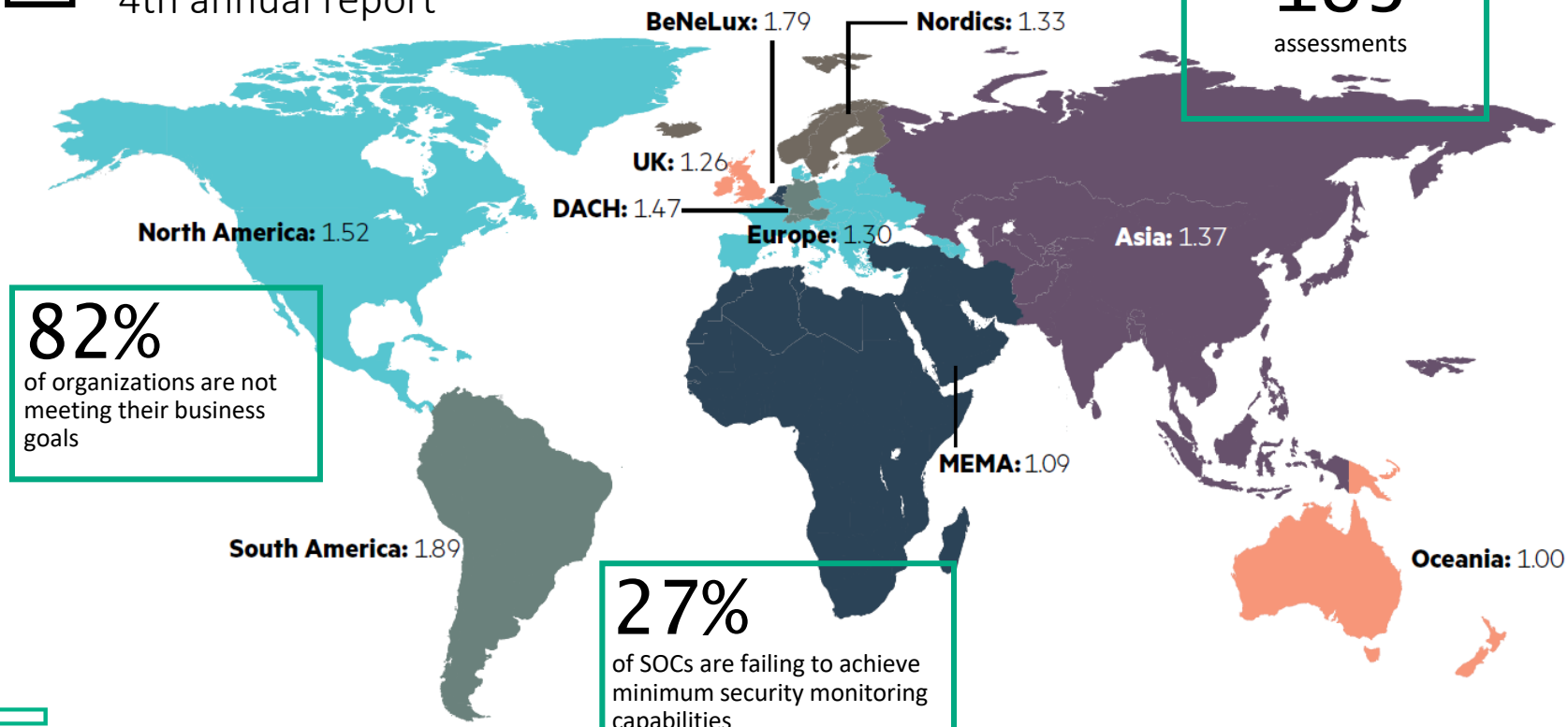
- Quantitative assessment of business, people, process, and technology components
- Framework based on Carnegie Mellon Software Engineering Institute's Capability Maturity Model for Integration (SEI-CMMI)
- Year-to-year trends and comparisons across industries



Hewlett Packard Enterprise

2017 State of Security Operations

4th annual report



183
assessments

82%
of organizations are not meeting their business goals

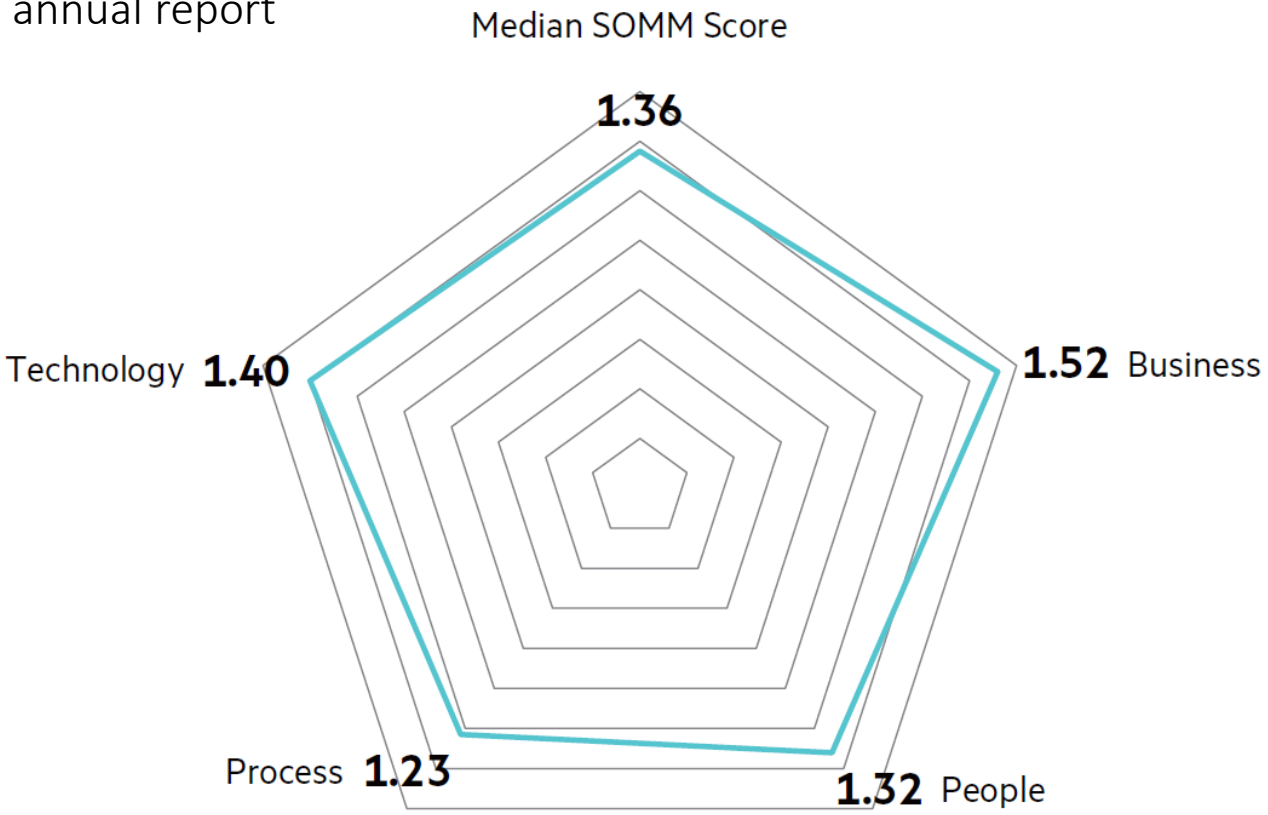
27%
of SOCs are failing to achieve minimum security monitoring capabilities

Hewlett Packard Enterprise

Read the full report at
hpe.com/software/StateOfSecOps

2017 State of Security Operations

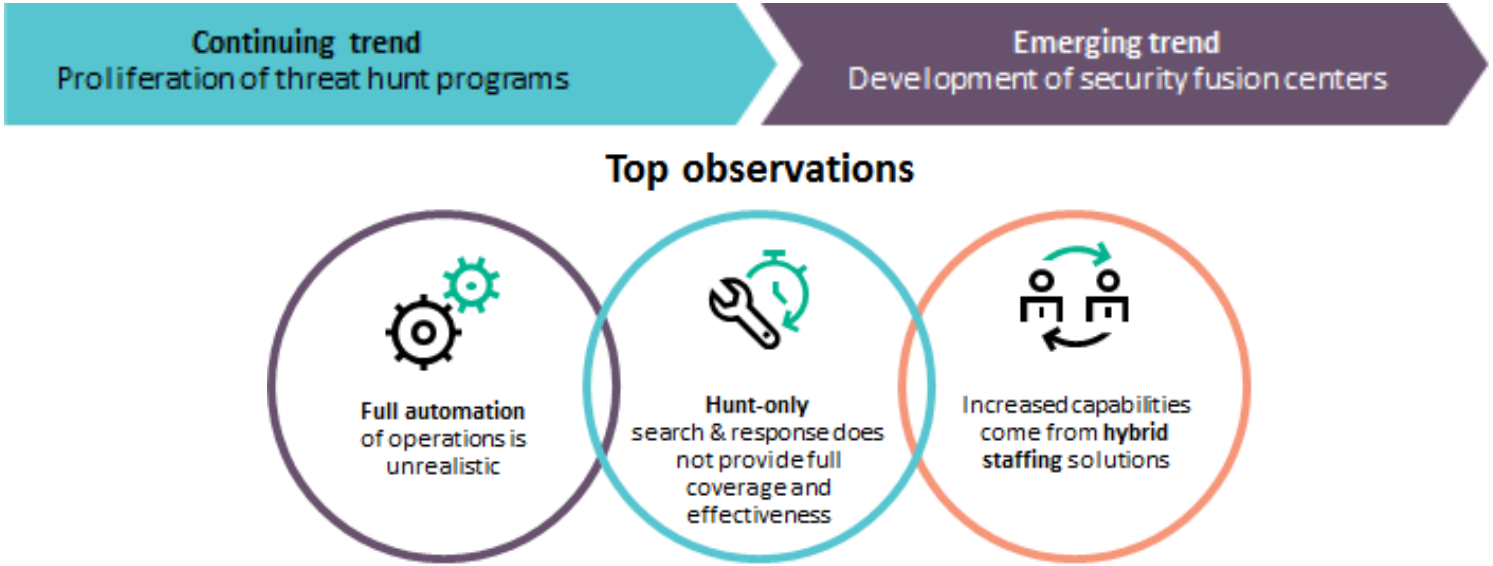
4th annual report



Hewlett Packard Enterprise

2017 State of Security Operations

4th annual report

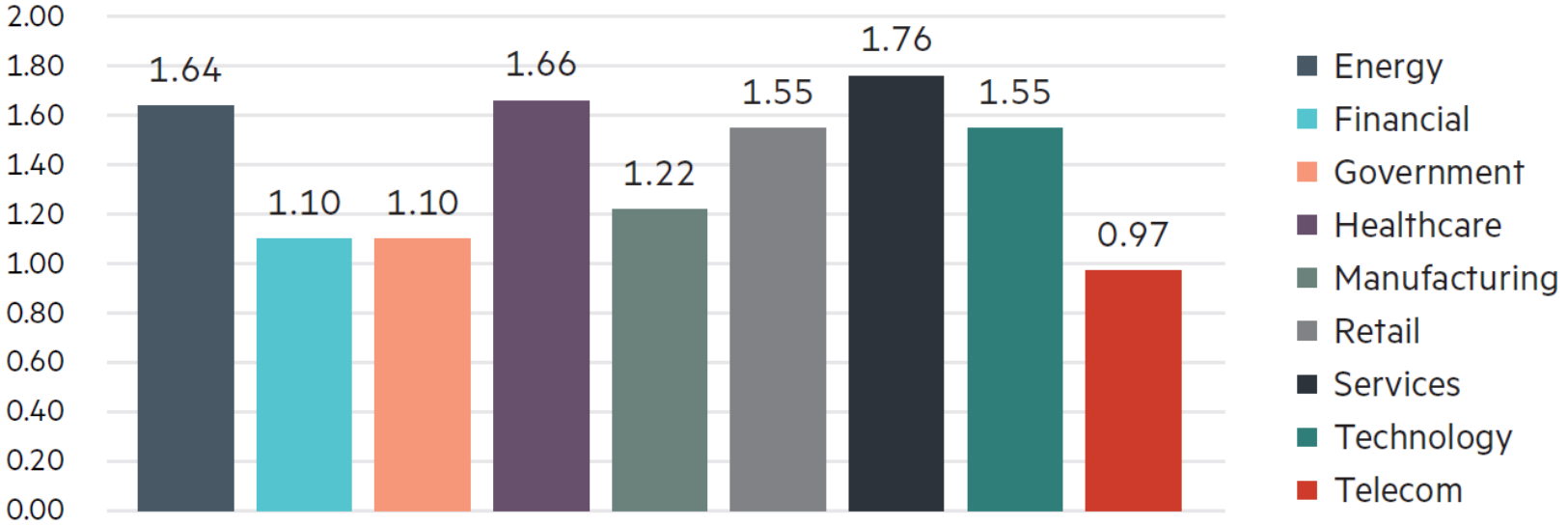


Business maturity outscored Technology maturity – Organizations getting better about understanding business alignment rather than just tool use.

Hewlett Packard Enterprise

Read the full report at
hpe.com/software/StateOfSecOps

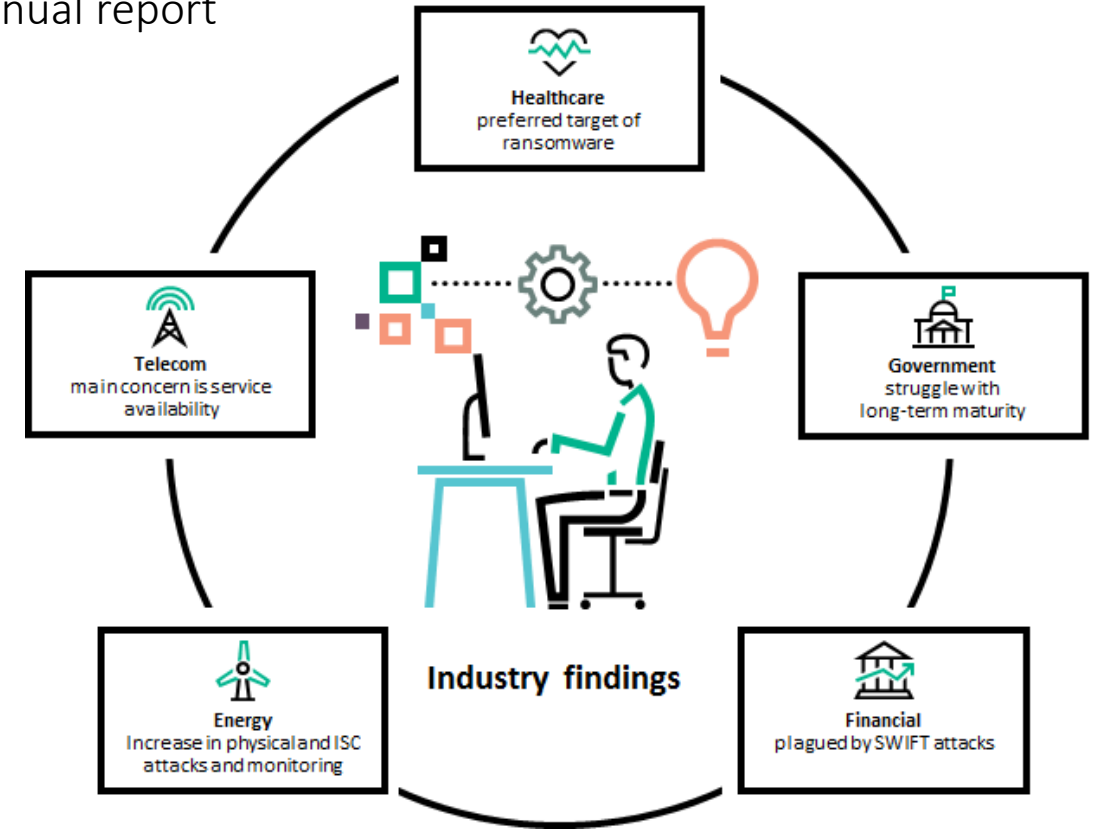
Median SOMM Score by Industry



Hewlett Packard Enterprise

2017 State of Security Operations

4th annual report



Hewlett Packard Enterprise

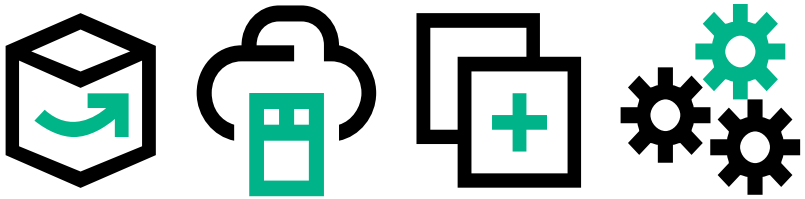
Read the full report at
hpe.com/software/StateOfSecOps

#1: Automation and Elimination of entry level analysts

Full automation is not realistic. Advanced threats require human investigation.

Hewlett Packard Enterprise

#2: Attempts to transfer risk with managed services



Organizations have experienced varied success with Managed Service based on their approach.

Hewlett Packard Enterprise

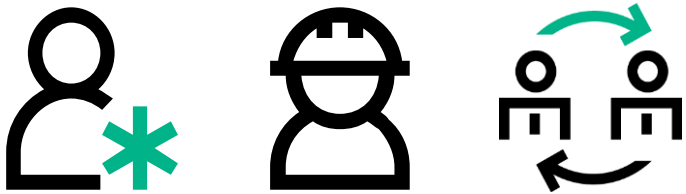
#3: Decreased maturity with hunt-only programs

Success is had when hunt is additive to stable real-time detection and response. Immaturity comes from hunt and search non-repeatable approaches.

Hewlett Packard
Enterprise

#4: Increased Capabilities via hybrid solutions

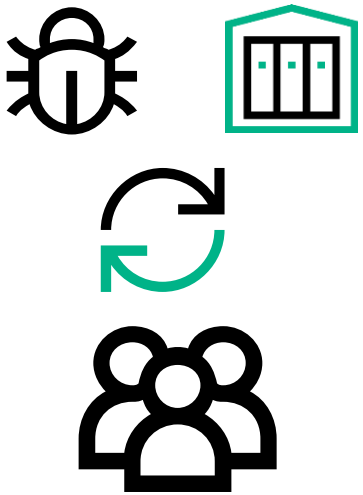
Keeping risk management in-house but scaling with external resources has improved maturity in some organizations



Hewlett Packard Enterprise

#5: Public Sector SOC struggles

The public sector struggles with mass outsourcing and high rates of turnover.



Hewlett Packard Enterprise

#6: No link between Organization Size and Maturity

Maturity is tied more closely to goals of security organization and not it's size.

"The use of security as competitive differentiator, market leadership and industry alignment = predictors of maturity."

Hewlett Packard Enterprise

Key Takeaways

Various approaches with wildly varying results

27% not providing minimum security monitoring capabilities

82% not achieving recommended maturity levels

https://www.hpe.com/software/StateOfSecOps

kerry.matre@hpe.com

Hewlett Packard Enterprise

Post Discover Summit 2017

Join HPE and Vivit for a Post Discover Summit 2017

Nine Webinars in 3 days focusing on ADM/ITOM

http://www.vivit-worldwide.org/default.asp?page=LondonSummit2017

vivit

Thank You

- Complete the short survey and opt-in for more information from Hewlett Packard Enterprise.

www.hpe.com/software

www.vivit-worldwide.org

Hewlett Packard
Enterprise

YOUR INDEPENDENT HPE SOFTWARE USER COMMUNITY

vivit

vivit

Thank You

vivit-worldwide.org