RSAConference2018
San Francisco | April 16–20 | Moscone Center

SESSION ID: SPO2-W14

GOING BEYOND DEFENSE: HOW SECURITY BECOMES A BUSINESS ENABLER

Monzy Merza

VP, Head of Security Research
Splunk
@monzymerza

Agenda

- The **Adaptive** Security Mindset
- **Responding** to business NOT just threats
- **Transparency** in Security operations
- Industry examples: Security Enabling the business

Security operations self-image as guardians

Stop bad things from happening

"Users are either dumb or victims"

The business doesn't get it

"We have a thankless job - but we serve"

We need more resources

FUNDAMENTAL FLAW OF ‘PREVENT DEFENSE’

“The **prevent defense** is a **defensive** alignment in American football that seeks to **prevent** the offense from completing a long pass or scoring a touchdown in a single play and seeks to run out the clock.”

Line of business sees security operations

"We don't know what we get for money spent"

Always causing slow downs

Out of touch with business

PRIMARY FUNCTION OF SECURITY IS TO MAINTAIN ACCEPTABLE RISK POSTURE

Security teams need to engage the business

- Don’t wait, be active – seek out IT projects to participate in
- Look for new horizons - follow industry IT trends
- Learn/train – how would secops help the business in a new terrain
- Compliance is NOT your enemy – use it as a lever

A R T OF ENABLING THE BUSINESS

A IS FOR ADAPTIVE MINDSET

The Adaptive Mindset – Adversary has to come to you

Security operation is NOT a passive activity

Build for business

Focus on the people

Security operation is NOT a passive activity

- Understand the current IT environment
- Business objectives and roadmap
- Identify opportunities for engagement

Build for business

- Security processes to serve the business
- Rooted in an anchoring principle for security
- Technology and integrations for adaptation

Focus on the people

- Processes and communication internally and externally
- Be proactive. Communicate and collaborate
- Enable personnel to make decisions

Build to Respond to Business - Anticipate

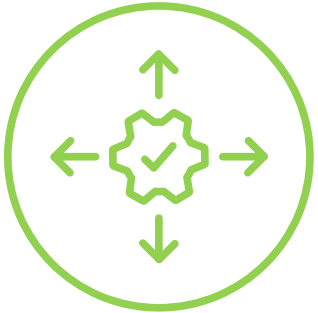
- Once you know the business roadmap/initiatives
- What new security processes may be required?
- What new personas will you interact with?
- Will there be new applications, services, terrains (e.g. cloud)
- Identify risks and changes to acceptable risks

R IS FOR RESPOND TO BUSINESS

R

Build to Respond to Business - Collaborate

- Reach out to IT, Line of business
- Verify your anticipations/assumptions
- Take on action items for the project
- Share the security requirements
- Highlight the risks and changes to acceptable risks



Build to Respond to Business - Prepare

- Create security sub-team to focus on business initiative
- Focus on the identified, agreed upon risks
- Develop proof of concept – processes, tech integration, examples
- Identify new skills required for security staff
- Empower staff to tinker in the new domain
- Participate regularly with line of business – report, feedback, adjust

Maintaining Acceptable Risk – Reduce Time 2

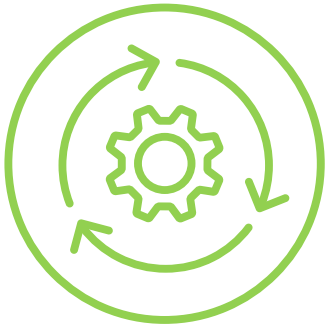
- Detect, Respond, Mitigate threats
- Report to management and compliance
- Collaborate with IT and line of business
- Implement learning into processes

Reducing Time – Focus on Decision

- Platform to bring people and technology together
- Integrations focused on faster decision making
- Capability to collaborate and share

Reducing Time – Automation

- Contextualize Alerts
  - Assets and identities
  - Auto investigate
- Preserve Evidence
  - Snapshot, Log/packet un-rotate
  - Create tickets, activate reporting clock
- Execute Config Changes
  - Reduce/enhance privileges
  - Update instrumentation, patch endpoints



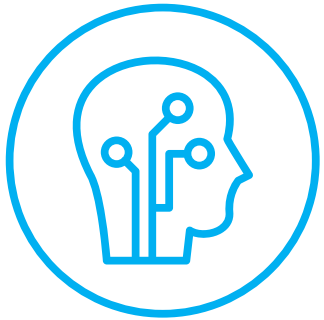
Managing the fear of automation

- **Auditability**
  - Who (person or system) took the action
  - When (was the action taken)
  - What was the result of the action
- **Reversibility**
  - Is there an *undo* action?
  - Is *undo* just as fast as the automation?
- **Transparency**
  - What is the logic behind the action?
  - Can the logic be modified?

T IS FOR TRANSPARENCY

Communicate your understanding

- In your mind, what does the business care about
- How are you addressing those risks
- What are your processes
- What are your expectations from the business



Share, Share

- Make it easy for others to see your work
- Send out weekly summaries
- Have a dashboard on progress towards new initiatives
- Invite non-security personnel to brown bags
- Share successes and failures

Celebrate successes

- Security is not alone
- Find reasons to celebrate with the team
- Celebrate with other teams, IT, line of business

When you get home – here's what you do

- **Adaptive**: Identify a business initiative
- **Respond**: Commit one deliverable for participating in the initiative
- **Transparent**: Communicate the priority and participation to security team and your leadership team

All together – ART of enabling the business

- **A**: Adaptive mindset
- **R**: Build to Respond
- **T**: Be transparent, collaborate, engage

Thank you!

#RSAC

The A R T of Enabling the Business

@monzymerza

monzy@splunk.com