Intrusion Detection Systems & Liability

NetDiligence®

HB LITIGATION CONFERENCES

Speakers

Andrew Obuchowski, *moderator*, *RSM*

Andy Schworer, *Crowdstrike*

Jason Rebholz, *Crypsis*

Bill Lysaught, *SecureWorks*

Brian Klenke, *Morphick*
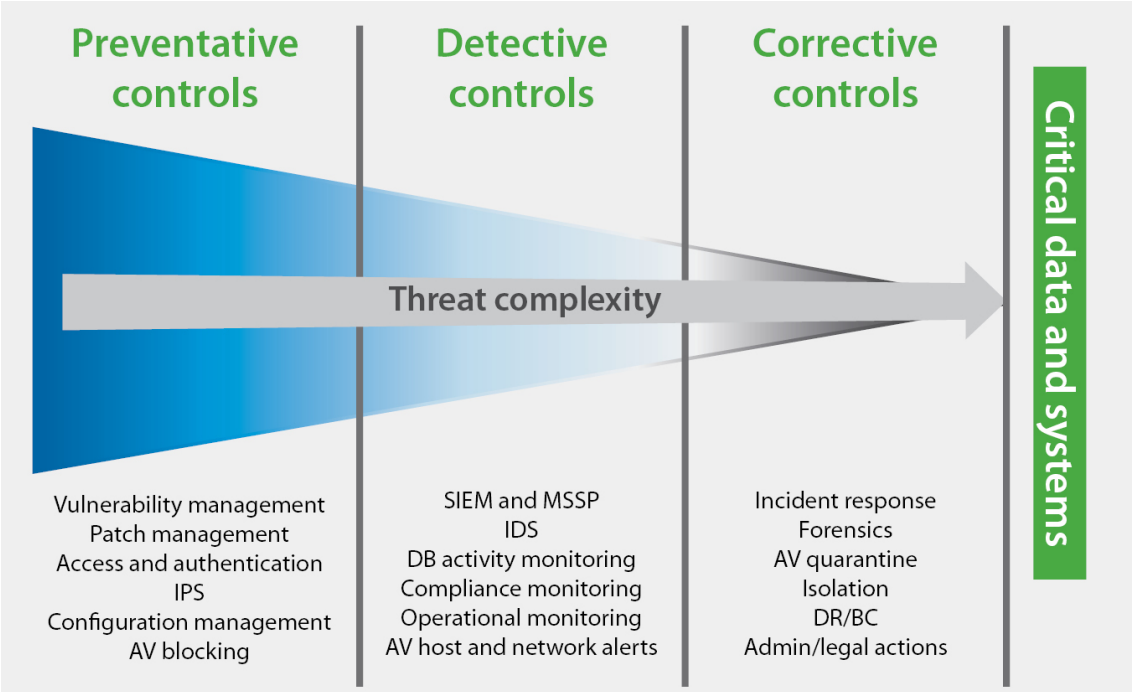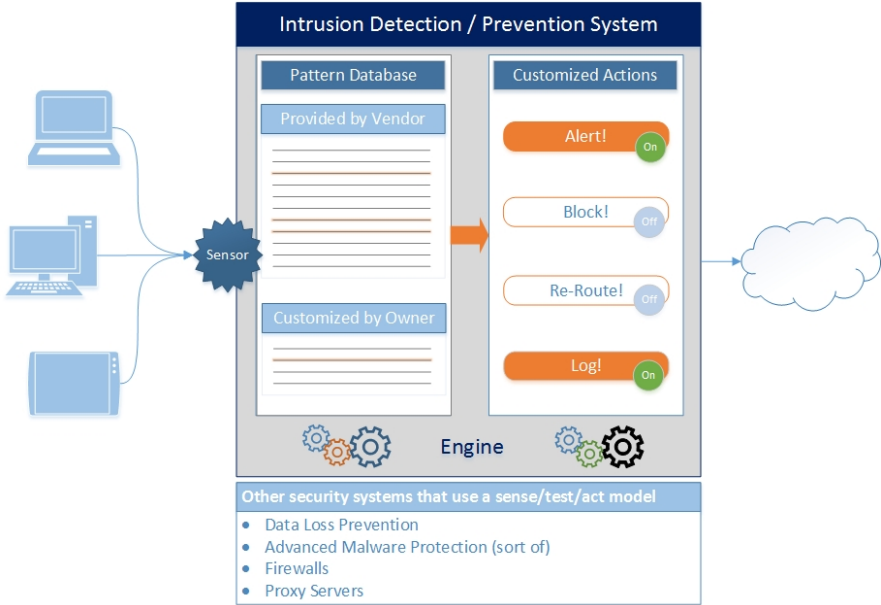
Chris Cronin, *Halock Security Labs*

Session Topics

- Introduction to Intrusion Detection Systems (IDS)

- Reasons many organizations FAIL to detect security incidents

- Benefits and ongoing challenges of IDS

- Determining Client's Capabilities – Handling Issues v. Check Box Approach
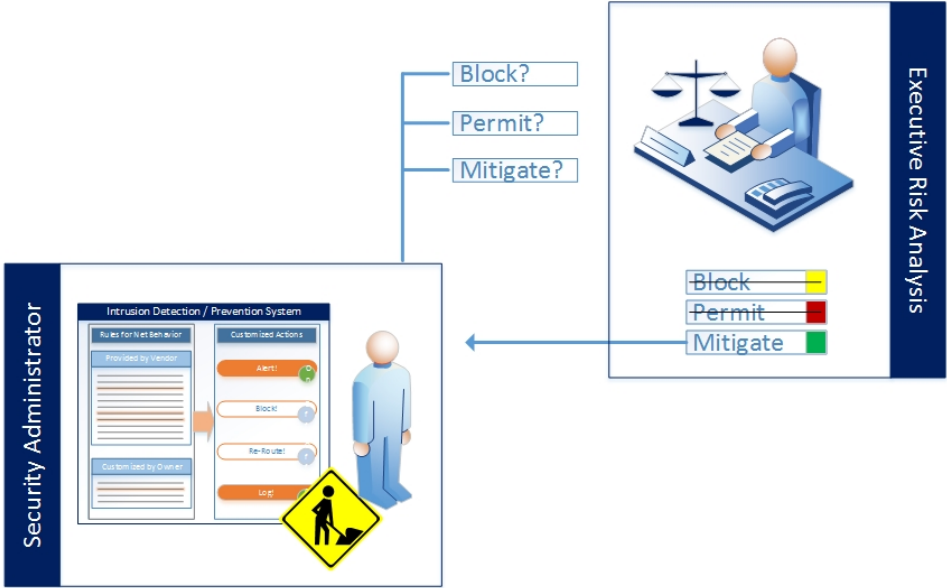
Introduction to IDS

Preventative controls	Detective controls	Corrective controls	
Vulnerability management	SIEM and MSSP	Incident response	
Patch management	IDS	Forensics	
Access and authentication	DB activity monitoring	AV quarantine	
IPS	Compliance monitoring	Isolation	
Configuration management	Operational monitoring	DR/BC	
AV blocking	AV host and network alerts	Admin/legal actions	

Threat complexity

Critical data and systems

Introduction to IDS

Introduction to IDS
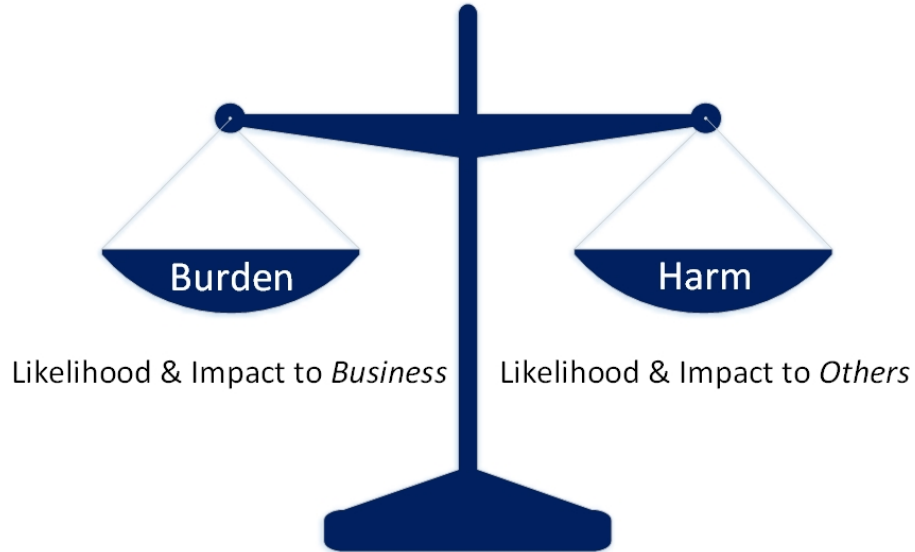
Pre-Incident Considerations

- Known v. Unknown Threats

- Implementation

- Human Element v. Automated

- Governance & Compliance

Ongoing Incident Considerations

- Responding to the Incident
  - Incident Triage
  - Validation
  - Scope of Incident
  - Containment/Isolation
    - Adjustments
  - Remediation

Post-Incident Considerations

Duty of Care Risk Analysis

Burden — Harm

Likelihood & Impact to *Business* — Likelihood & Impact to *Others*

Post-Incident Considerations

- Lessons Learned
  - IDS Implementation
  - Training/Awareness
  - Policies/Procedure Review

- Intelligence Obtained
  - What could we have done differently up front?
  - Utilize new intelligence to reduce future risk

Speakers

Andrew Obuchowski, *moderator*, *RSM*

Andy Schworer, *Crowdstrike*

Jason Rebholz, *Crypsis*

Bill Lysaught, *SecureWorks*

Brian Klenke, *Morphick*

Chris Cronin, *Halock Security Labs*