RSAConference2015
San Francisco | April 20-24 | Moscone Center

SESSION ID: CRWD-01

Active Response: Automated Risk Reduction or Manual Action?

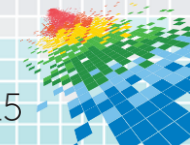
sec ops | dream

Monzy Merza

Chief Security Evangelist
Splunk
@monzymerza

Agenda

- Active Response Drivers
- Facets of Active Response
- Balancing Business Risk and Active Response
- Required Capabilities



Sources of Cyber Risk

Cyber Criminals

Malicious Insiders

Nation States

Active Response Drivers

- Constant, Simultaneous Attacks
- Triaging and False Positives
- Time to Response
- Human Resource Constraints

HUMAN TIME RESPONSE IS UNTENABLE

Human-Enabling Active Reponse

Risk Based

Connecting Data and People

Context & Intelligence

Facets of Active Response

- Transparency and human enablement is core to risk based active response

Conventional Active Response

- Block and tackle
  - Config changes on endpoints, network or gateways
  - Policy changes on access/auth or business systems
- Attach back
  - Fire packets at the attack source
  - Interact via CnC or payload

Conventional Active Response

Challenges

- Complex business and mission requirements
- Distributed and diverse infrastructure
- Repercussions

Advantages

- Block-and-tackle cause and effect is well understood
- Action is decisive
- Attack back is human mediated

Facets of Active Response – Risk Based

- Context through post-processing
  - Enrichment of event data – asset, identity, access lookup
  - Tiered analysis – submit malware to a sanbox
- Signaling and messaging
  - Expert system communication – start packet capture
  - Summarization – forward summary data to ticketing system
- Evidence preservation
  - Disk forensic snapshot
  - Move event data out of rotation repository

Risk-Based Active Response

Challenges

- Technology managed by different teams
- Integration challenges – lack of open APIs
- No central broker or nerve center

Advantages

- Low business risk in case of errors
- Analyst has deeper context and knowledge
- Not making any configuration changes

AND NOW FOR SOMETHING CONTROVERSIAL…

…LOW OR HIGH CONFIDENCE → AS IT RELATES TO BUSINESS RISK

Confidence Drives Depth of Decision

- What is the business risk?
- How complete is the threat context?
- What/who will be impacted by change?
- How hard is it to revert the change?
- Who has the Get Out of Jail Free Card?

Natural Remedy for Active Response

- Focus on business risk and mission
- Let the machines be machines
- Enable the human to be human

BALANCING BUSINESS RISK AND ACTIVE RESPONSE

Who Does What

Machine

- Correlate
- Auto-collect
- Message, signal
- Execute action

Human

- Contextualize
- Prioritize
- Mediate action
- Apply gut feel

Production Active Response Actions

High Confidence

- Alert on correlations
- Block on IP or domain
- Modify configs
- Report on actions taken

Low Confidence

- Alert on correlations
- Contextualize alerts
- Gather more data for alert artifacts
- Kick off secondary analysis
- Prepare for human

Examples of Confidence

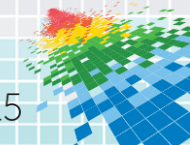
High Confidence

- Threat feed matches from ISAC or internal sources
- Trigger from inline dynamic analysis engine
- Correlation alert for beaconing activity

Low Confidence

- Threat feed match from a free intel feel
- Correlation alert from a statistical engine
- Individual signature match from IDS/IPS

THE MACHINE CAPABILITY



Key Technical Capabilities

- Security instrumentation
- Aggregation, correlation, alert
- Integration across the instrumentation
- A nerve center – orchestration, messaging
- Tracking of all actions and messages

Security Instrumentation

Network

Endpoint

Threat Intelligence

Authentication

splunk>

Security Instrumentation – Core Capabilities

Threat intelligence

- Third-party threat intel
- Open source blacklist
- Internal threat intelligence

Reputation services, known relay/C2 sites, infected sites, IOC, attack/campaign intent and attribution

Network

- Firewall, IDS, IPS
- DNS
- Email
- Web proxy
- NetFlow
- Network

Who talked to whom, traffic, malware download/delivery, C2, exfiltration, lateral movement

Endpoint

- AV/IPS/FW
- Malware detection
- Endpoint forensics
- Config mgmt
- OS logs
- File system

Running process, services, process owner, registry mods, file system changes, patching level, network connections by process/service

Access/Identity

- Directory services
- Asset mgmt
- Authentication logs
- Application Services
- VPN, SSO

Access level, privileged use/escalation, system ownership, user/system/service business criticality

Building Confidence for Active Response

Persist, Repeat

Threat intelligence

- Third-party threat intel
- Open-source blacklist
- Internal threat intelligence

Update threat lists. Enrich threat list info with new knowledge.

Network

- Firewall, IDS, IPS
- DNS
- Email
- Web proxy
- NetFlow
- Network

Add to custom policy groups: vlans, watch list, bad actors, policy groups. Start/stop packet capture.

Endpoint

- AV/IPS/FW
- Malware detection
- Endpoint forensics
- Config mgmt
- OS logs
- File system

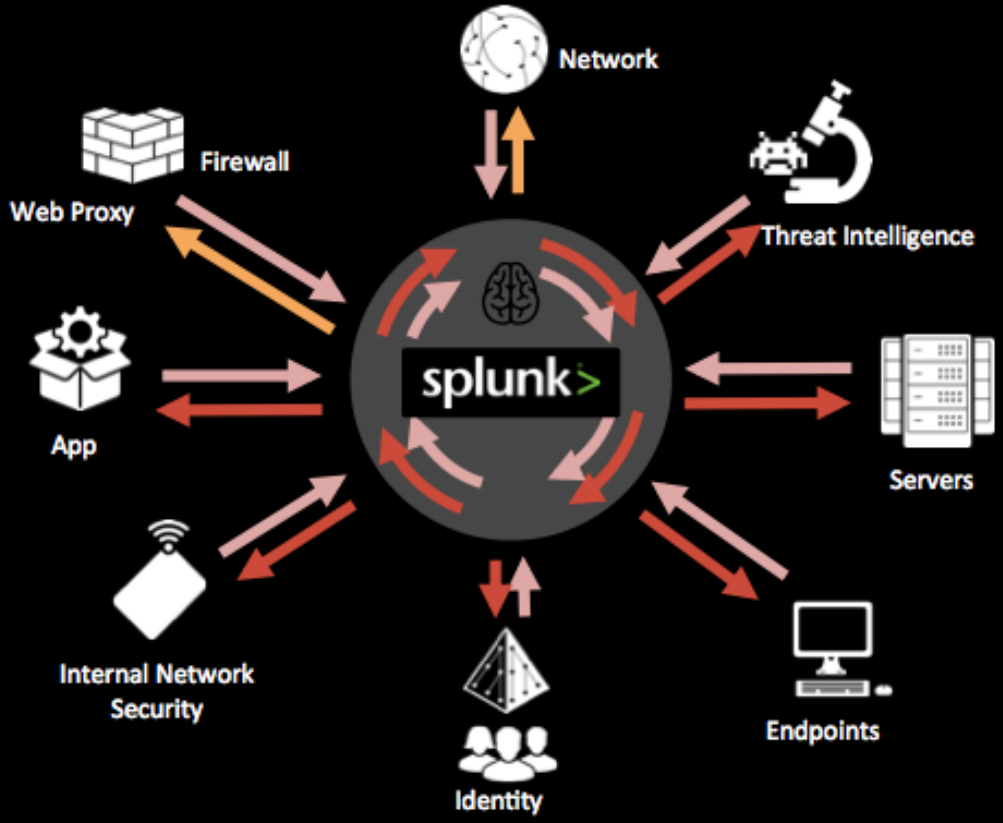
Acquire config info, invoke snapshots, submit files to sandbox, update local signatures, clean up infected files, start/stop processes and services.

Access/Identity

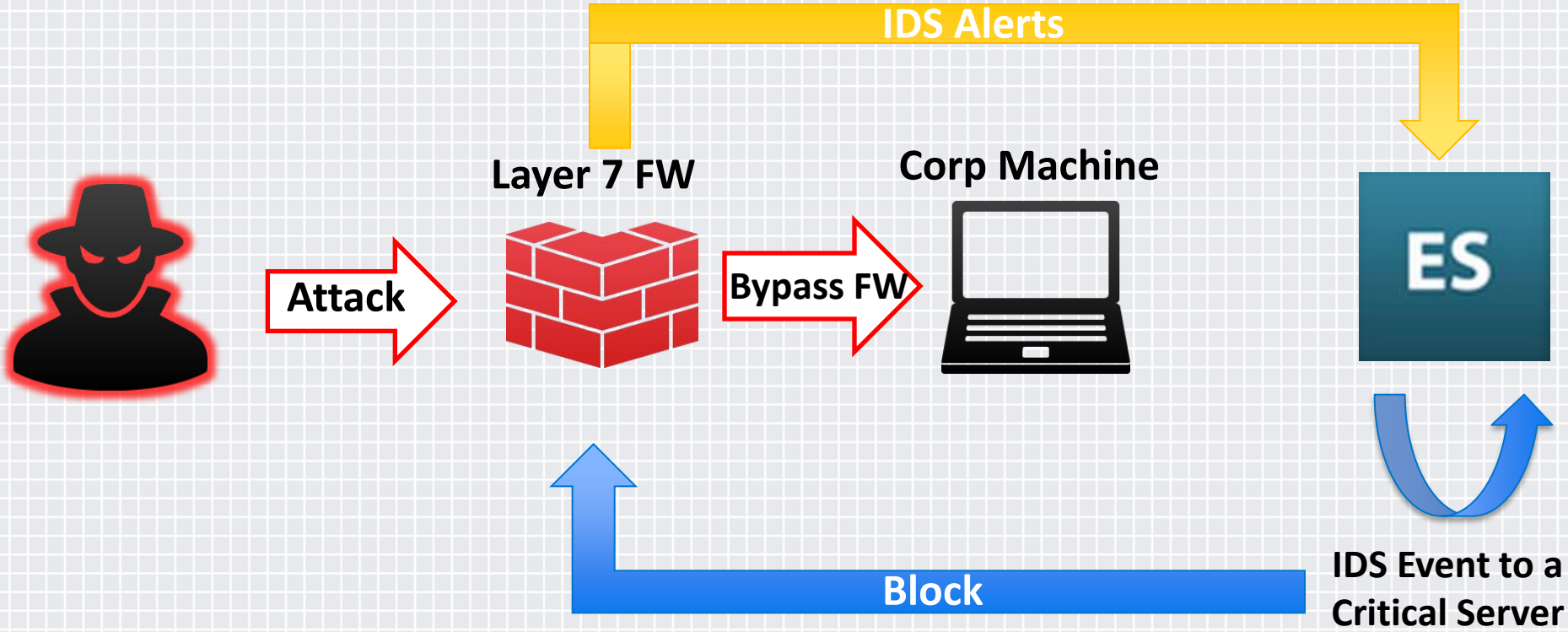
- Directory services
- Asset mgmt
- Authentication logs
- Application Services
- VPN, SSO

Acquire business info, groups, travel, organizational priority. Modify membership, revoke tokens or certs.

Nerve Center



High Confidence Policy Change



Low Confidence Aggregation

- Dynamic analysis alert
- Did it detonate on the endpoint?
  - Check for endpoint logs
  - Check for AV logs
- Take a snapshot – proc list, netstat
- Start packet capture
- Disk forensic snapshot

Active Response Is Survival

- Attack volume is high
- Human time response is not tenable
- Active response enables the human analyst
- Active response != cutting people's Internets

Thank You

- Questions?
- More discussions: monzy@splunk.com