OFFICE OF INFORMATION SECURITY
Always alert, always ready to help.

Applied Security Operations at Penn

SAM JENKINS

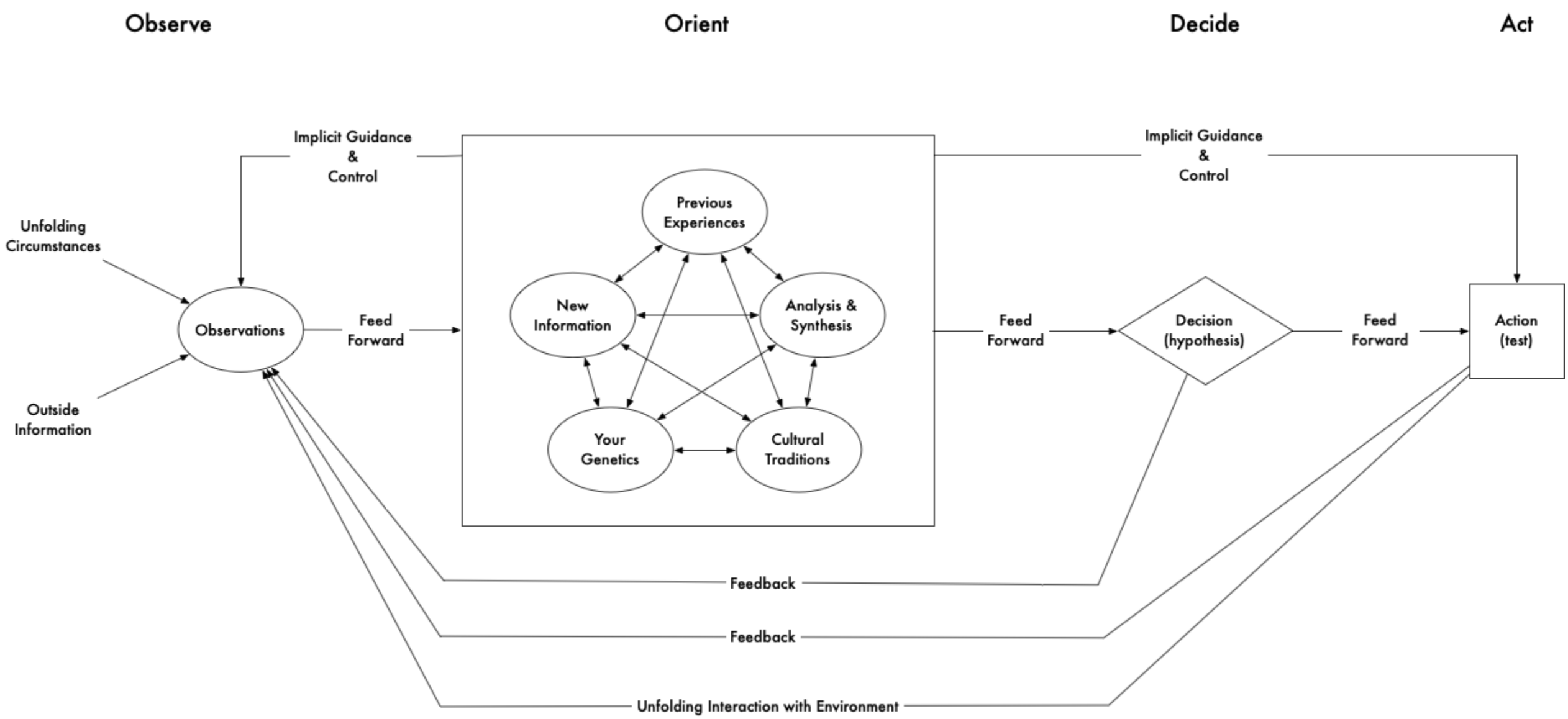
SR IT SECURITY ENGINEER

ISC OFFICE OF INFORMATION SECURITY

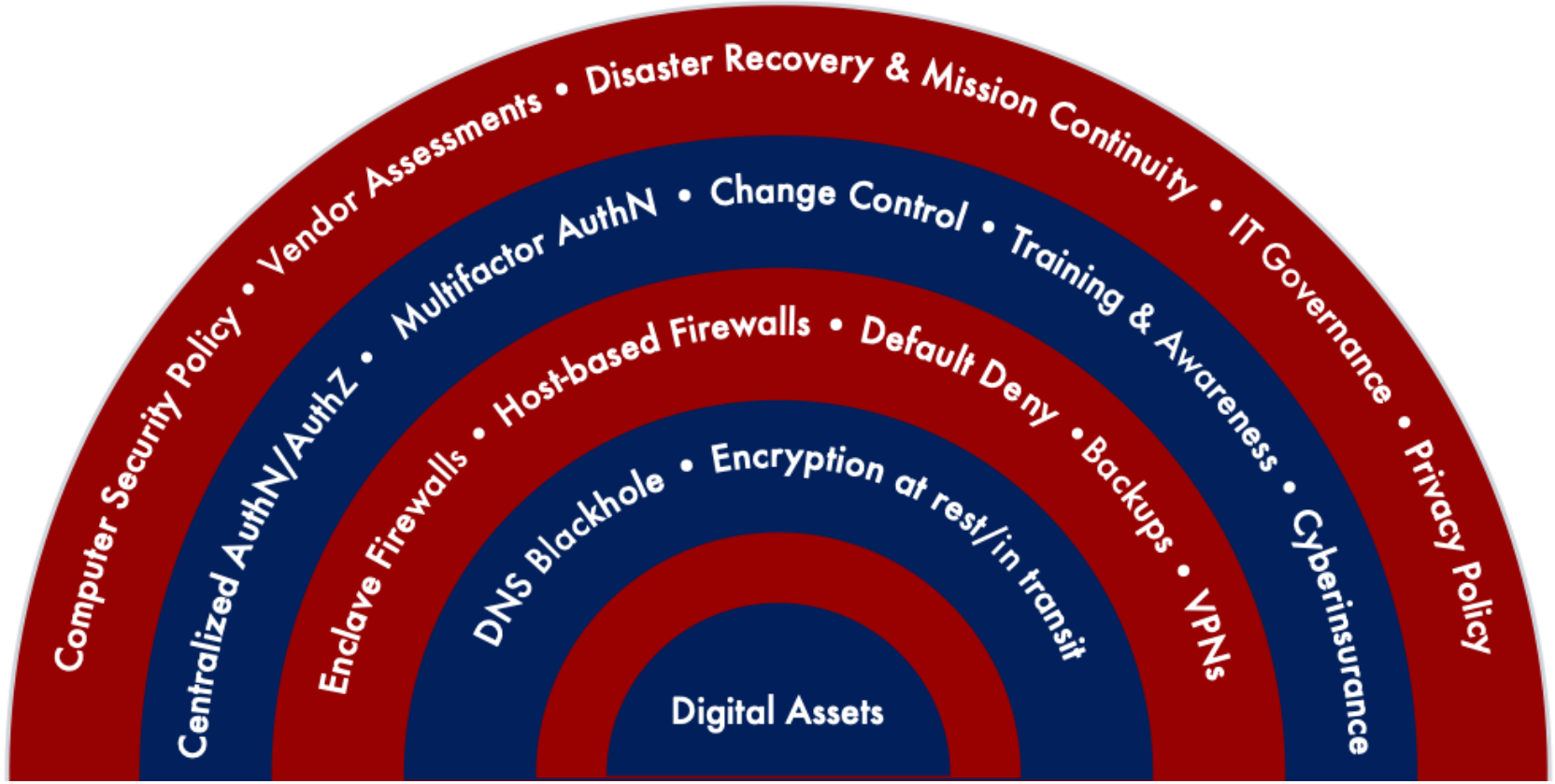
Penn is Not Normal

- *Decentralization!*
  - 12 schools, 36 administrative centers
  - About 2000 departments
  - 5 campuses
  - 60,000 active users
  - We had Tor exit nodes!
- ***Security*** is even decentralized
  - Office of Information Security
  - Information Security Officers in the Schools/Centers
  - System security is a responsibility of system owners
- Secure IT is IT done well

Security operations is about workflows, not tools

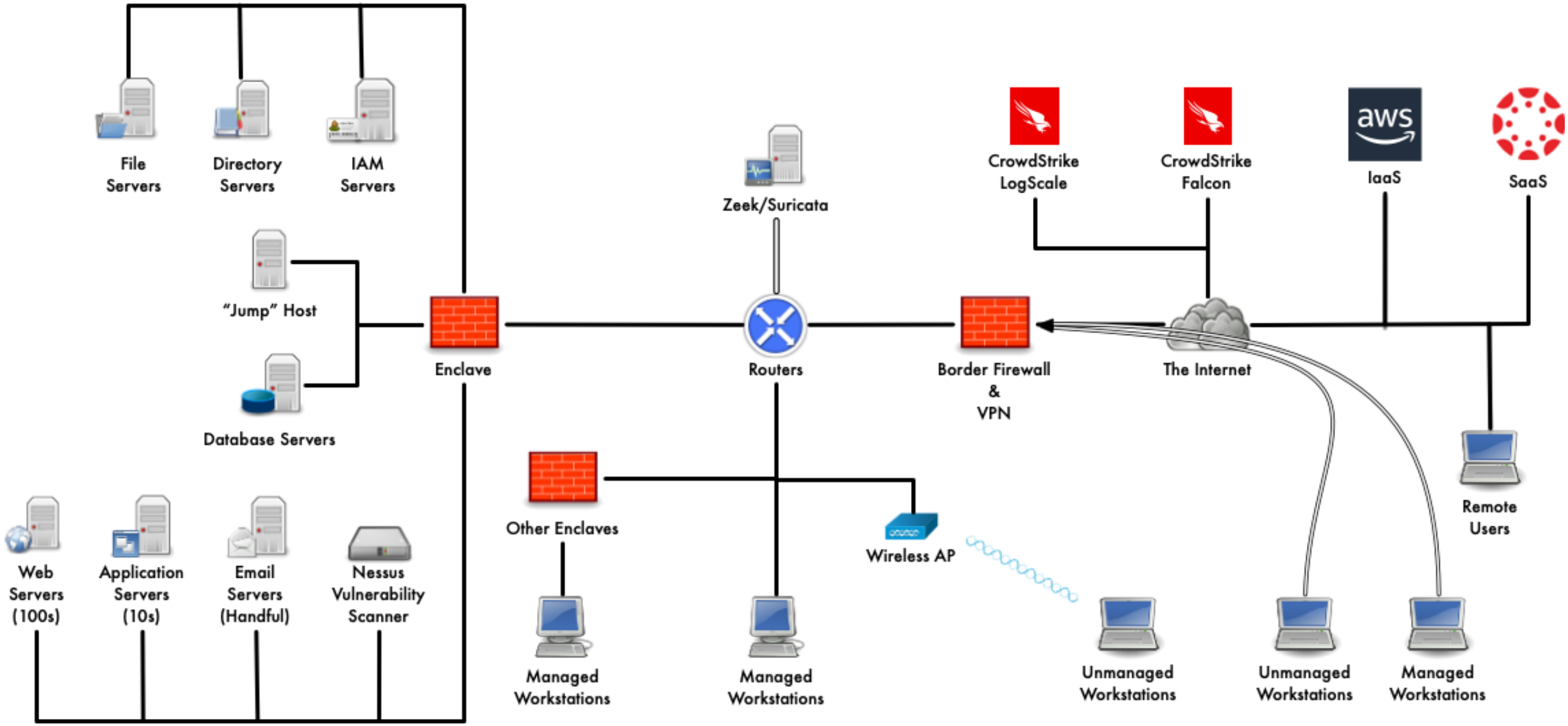

Observe
Orient
Decide
Act
Implicit Guidance & Control
Unfolding Circumstances
Observations
Feed Forward
Outside Information
Previous Experiences
New Information
Analysis & Synthesis
Your Genetics
Cultural Traditions
Implicit Guidance & Control
Feed Forward
Decision (hypothesis)
Feed Forward
Action (test)
Feedback
Feedback
Unfolding Interaction with Environment

Penn does a lot…



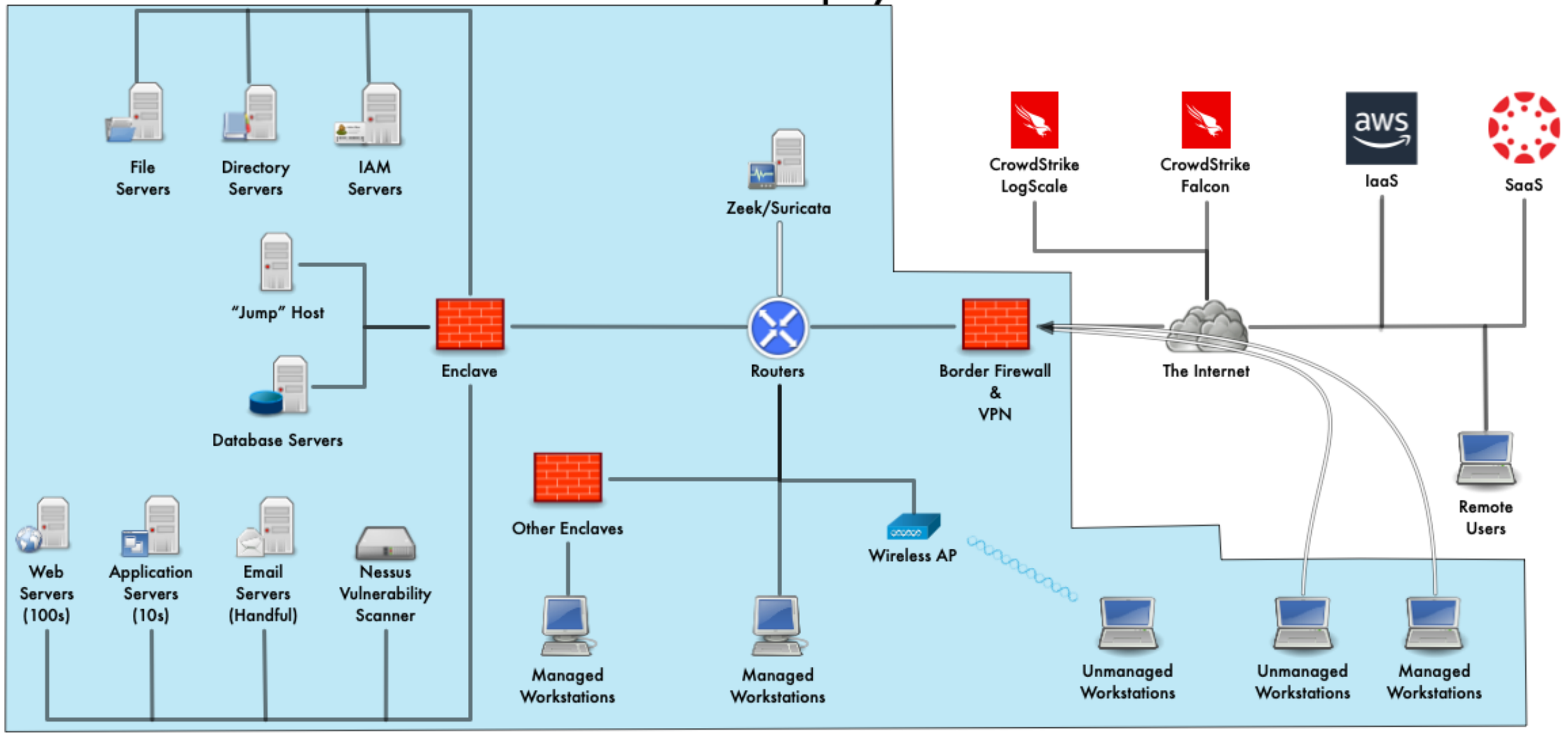
Asset Inventory

Reference Deployment

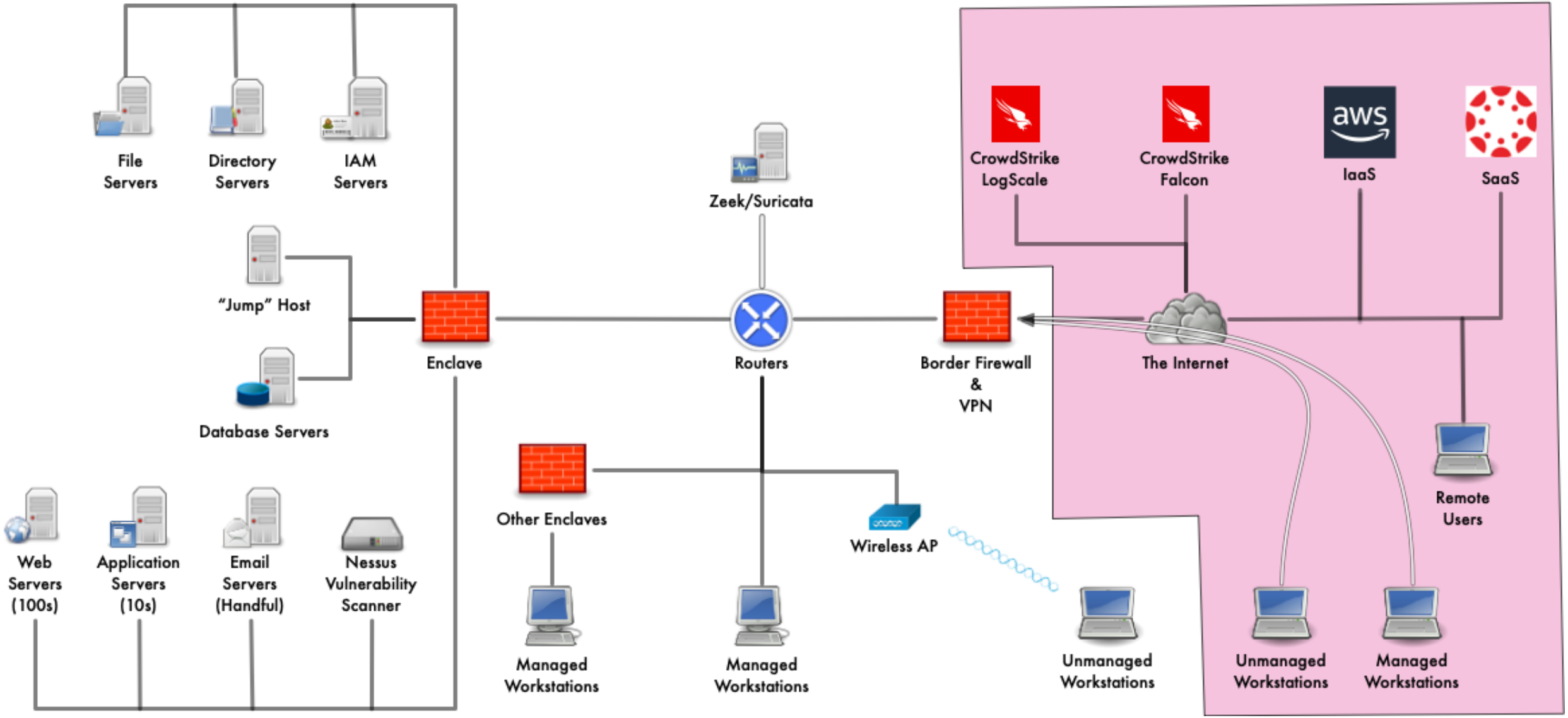



Endpoints
on Your
Network
VPN Users
(students, contractors)
Endpoints
off of Your
Network
Personal
Devices
VPN Users
(employees)
Workstations
Servers
Applications
Appliances
SaaS
IaaS
Remote Users
Endpoints
You Own

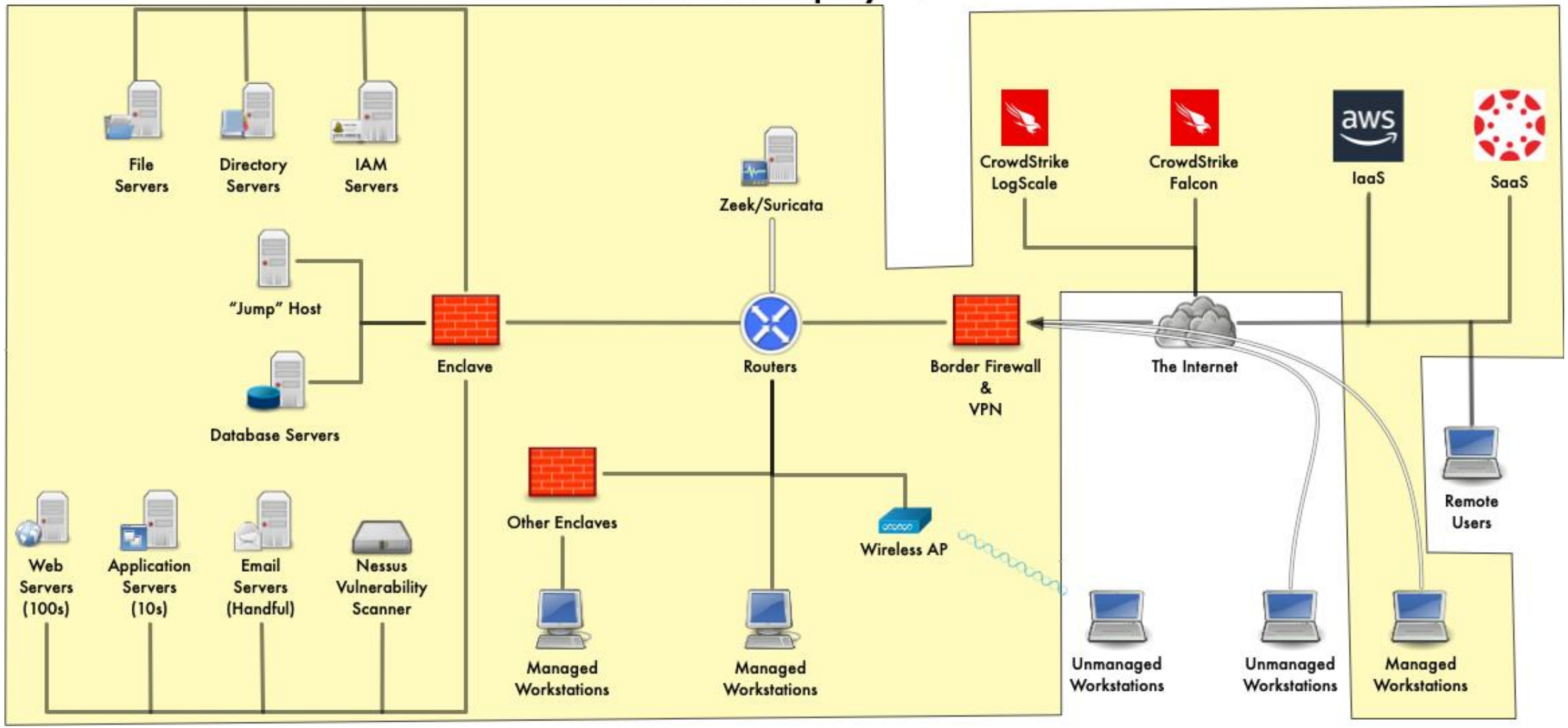
Reference Deployment



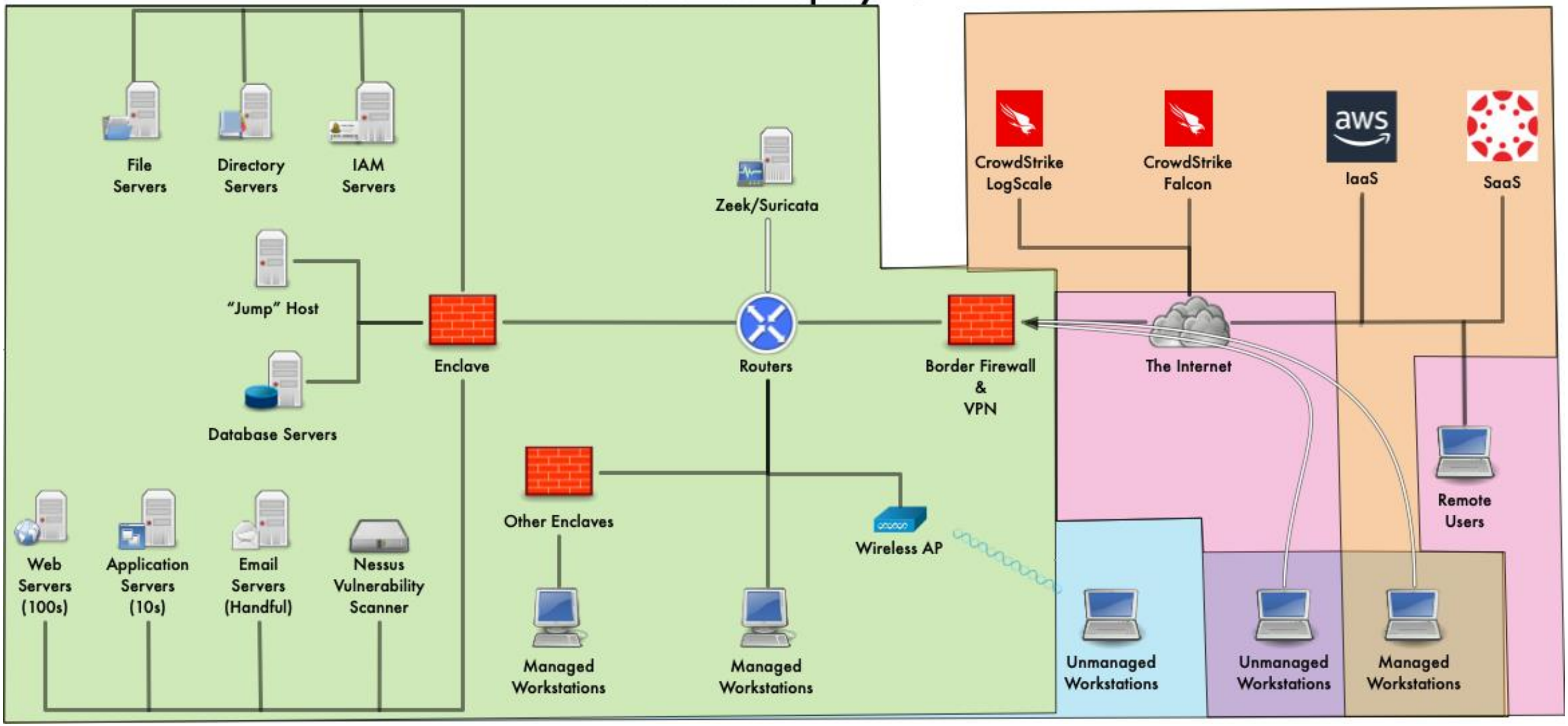
Reference Deployment



Reference Deployment



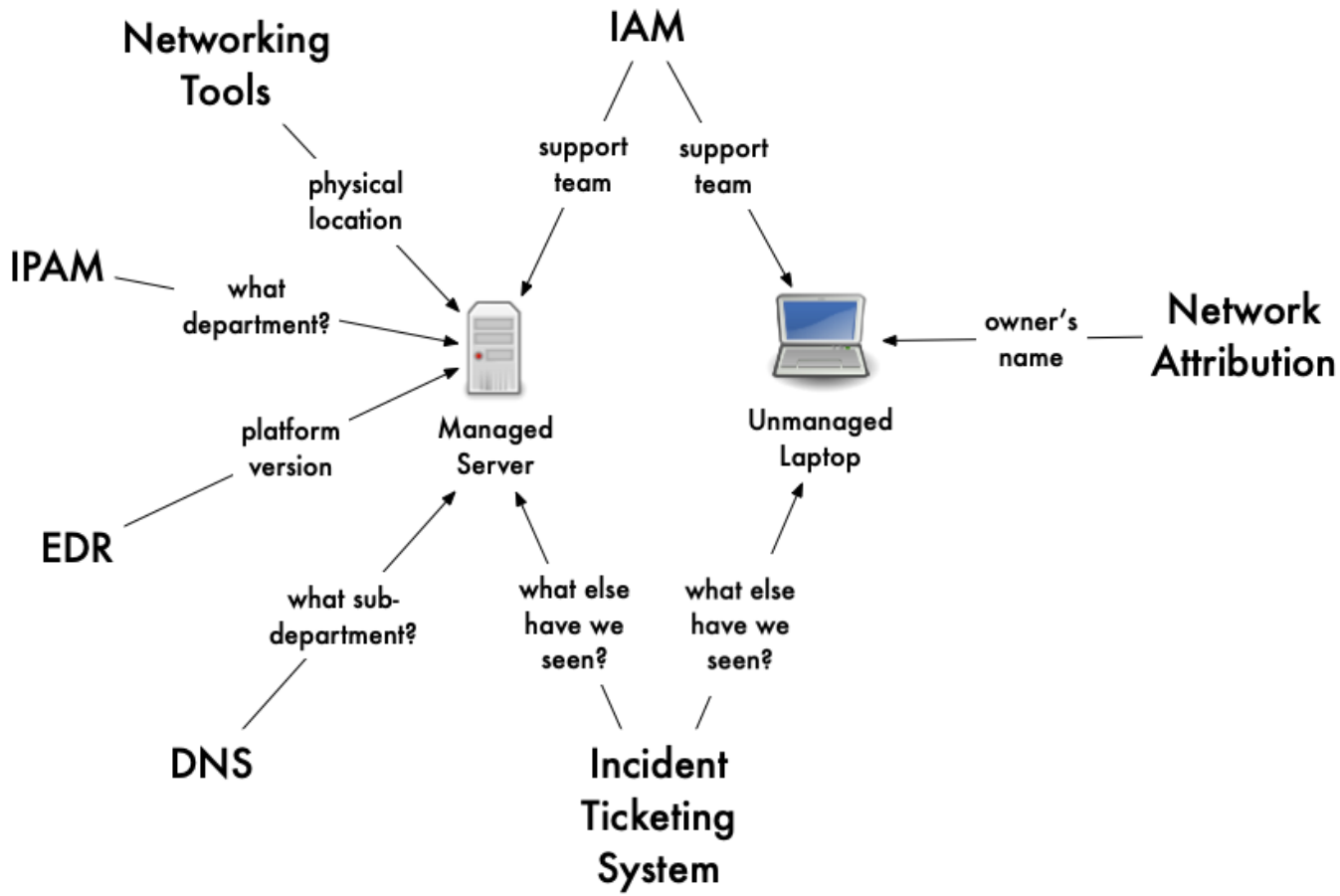
Reference Deployment



Inventories: three approaches

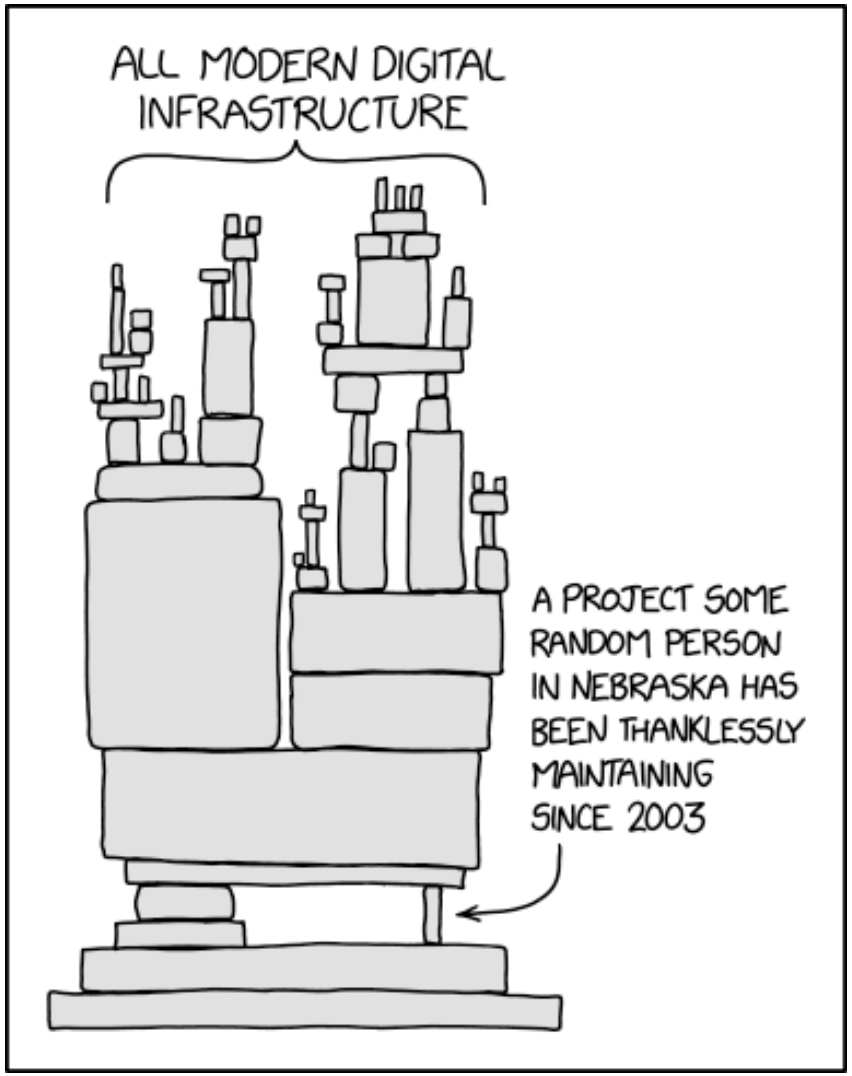
- Data-oriented:
  - Data Risk Classification
  - Annual inventory of data (Security & Privacy Impact Assessment, aka SPIA) by schools & centers
- Criticality-oriented:
  - System owners register hosts and applications in central repository (Critical Components)
- Operations-oriented:
  - IP Address Management (IPAM) captures metadata on IP addresses and domain names
- Continuous improvement
  - As you deploy/discover/delete datasets, update SPIA
  - As you deploy/discover/decommission assets, update Critical Components.
  - Results of threat hunting, penetration testing, and audits.
  - Risk Cloud starting to replace Critical Components and SPIA in FY27.

Source Systems as “Inventories”



Asset Inventory Challenges

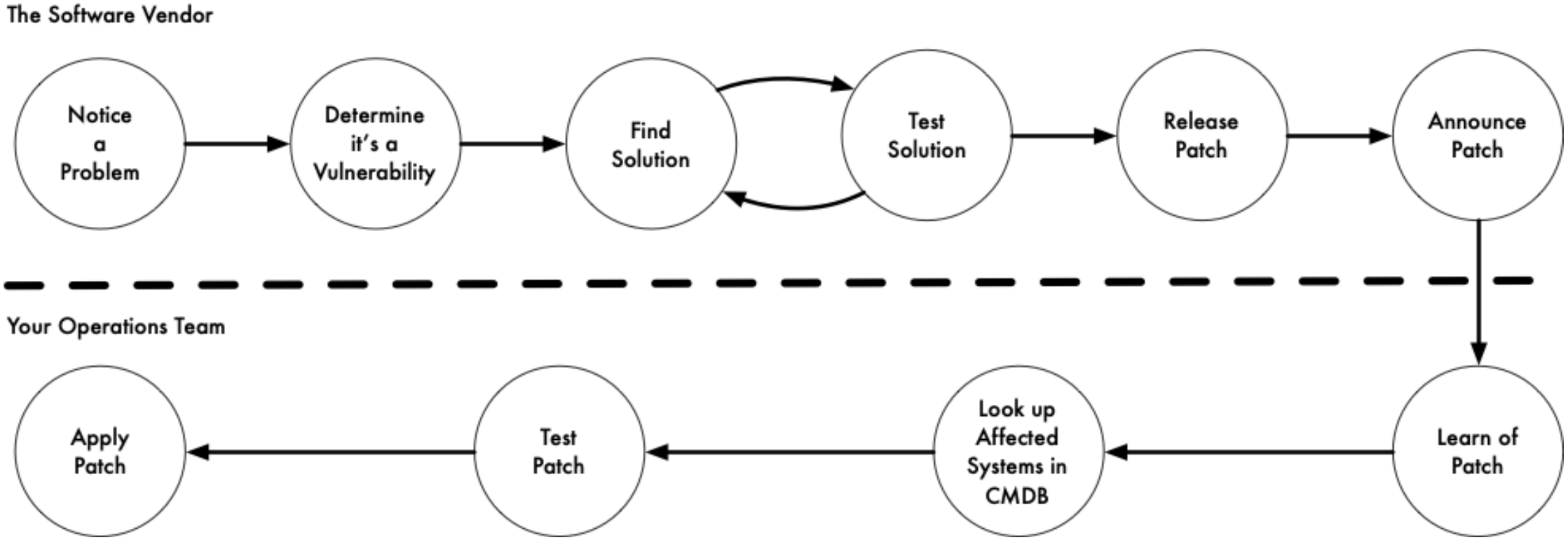
- Multiple departments
  - Different naming conventions
    - Different patch cycles
      - Different kinds of devices (workstations, servers, appliances, IaaS, SaaS, OT, etc.)
        - Different deployment tools
- Ephemerrality:
  - Of presence (Local today, remote tomorrow; on/off; crashed?)
  - Of identity



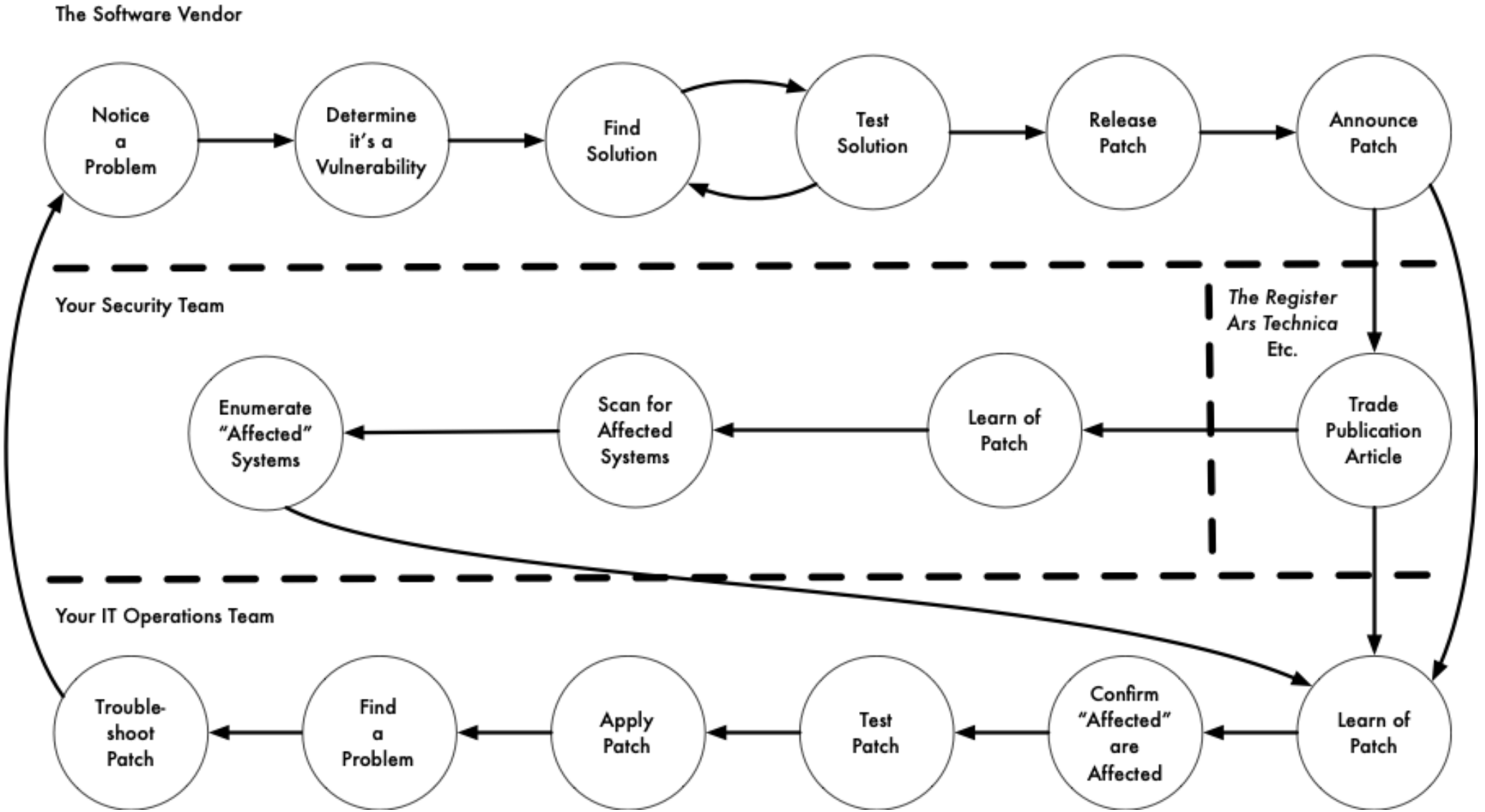
https://xkcd.com/2347/

Vulnerability Management

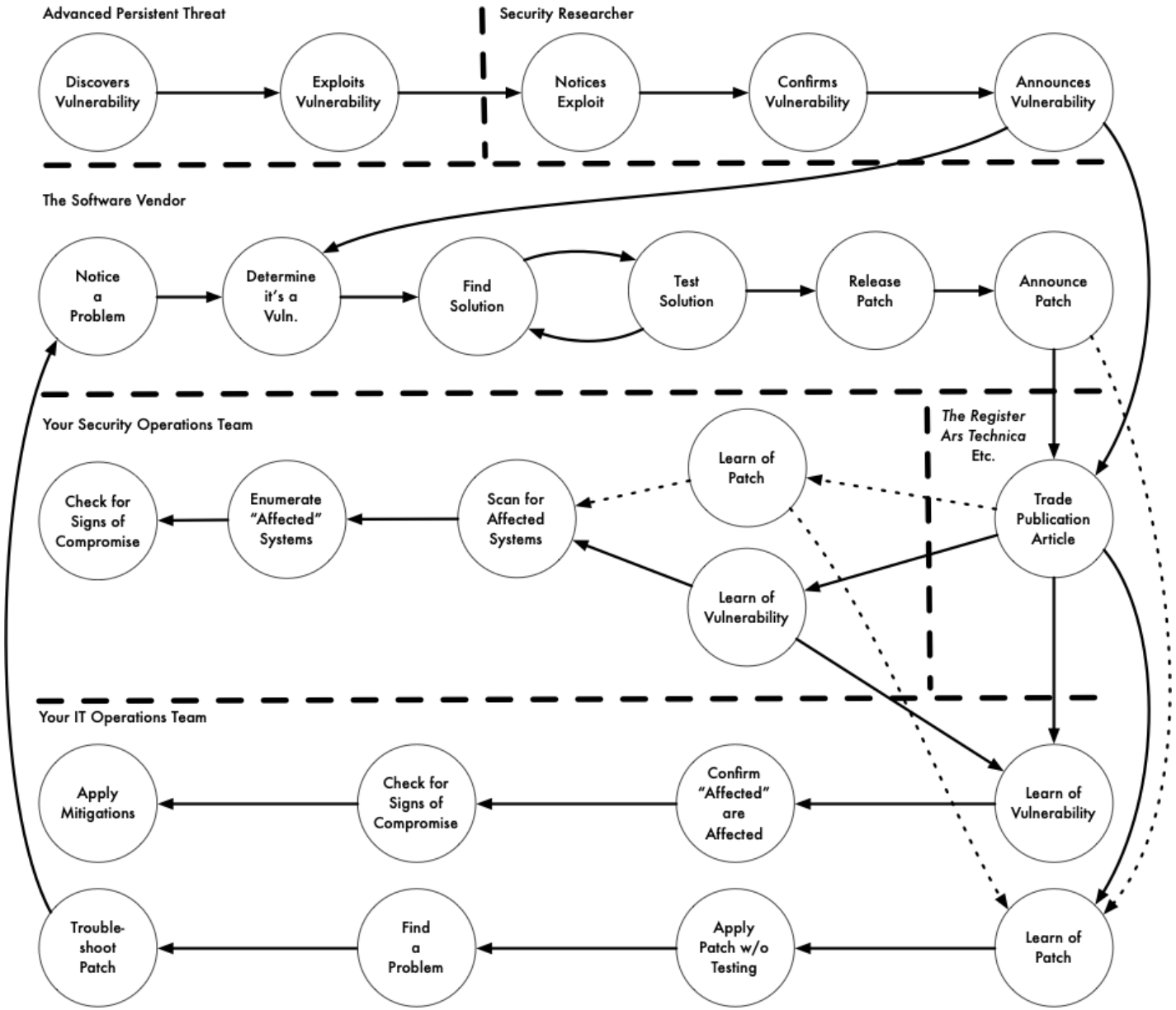
Platonic Ideal of the Patching Cycle



The Critical Vulnerability Patching Cycle



Zero-Day Patching Cycle

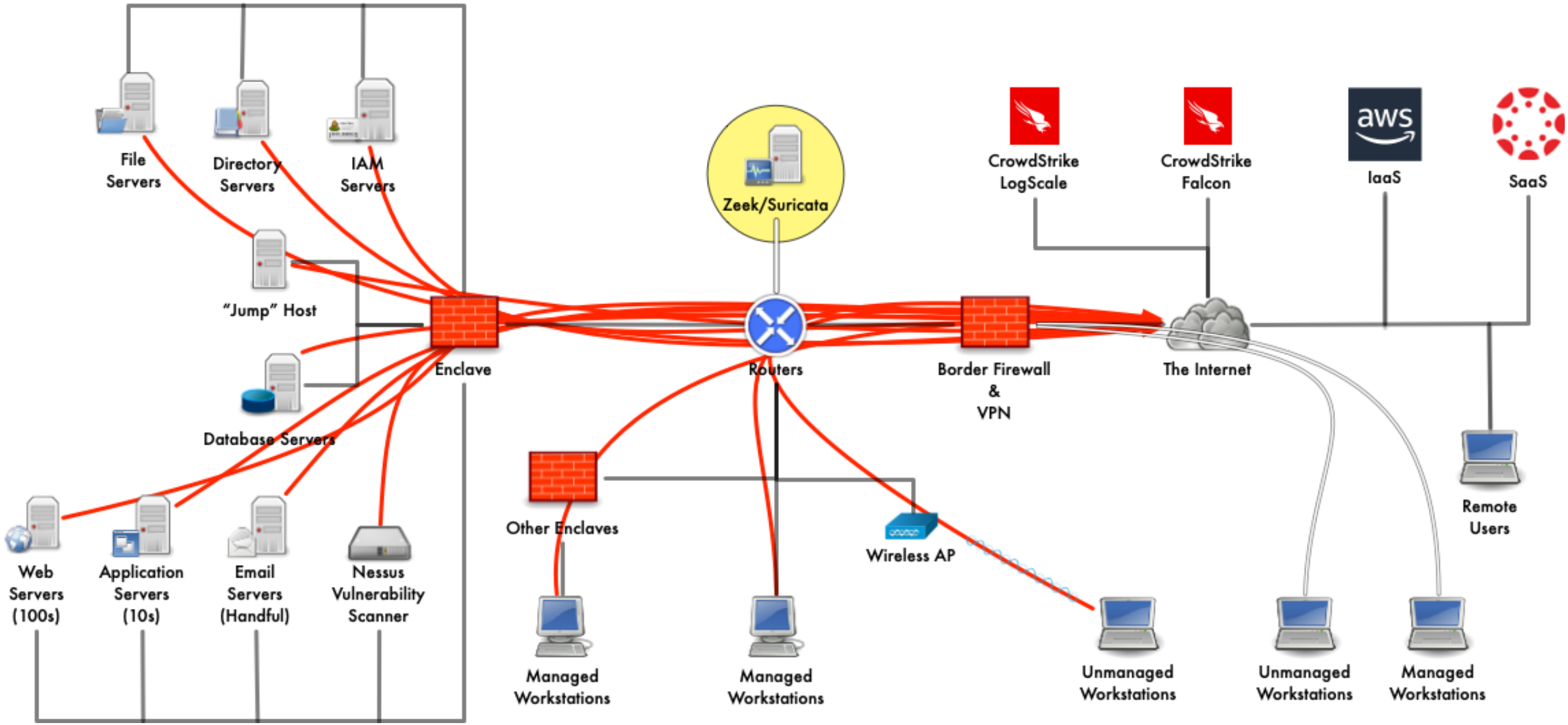


Patch Management Practices

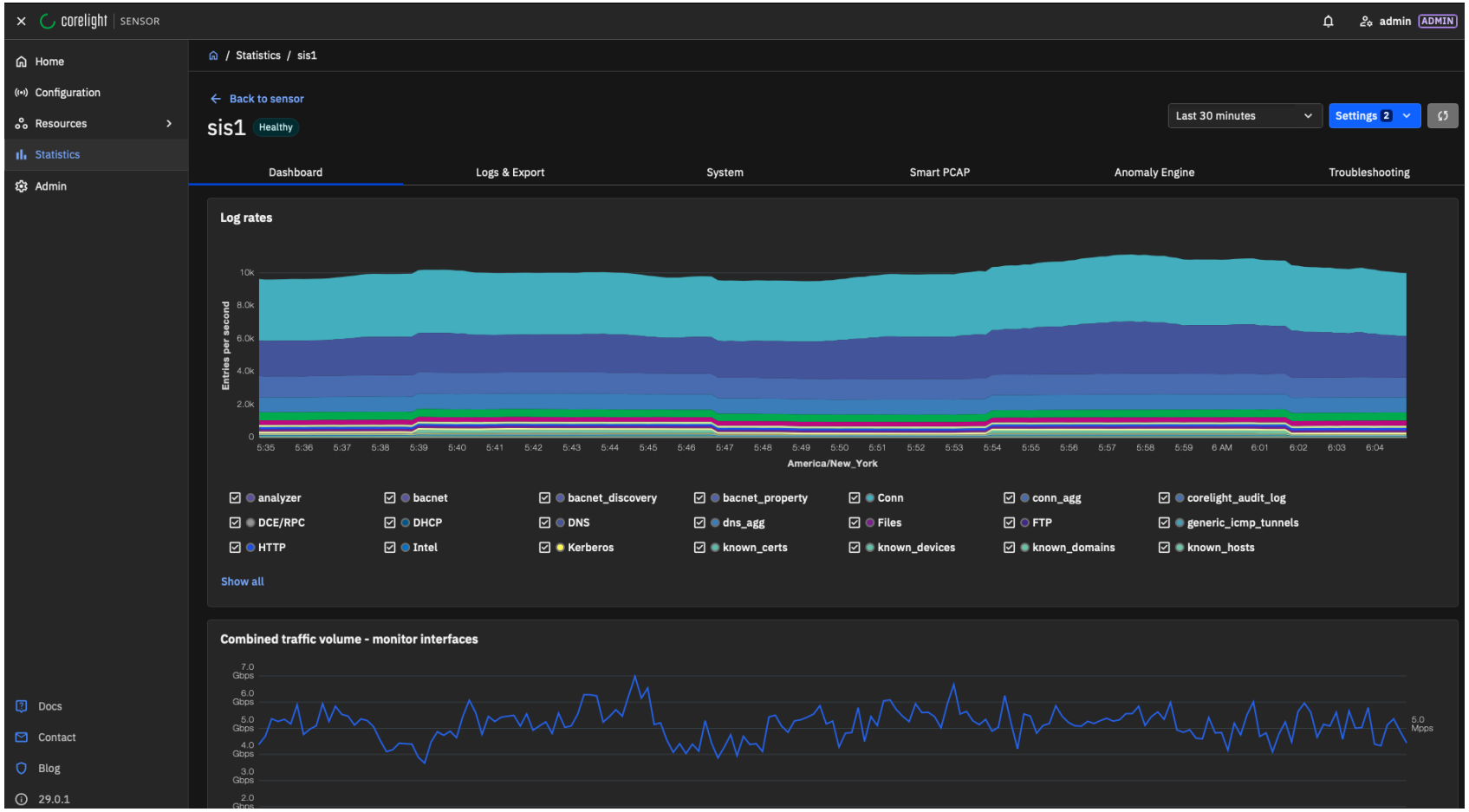
- Prompt patching: 2 business days for critical vulnerabilities.
- Scheduled scans:
  - Daily for Critical Components
  - Weekly for all of campus for Critical vulnerabilities
- Weekly review for situational awareness and to chase down stragglers.
- Defense-in-depth for when you can’t patch fast enough
  - IP access restrictions
  - Force authentication
  - Inbound traffic filtering
  - Endpoint Detection & Response
  - Logging
  - Run less software, or shift risk to SaaS

Detection Tools

Reference Deployment



Network Security Monitoring (Zeek)



Zeek Example: visiting a website

{"_path":"dns_agg","_system_name":"sis5","_write_ts":"2026-03-05T20:04:51.586164Z","answers":["3.12.1.154"],"count":1,"id.orig_h":"2607:f470:6:4001:408d:ae6f:2603:7b2e","id.resp_p":53,"qtype":1,"qtype_name":"A","query":"www.samjenk.com","rcode":0,"rcode_name":"NOERROR","rejected":[false],"ts":"2026-03-05T19:59:50.352067Z","ts_last":"2026-03-05T19:59:50.352067Z","uids":["CQvNgO3BAEb1JLKB9"]}

{"_path":"ssl","_system_name":"sis1","_write_ts":"2026-03-05T20:08:35.779048Z","established":false,"id.orig_h":"10.103.99.115","id.orig_p":55827,"id.resp_h":"3.12.1.154","id.resp_p":443,"ja3":"2bab0327a296230f9f6427341e716ea0","resumed":false,"server_name":"www.samjenk.com","ssl_history":"C","ts":"2026-03-05T20:03:35.695199Z","uid":"CUgHCJ31DcL0G0OMSc"}

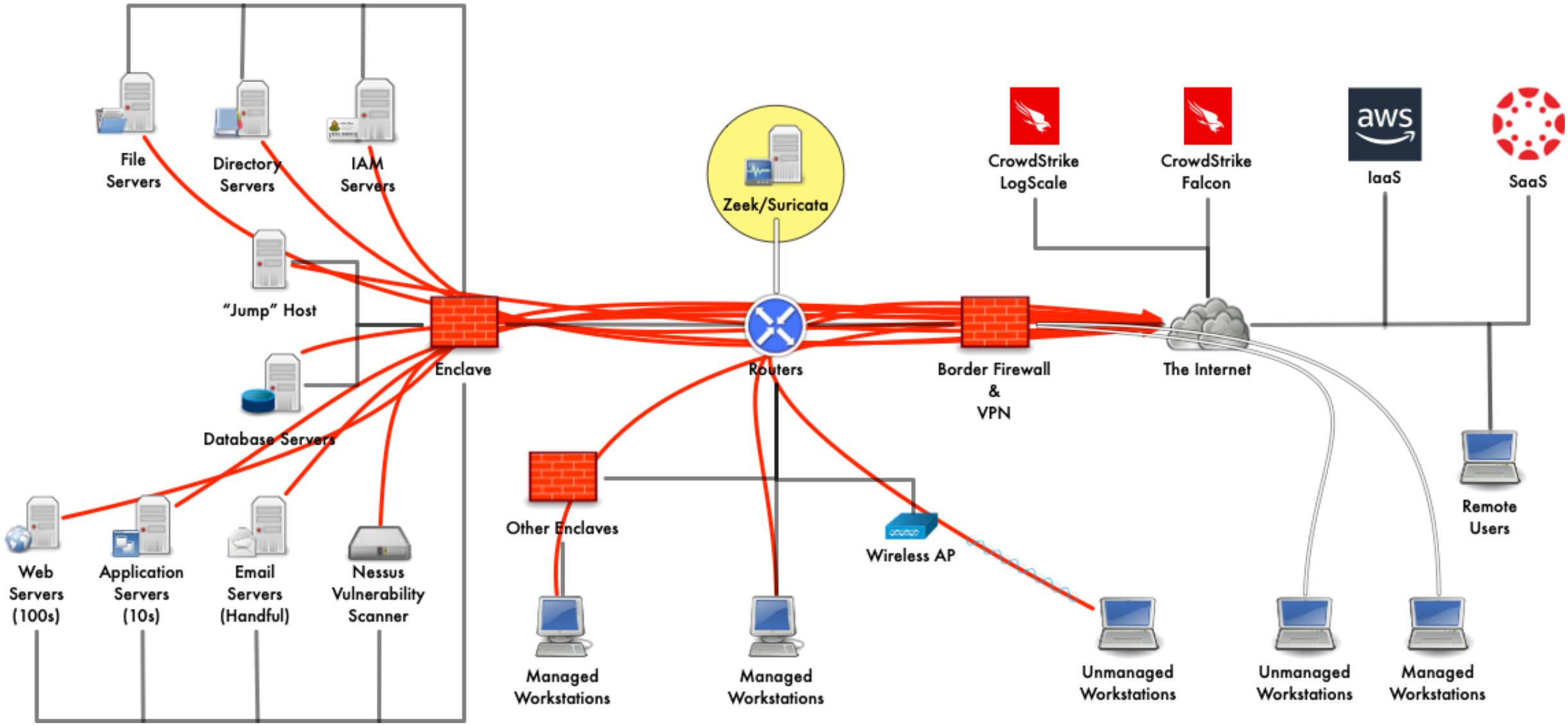
Zeek Example: visiting a website

{"_path":"conn_agg","_system_name":"sis1","_write_ts":"2026-03-05T20:11:48.584732Z","community_ids":["1:bCp6bkheP0Qvz6P2XkYHW80LtEY=","1:cYmXxCTZwdnd94UyfZpeyBc9uEI=","1:v7/hW3/krUDpzfXwyy3wBp2in2k=","1:A3J48BqIt6WmFdb2dcXvzSaaAKk=","1:pyi4kUgXgmbOsfg41fkMYx6uGPs=","1:18Z7xbFRBGgP54j7KOkMsWzyo6c="],"conn_state":"S1","count":6,"duration":0.579904317855835,"history":"^hADaGd","id.orig_h":"10.103.99.115","id.resp_h":"3.12.1.154","id.resp_p":443,"local_orig":true,"local_resp":false,"missed_bytes":3329,"orig_bytes":3190,"orig_ip_bytes":5244,"proto":"tcp","resp_bytes":16914,"resp_ip_bytes":12363,"service":["ssl"],"ts":"2026-03-05T20:01:47.926410Z","ts_last":"2026-03-05T20:05:22.440561Z","uids":["CC3FIC3nJ4ir7ulczb","CwvGwP3sTnmUn1YpC8","CXT2du4k3UodNWZ6lj","CUXj4rny5TIdTtS51","C7N6OD1LJh6c1NuXKg","CUgHCJ31DcL0G0OMSc"]}

Network Monitoring (Zeek)

- Encryption is blinding. We look at metadata.
- Forensics!
- As a passive inventory tool for other workflows

Reference Deployment



Intrusion Detection System (Suricata)

- Straight-forward to implement, hard to tune.
- suricata_eve.log is WAY more useful than suricata.log
- Useful for:
  - Emerging threats
  - Detecting commodity malware
  - When you can break TLS
  - Tightly-controlled networks
  - Flow data, if you have no other options.
- Drawbacks, for Penn:
  - Pay for a lot of stuff that we don’t need
  - Used to spend a lot of time tuning
  - Detect only, no inline block
  - We don’t break TLS

OFFICE OF INFORMATION SECURITY
Always alert, always ready to help.

Example: High Confidence

alert dns $HOME_NET any -> any any (msg:"ET MOBILE_MALWARE APT-C-23 Related CnC Domain in DNS Lookup (javan-demsky .website)"; dns.query; content:"javan-demsky.website"; nocase; bsize:20; reference:md5,dd4596cf68c85eb135f7e0ad763e5dab; reference:url,twitter.com/malwrhunterteam/status/1437498154501480451; reference:url,blog.cyble.com/2021/09/15/apt-c-23-using-new-variant-of-android-spyware-to-target-users-in-the-middle-east/; classtype:domain-c2; sid:2033980; rev:1; metadata:attack_target Mobile_Client, created_at 2021_09_17, deployment Perimeter, former_category MOBILE_MALWARE, signature_severity Major, updated_at 2021_09_17;)

Items in blue (5), plus no false positives (1), plus active in the rule feed (1) = 7

OFFICE OF INFORMATION SECURITY
Always alert, always ready to help.

Example: Medium Confidence

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"ET WORM Win32.Socks.s HTTP Post Checkin"; flow:established,to_server; http.method; content:"POST"; http.uri; content:".php"; http.request_body; content:"proc=[System Process]|0a|"; depth:22; reference:url,doc.emergingthreats.net/2008020; classtype:trojan-activity; sid:2008020; rev:6; metadata:created_at 2010_07_30, updated_at 2020_08_18;)

Items in blue (2) + no false positives (1) + active in rule feed (1) = 4

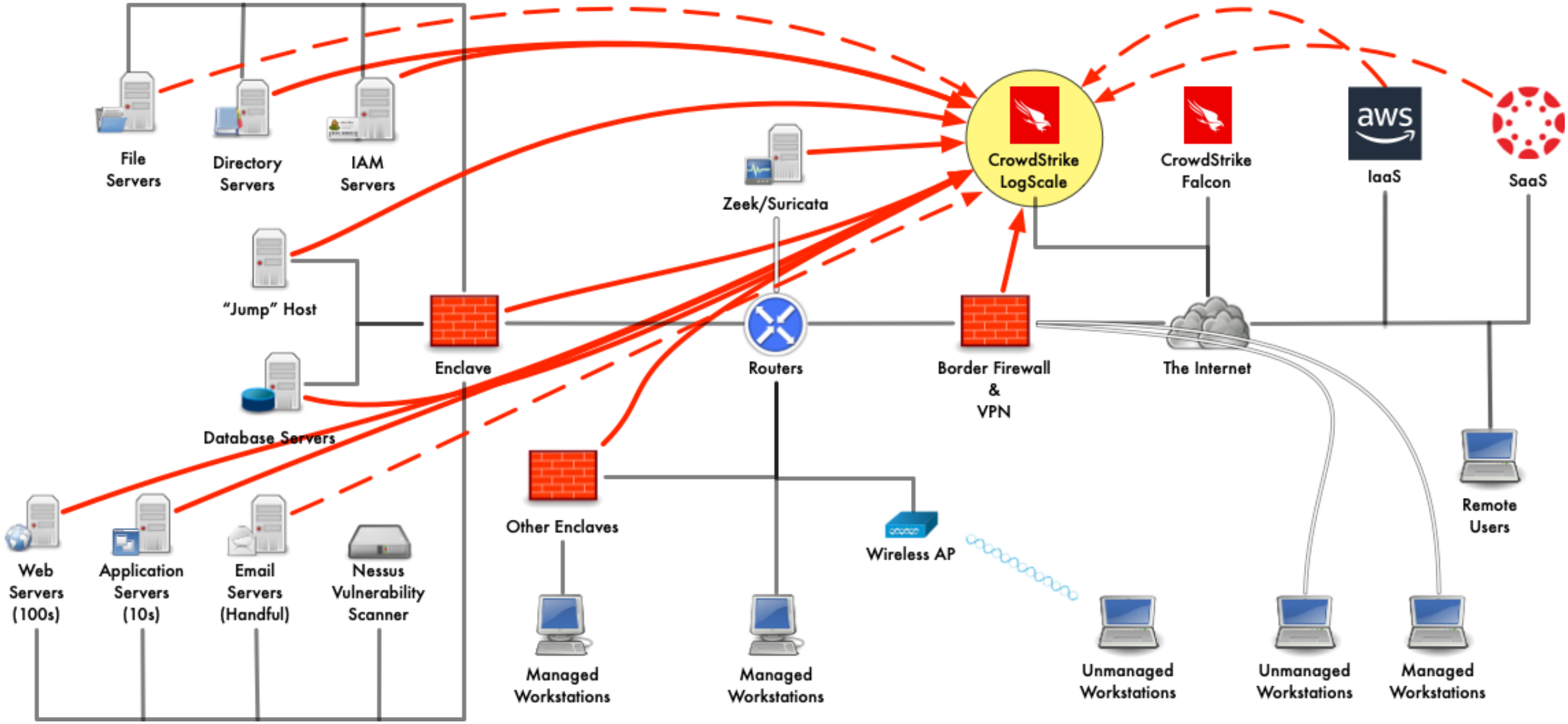
OFFICE OF INFORMATION SECURITY
Always alert, always ready to help.

Example: Low Confidence

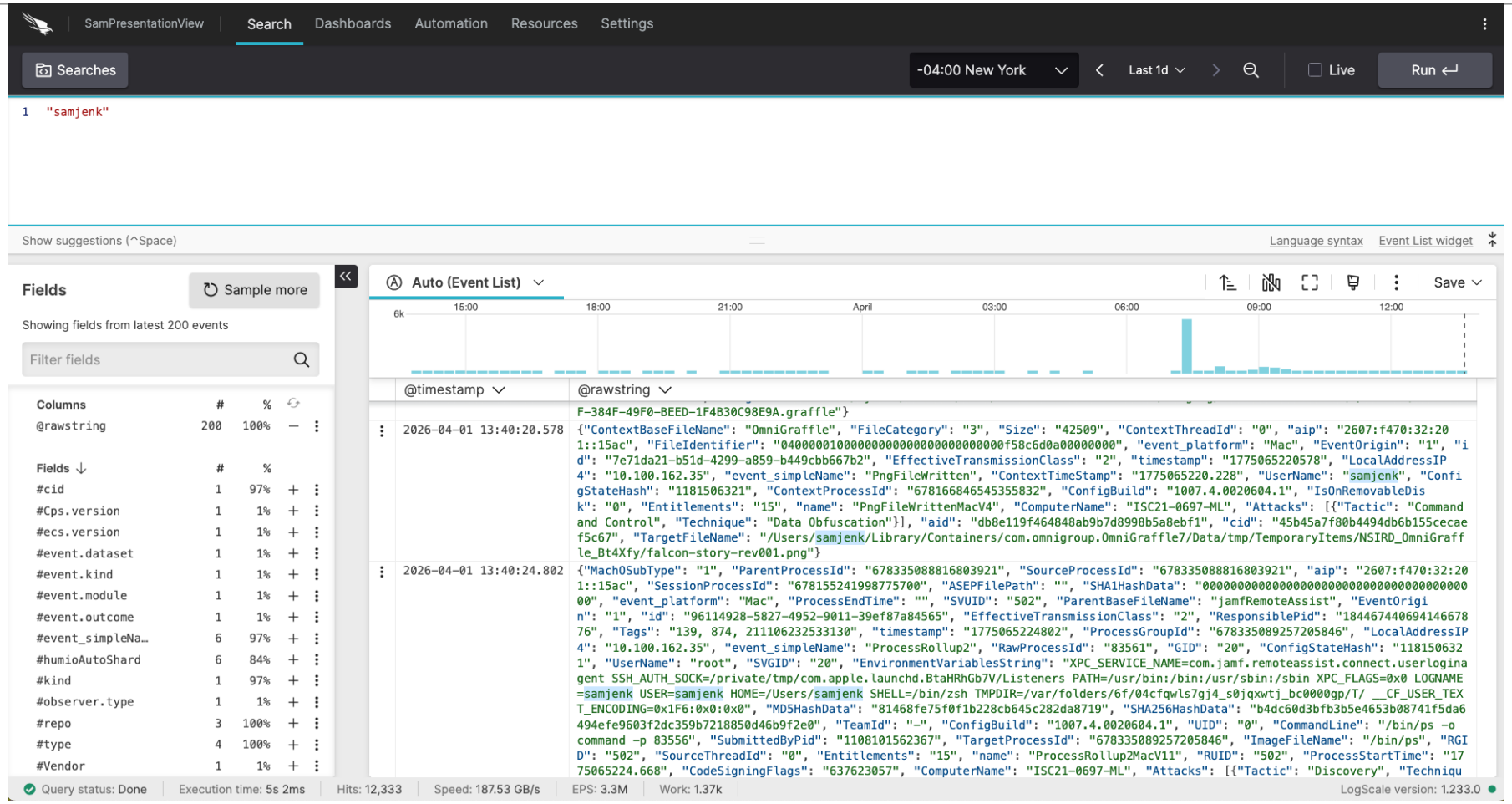
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"ET POLICY Data POST to an image file (gif)"; flow:established,to_server; http.method; content:"POST"; http.uri; content:".gif"; fast_pattern; endswith; content:!"__utm.gif"; endswith; http.host; content:!".tealiumiq.com"; content:!"snackly.co"; content:!"otf.msn.com"; reference:url,doc.emergingthreats.net/2010066; classtype:trojan-activity; sid:2010066; rev:17; metadata:created_at 2010_07_30, former_category POLICY, updated_at 2020_09_16;)

Item in blue (1) + active in rule feed (1) = 2

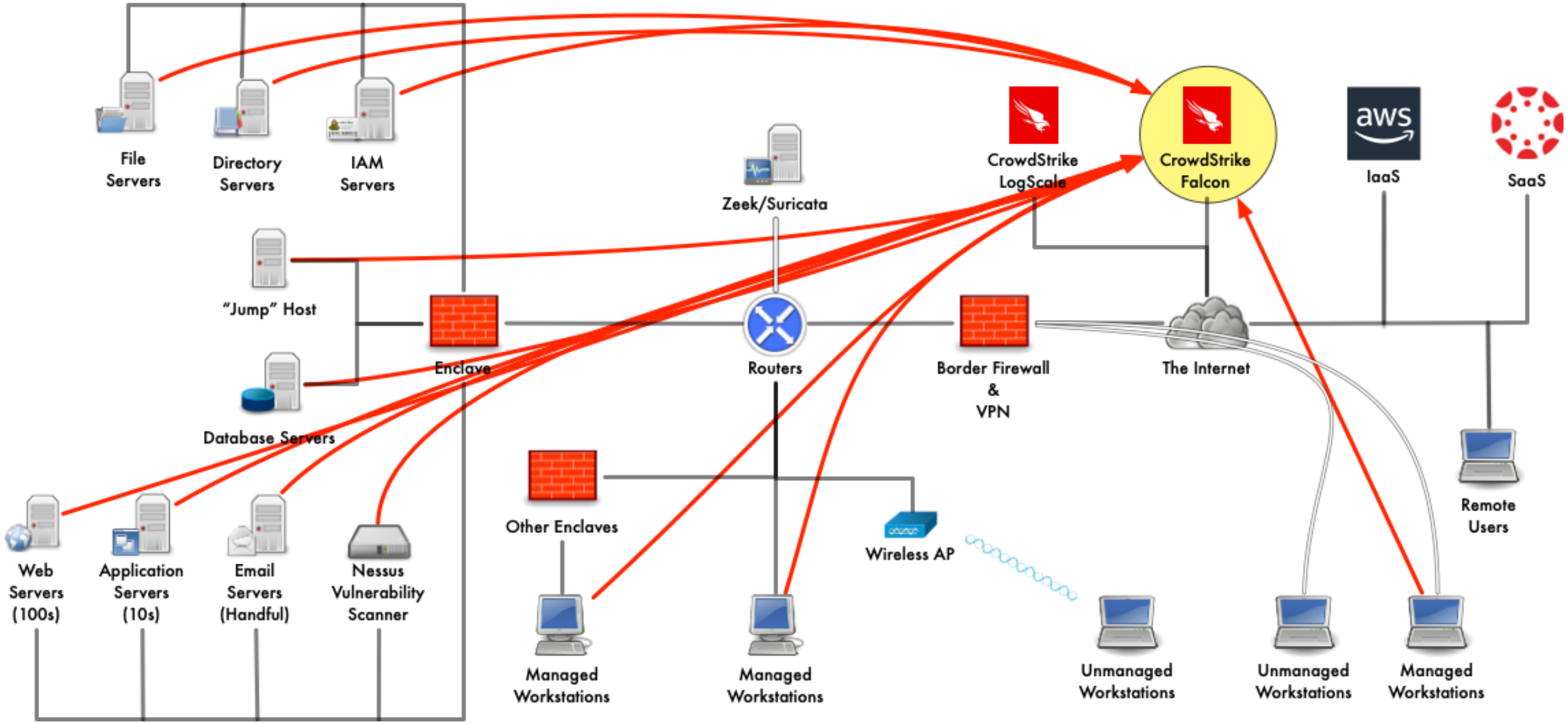
Reference Deployment



Log Analysis (LogScale)

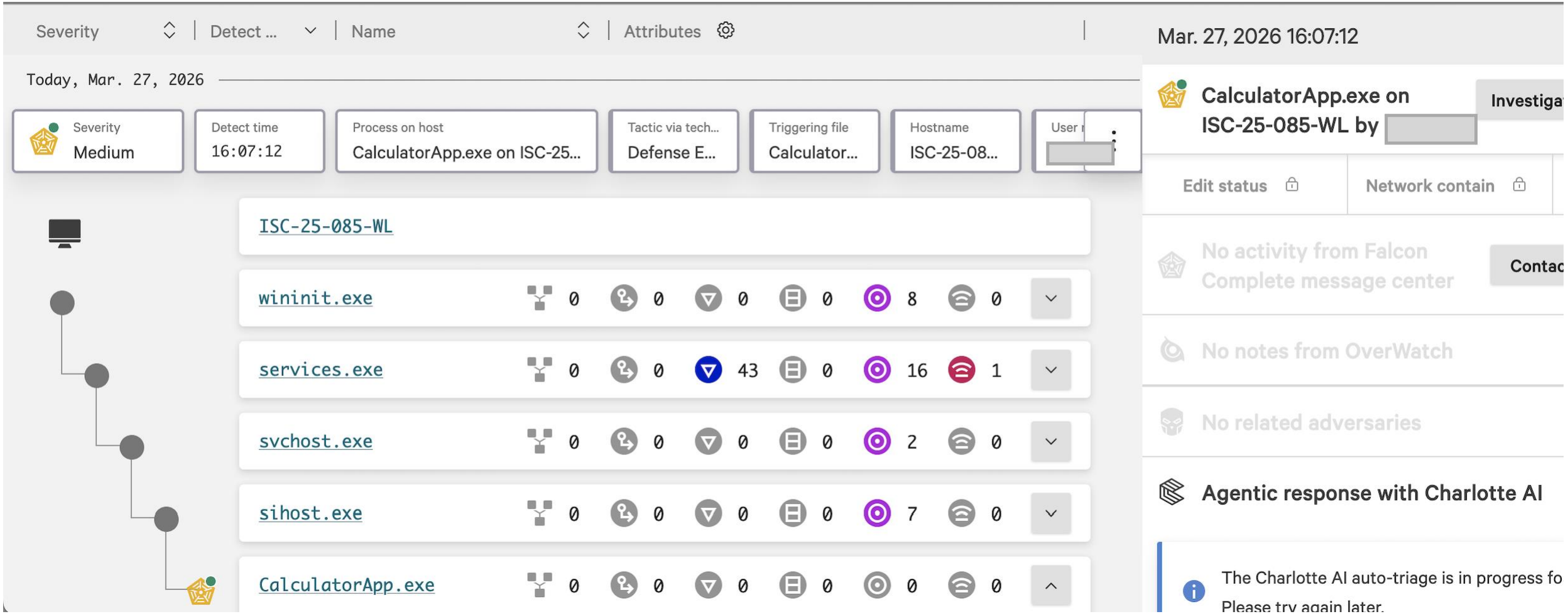


Reference Deployment



Endpoint Detection & Response (Falcon)

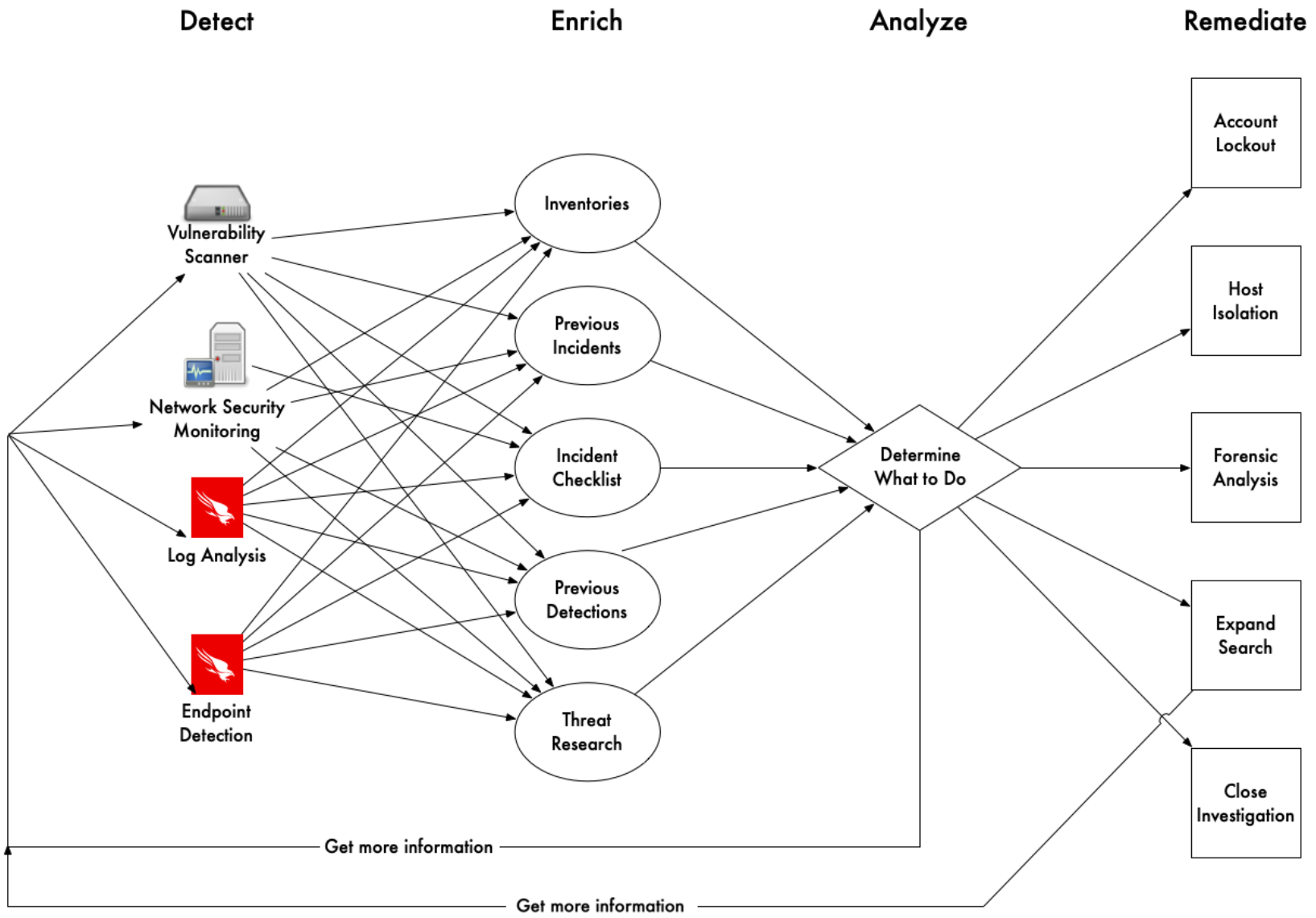
- Pros:
  - Assists with asset discovery
  - Monitors the endpoint when it leaves your network
  - Much more sophisticated that A/V
  - Usually bundled with MSSP services (paid experts)
- Cons:
  - Needs a ton of management: roll-out, alert tuning, response tuning
  - Expensive


Severity
Detect ...
Name
Attributes
Today, Mar. 27, 2026
Severity
Medium
Detect time
16:07:12
Process on host
CalculatorApp.exe on ISC-25...
Tactic via tech...
Defense E...
Triggering file
Calculator...
Hostname
ISC-25-08...
User
ISC-25-085-WL
wininit.exe 0 0 0 0 8 0
services.exe 0 0 43 0 16 1
svchost.exe 0 0 0 0 2 0
sihost.exe 0 0 0 0 7 0
CalculatorApp.exe 0 0 0 0 0 0
Mar. 27, 2026 16:07:12
CalculatorApp.exe on ISC-25-085-WL by
Investiga
Edit status
Network contain
No activity from Falcon Complete message center
Contac
No notes from OverWatch
No related adversaries
Agentic response with Charlotte AI
The Charlotte AI auto-triage is in progress fo
Please try again later.

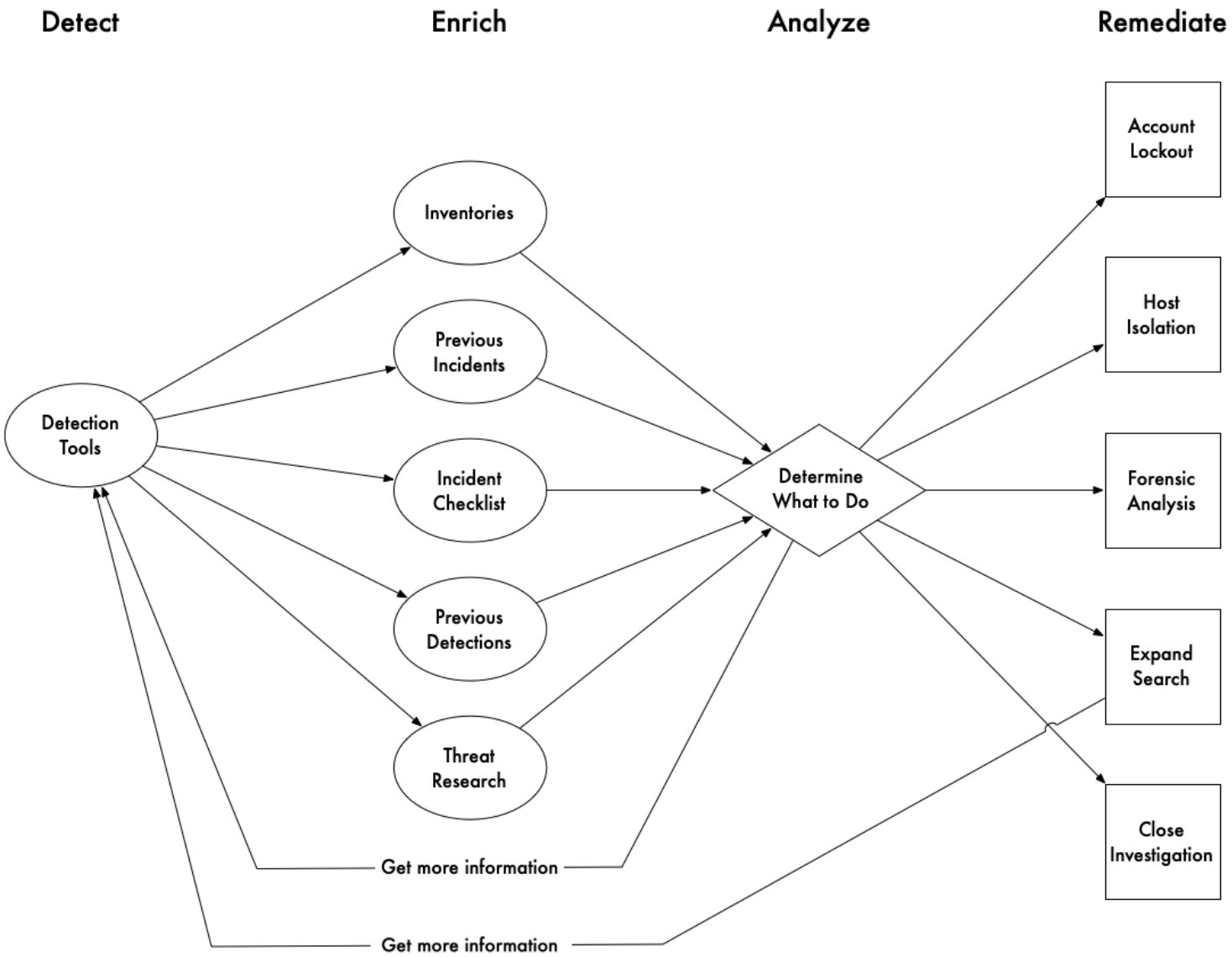
{"ProcessStartTime":1774641939,"ProcessEndTime":1774641939,"ProcessId":296730478583,"ParentProcessId":25365105840
2,"Hostname":"ISC-25-085-WL","UserName":"<Sam's Co-worker>","Name":"Suspicious Activity","Description":"A suspicious
process injected into another process in an unusual way. Investigate the process trees for the injector and
injectee.","Severity":50,"SeverityName":"Medium","FileName":"CalculatorApp.exe","FilePath":"\\Device\\HarddiskVolume3\\
Program
Files\\WindowsApps\\Microsoft.WindowsCalculator_11.2508.4.0_x64__8wekyb3d8bbwe\\CalculatorApp.exe","CommandLin
e":"\"C:\\Program
Files\\WindowsApps\\Microsoft.WindowsCalculator_11.2508.4.0_x64__8wekyb3d8bbwe\\CalculatorApp.exe\"","SHA256Stri
ng":"62b532a855b1151331937cc1dedd94e22bbaca76086d688422e5cb7f9c6b4b05","MD5String":"c189760c967ba93d2dfbcc
b41804df48", "LocalIP":"10.100.128.111","Tactic":"Defense Evasion","Technique":"Process Injection","Objective":"Keep
Access","PatternDispositionDescription":"Prevention, process
killed.","PatternDispositionValue":16,"ParentImageFileName":"sihost.exe","ParentCommandLine":"sihost.exe","GrandParentI
mageFileName":"svchost.exe","GrandParentCommandLine":"C:\\windows\\system32\\svchost.exe -k netsvcs -p -s
UserManager",SourceVendors":"CrowdStrike","SourceProducts":"Falcon
Insight","DataDomains":"Endpoint","AggregateId":"aggind:10fa6536f73c4ecd8690526031e37e6d:60132758769","Type":"ldt",
"ParentImageFilePath":"\\Device\\HarddiskVolume3\\Windows\\System32\\sihost.exe","GrandParentImageFilePath":"\\Devi
ce\\HarddiskVolume3\\Windows\\System32\\svchost.exe","PlatformName":"Windows","RiskScore":22,"UTCTimestamp":177
4642060,"AgentIdString":"10fa6536f73c4ecd8690526031e37e6d","timestamp":"2026-03-
27T20:07:40Z","EventType":"Event_ExternalApiEvent","ExternalApiType":"Event_EppDetectionSummaryEvent"}

Incident Response Stories

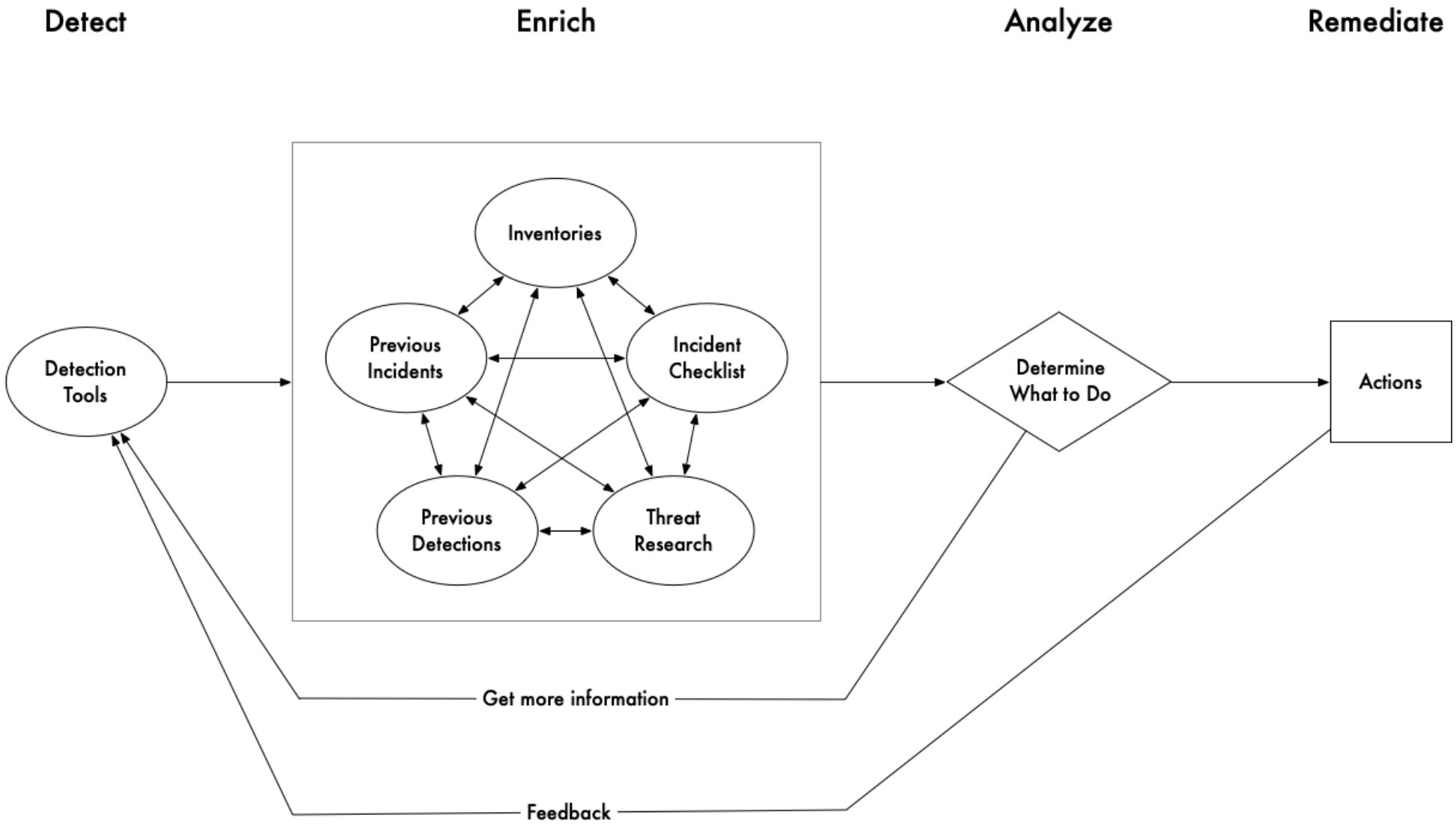
Tools & Inventories = Workflows



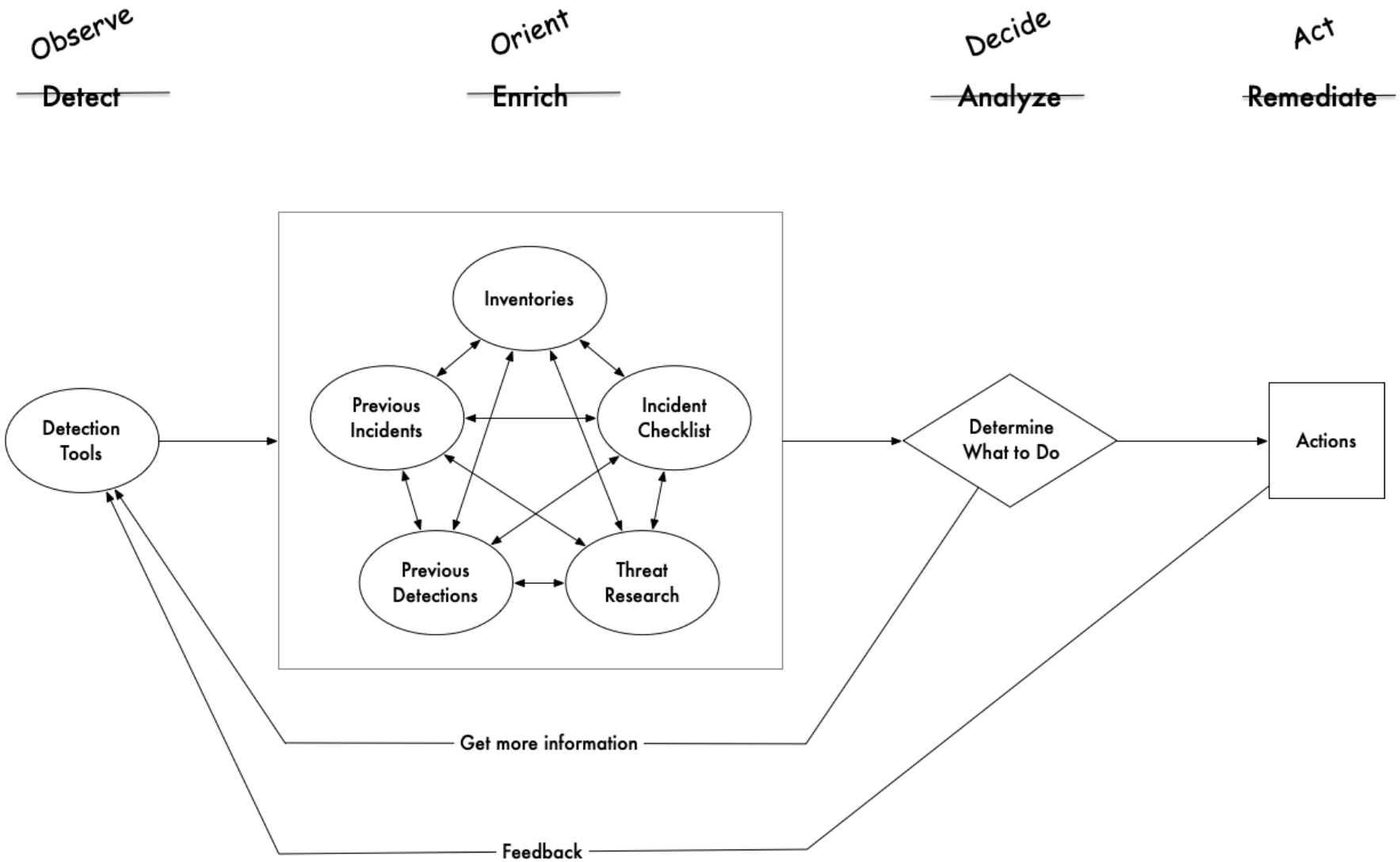
Tools & Inventories = Workflows



Tools & Inventories = Workflows



Tools & Inventories = Workflows



Suricata Rule

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"ET MALWARE Jupyter Stealer CnC Checkin M2"; flow:established,to_server; http.start; content:"POST / HTTP/1.1|0d 0a|Host|3a 20|"; startswith; http.host.raw; pcre:"/^\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}$/"; http.header_names; content:"|0d 0a|Host|0d 0a|Content-Length|0d 0a|Expect|0d 0a|Connection|0d 0a 0d 0a|"; bsize:46; fast_pattern; http.content_len; byte_test:0,>=,200,0,string,dec; byte_test:0,<=,999,0,string,dec; http.connection; content:"Keep-Alive"; bsize:10; http.request_body; content:!"|0d 0a|"; pcre:"/^[\x20-\x7e\r\n]{0,20}[^\x20-\x7e\r\n]/"; reference:md5,772816f913a48aabe00ab1e7db8aa48e; reference:url,blogs.vmware.com/security/2023/11/jupyter-rising-an-update-on-jupyter-infostealer.html; classtype:trojan-activity; sid:2050051; rev:1; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, affected_product Windows_11, attack_target Client_Endpoint, created_at 2024_01_12, deployment Perimeter, malware_family Stealer, malware_family Jupyter, confidence Medium, signature_severity Major, updated_at 2024_01_12, mitre_tactic_id TA0009, mitre_tactic_name Collection, mitre_technique_id T1005, mitre_technique_name Data_from_local_system; target:src_ip;)

Suricata Detection: eve log snippet

alert.action: allowed

alert.signature: ET MALWARE Jupyter Stealer CnC Checkin M2

alert.category: A Network Trojan was detected

alert.severity: 1

alert.source.ip: 146.70.80.66

alert.source.port: 80

alert.target.ip: 10.103.43.173

alert.target.port: 50525

direction: to_server

event_type: alert

files.filename: /

files.gaps: False

files.state: CLOSED

files.stored: False

files.size: 710

http.hostname: 146.70.80.66

http.url: /

http.http_content_type: text/html

http.http_method: POST

http.protocol: HTTP/1.1

http.status: 503

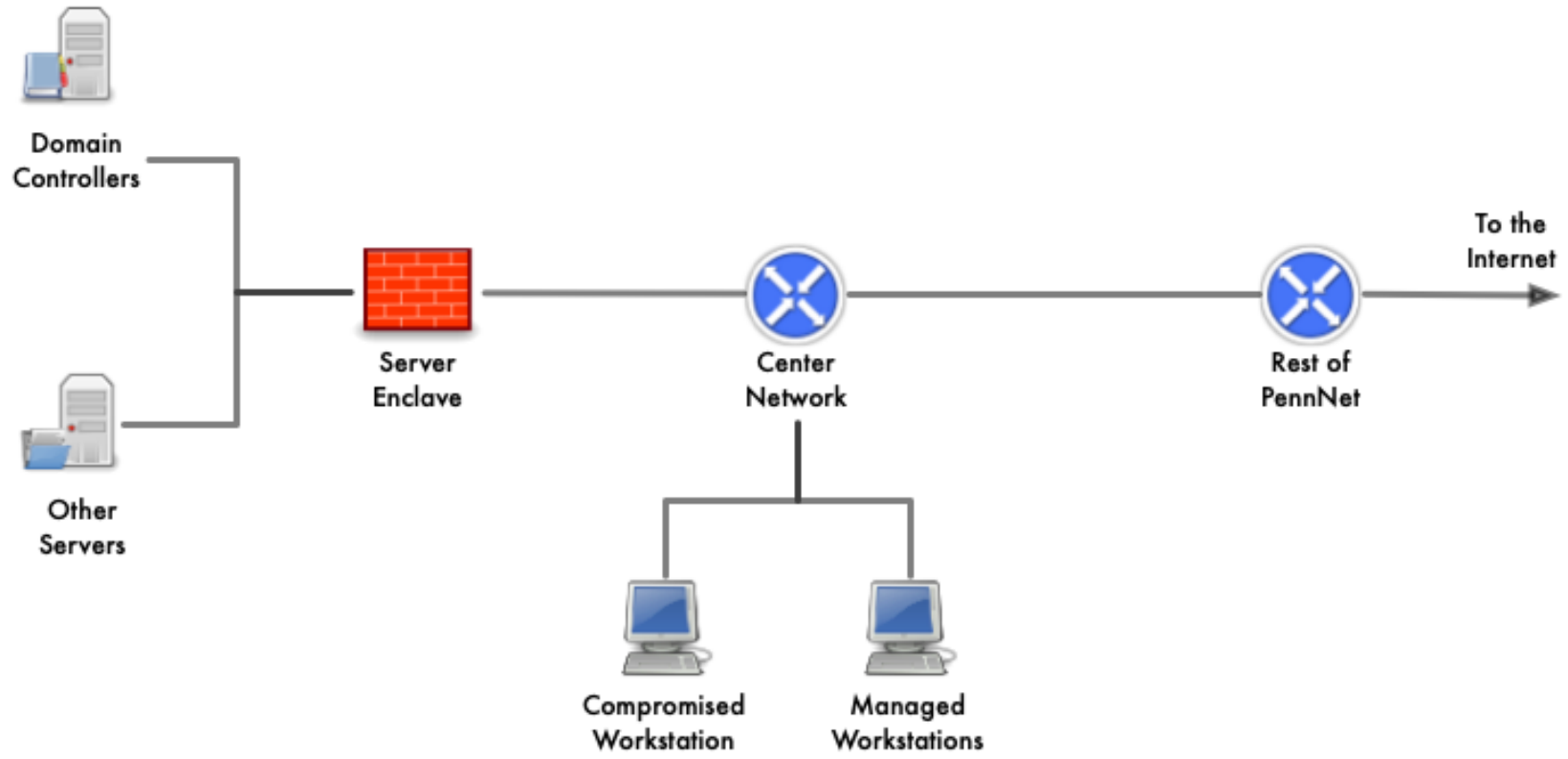
http.length: 190

proto: TCP

Zeek Detections

- As threat intelligence on external hosts:
  - Probing RDP, ARD and VNC (rdp.log, rfb.log)
  - Attempting Log4j/jndi exploits (http.log)
  - Scanning campus hosts.
- As alerting on Penn hosts:
  - conducting unauthorized scans
  - mining cryptocurrencies (students exempted)
  - RDP connections between schools/centers (noisy)
- Threat hunting during incident response

Crowdstrike Falcon



Philippines Login Incident

- Detect: A medium-confidence alert fired (multiple logins from same IP address)
- Enrich: Looking into it, I saw that none of the users were enrolled in multifactor auth.
- Analysis:
  - All of the logins were from the Philippines
  - All of the logins were for users in the same department
  - All of the users were not enrolled in MFA
  - Conclusion: lock and remediate the accounts, notify their IT support
- Detect: two days later, same alert for the same people!
- Enrich: the users had all reset their passwords!
- Conclusion: users needed to input data to a rickety old app with no impersonation feature, shared passwords with a contractor to input the data

Security operations is about workflows, not tools

Backup Slides

AI in everything

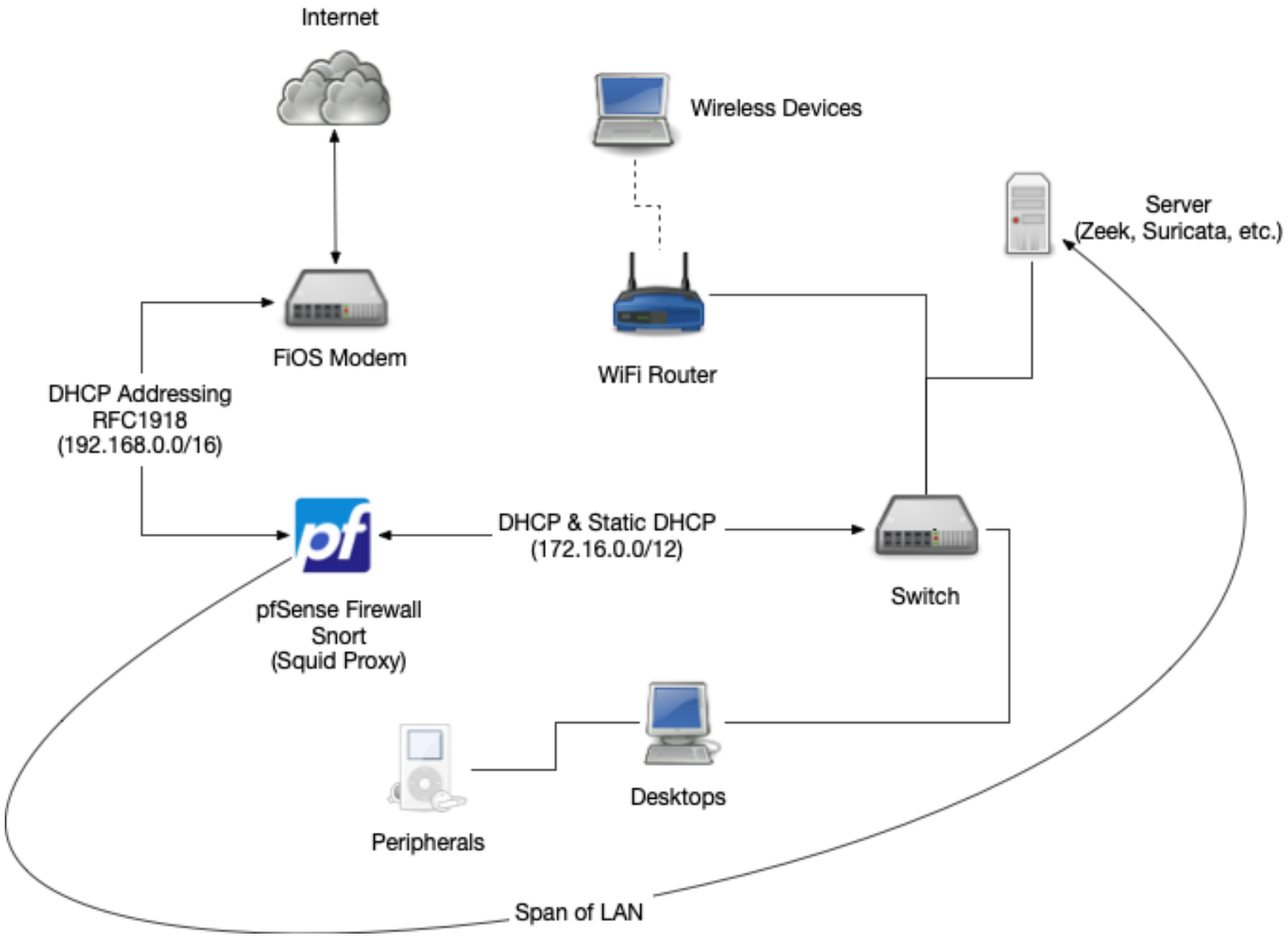
- Done well: Expert systems
  - Put the AI in the tool to help you make decisions within a confined domain.
    - Powerpoint helped me design the “Vulnerability Management” slide
  - Online-go (given what I’ve seen of this host, what’s the current probability that it will be compromised?)
- Agents are promising for workflow automation
- Done poorly:
  - The “Who is Chris Hyzer?” problem
  - Colleague who takes longer to answer a simple question because he insists on running my query through AI.
  - Generate inaccurate diagrams with confidence!
  - Make it available, but licensing and token costs are barriers to use
- What do you all think? What have you seen work well?

Career advice

1. Enjoy the challenge of adapting what you learn to real-world constraints.
2. Be good at managing lists.
3. Documentation is always behind reality.
4. The problems are technical, but the challenges are organizational.
5. Become comfortable with ambiguity, but don’t put up with it.
6. Join your industry’s Information Sharing & Analysis Center (ISAC)

Career advice 2

1. If you're going into operations:
    1. Enjoy solving problems
    2. Be comfortable with ambiguity
    3. Keep learning new things
    4. Treasure your good COTS tools
2. If you're going to make security products:
    1. Do as little as possible really really well. (Corelight, Splunk/LogScale)
    2. Make underlying data as accessible as possible (Corelight, Falcon)
    3. Don't assume you know how your tool will be deployed


Internet
Wireless Devices
Server
(Zeek, Suricata, etc.)
FiOS Modem
WiFi Router
DHCP Addressing
RFC1918
(192.168.0.0/16)
DHCP & Static DHCP
(172.16.0.0/12)
Switch
pfSense Firewall
Snort
(Squid Proxy)
Desktops
Peripherals
Span of LAN

Recommended Reading

- *The Practice of Network Security Monitoring* (Bejtlich)
- *The Unix and Linux System Administration Handbook* (Nemeth, et al)
- *The TCP/IP Guide* (Kozierok)
- *The Cuckoo's Egg* (Stoll)